Forslag
til
Lov om ændring af lov om finansiel virksomhed, lov om betalinger, lov om kapitalmarkeder og forskellige andre love[1]

(Tilsyn efter forordning om digital operationel modstandsdygtighed i den finansielle sektor og forordning om markeder for kryptoaktiver)

§ 1

I lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 406 af 29. marts 2022, som ændret bl.a. ved § 1 i lov nr. 2383 af 14. december 2021, § 5 i lov nr. 568 af 10. maj 2022, § 1 i lov nr. 570 af 10. maj 2022, § 7 i lov nr. 243 af 7. marts 2023, § 27 i lov nr. 405 af 25. april 2023, § 1 i lov nr. 409 af 25. april 2023, § 3 i lov nr. 480 af 12. maj 2023 og senest ved § 337 i lov nr. 718 af 13. juni 2023, foretages følgende ændringer:

1. I *fodnoten* til lovens titel udgår »dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 (NIS-direktivet), EU-Tidende 2016, nr. L 194, side 1,«, og »og dele af Europa-Parlamentets og Rådets direktiv (EU) 2019/2162 af 27. november 2019 om udstedelse af dækkede obligationer og offentligt tilsyn med dækkede obligationer og om ændring af direktiv 2009/65/EF og 2014/59/EU, EU-Tidende 2019, nr. L 328, side 29« ændres til: »dele af Europa-Parlamentets og Rådets direktiv (EU) 2019/2162 af 27. november 2019 om udstedelse af dækkede obligationer og offentligt tilsyn med dækkede obligationer og om ændring af direktiv 2009/65/EF og 2014/59/EU, EU-Tidende 2019,

[1] Loven indeholder bestemmelser, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014, EU-Tidende 2014, nr. L 173, side 349, dele af Europa-Parlamentets og Rådets direktiv (EU) 2019/2177 af 18. december 2019 om ændring af direktiv 2009/138/EF om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II), direktiv 2014/65/EU om markeder for finansielle instrumenter og af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme (omnibusdirektivet), EU-Tidende 2019, L 334, side 155, og dele af Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, EU-tidende 2015, L 337, side 35. I loven er der medtaget visse bestemmelser fra Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, EU-Tidende 2023, L 150, side 40. Ifølge artikel 288 i EUF-Traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i loven er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark

nr. L 328, side 29 og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

2. I *§ 1* indsættes efter stk. 13 som nyt stykke:

»*Stk. 14.* Kapitel 19 b finder anvendelse på fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse af kryptoaktiver til handel, eller som leverer tjenesteydelser i forbindelse med kryptoaktiver.«
Stk. 14-18 bliver herefter stk. 15-19.

3. I *§ 10, stk. 1, 2. pkt.,* indsættes efter »§ 10 a«: », § 10 b«.

4. Efter § 10 a indsættes:

»§ 10 b. Et investeringsforvaltningsselskab kan levere tjenester med kryptoaktiver som angivet i artikel 60, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, svarende til de tjenester, som det er meddelt tilladelse til i henhold til § 10, hvis selskabet giver Finanstilsynet meddelelse mindst 40 arbejdsdage inden disse tjenester leveres første gang. Meddelelsen skal ledsages af de oplysninger, der er anført i artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

5. I *§ 71, stk. 1, nr. 8,* indsættes efter »it-området«: »og for net- og informationssystemer, som oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 om digital operationel modstandsdygtighed i den finansielle sektor«.

6. *§ 71, stk. 2, 2. pkt.,* ophæves.

7. I *§ 72 a* indsættes som *stk. 4:*

»*Stk. 4.* Stk. 1-3 finder ikke anvendelse for outsourcing på det digitale operationelle område.«

8. *§ 72 c* ophæves.

9. I *§ 80, stk. 5,* udgår »Landbrugets FinansieringsBank A/S,«.

10. I *§ 124, stk. 2,* indsættes som *3. pkt.:* »Den del af solvensbehovet, der vedrører overdreven risiko for gearing opgøres i procent af den samlede

ikke-risikovægtede eksponering.«, og i *§ 124, stk. 3, 3. pkt.,* der bliver 4. pkt., indsættes efter »i artikel 93«: »eller gearingsgradskravet efter artikel 92, stk. 1, litra d,«.

11. I *§ 124, stk. 3, 1. pkt.,* indsættes efter: »92, stk. 1, litra c,«: »eller til gearingsgradskravet, der fremgår af artikel 92, stk. 1, litra d,«, og i *§ 124, stk. 3, 2. pkt.,* indsættes efter »samlede risikoeksponering«: »og i procent af den ikke-risikovægtede eksponering, hvis solvenskravet vedrører risiko for overdreven gearing«.

12. I *§ 124 a, stk. 1, 1. pkt.,* ændres: »meddeler« til: »informerer«.

13. I *§ 124 a, stk. 1, 2. pkt.,* indsættes efter: »risikoeksponering«: »og i procent af den samlede ikke-risikovægtede eksponering«.

14. I *§ 124 a, stk. 3,* udgår »egentlig« og »egentlige«.

15. I *§ 125 d, stk. 1,* indsættes efter »§ 125 a, stk. 1,«: »eller gearingsgradbufferkravet, jf. artikel 92 stk. 1, litra a, hvis gearingsgradsbufferkravet finder anvendelse,«, og »§ 125 b, stk. 3,« ændres til: »§ 125 b, stk. 5,«.

16. *§ 199, stk. 12, 2. pkt.,* ophæves.

17. I *§ 224, stk. 1, nr. 1,* indsættes efter »om markeder for finansielle instrumenter«: »og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

18. I *§ 267, stk. 2,* ændres »der er omfattet af stk. 1, nr. 2-4, og som opfylder kravene i artikel 92 a eller 92 b i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter«, til: »der opfylder betingelserne i artikel 72 a-72 d i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter med de fradrag, der følger af artikel 72 e i nævnte forordning, eller nedskrivningsegnede forpligtelser, der er omfattet af stk. 1, nr. 3 og 4, dog således at forpligtelserne skal opfylde kravene i artikel 72 a-72 d med undtagelse af betingelsen i artikel 72 a, stk. 2, litra l«.

19. I *§ 269 a, stk. 3, nr. 2,* ændres »opfylder betingelserne for afvikling« til: »bliver nødlidende eller forventeligt nødlidende, jf. § 224 a«.

20. I *§ 272* indsættes som *stk. 8* og *9:*

»*Stk. 8.* Kapitalejere og kreditorer, hvis krav er blevet nedskrevet eller konverteret i henhold til stk. 1, må ikke lide større tab end ved konkursbehandling af virksomheden eller enheden under afvikling.
Stk. 9. Finanstilsynets vurdering efter stk. 8 foretages på baggrund af værdiansættelsen i § 8 i lov om restrukturering og afvikling af visse finansielle virksomheder. Værdiansættelsen foretages af Finansiel Stabilitet efter anmodning fra Finanstilsynet. Konstateres det, at en kapitalejer eller kreditor, herunder Garantiformuen, har lidt større tab, end den ville have gjort ved konkursbehandling af virksomheden eller enheden, betales forskellen af Afviklingsformuen.«

21. *§ 274, stk. 3,* affattes således:
»Stk. 3. Stk. 1 finder ikke anvendelse, hvis
1) forpligtelsen er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder, eller
2) forpligtelsen er en del af et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, jf. § 2, nr. 19 i lov om restrukturering og afvikling af visse finansielle virksomheder, og overstiger beløbsgrænsen for dækkede indskud, jf. § 9 i lov om en indskyder- og investorgarantiordning, eller
3) forpligtelsen ville være et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, hvis ikke det var foretaget gennem filialer af institutter, der er etableret inden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område, når filialen er beliggende uden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område.«

22. I *§ 275, stk. 1,* indsættes efter »konkurslovens § 97«: », med undtagelse af usikrede obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld«.

23. *Afsnit VIII a* ophæves.

24. *Afsnit IX a* ophæves og i stedet indsættes:

»Afsnit IX a

Offentlig forbrugerinformation

Kapitel 19 a

Offentlig forbrugerinformation

§ 331. Finanstilsynet fremmer den offentlige forbrugerinformation på det finansielle område.

Afsnit IX b

Markeder for kryptoaktiver

Kapitel 19 b

Markeder for kryptoaktiver

Tilladelse og underretning

§ 332. En juridisk person eller anden virksomhed, der udbyder aktivbaserede tokens til offentligheden eller anmoder om optagelse af aktivbaserede tokens til handel i EU, skal være udsteder af disse aktivbaserede tokens og have tilladelse af Finanstilsynet i overensstemmelse med artikel 21, jf. artikel 16, stk. 1, litra a, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.
Stk. 2. Stk. 1 finder ikke anvendelse på et pengeinstitut, der opfylder kravene i artikel 17 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.
Stk. 3. Stk. 1 finder ikke anvendelse på en udsteder af aktivbaserede tokens, som er undtaget efter artikel 16, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, såfremt udstederen giver meddelelse om en hvidbog om kryptoaktiver i overensstemmelse med artikel 19 i samme forordning, og efter anmodning Fra Finanstilsynet giver meddelelse om enhver markedsføringskommunikation til Finanstilsynet.

§ 332 a. En person, der udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU, skal være udsteder af disse, være meddelt tilladelse fra Finanstilsynet som pengeinstitut eller e-pengeinstitut og offentliggøre en hvidbog om kryptoaktiver, som Finanstilsynet er blevet underrettet om i overensstemmelse med artikel 51, jf. artikel 48, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

§ 332 b. En juridisk person eller anden virksomhed, der leverer kryptoaktivtjenester i EU skal have tilladelse af Finanstilsynet efter artikel 63, jf. artikel 59, stk. 1, litra a, i Europa-Parlamentets og Rådets

forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.
Stk. 2. Stk. 1 finder ikke anvendelse på et pengeinstitut, en værdipapircentral, et fondsmæglerselskab, en markedsoperatør, et e-pengeinstitut, et investeringsforvaltningsselskab eller en forvalter af alternative investeringsfonde, der har underrettet Finanstilsynet i henhold til artikel 60, stk. 1-6, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, jf. artikel 59, stk. 1, litra b, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

§ 332 c. I denne lov forstås ved:

1) Kryptoaktiv: En digital gengivelse af en værdi eller af en rettighed, som kan overføres og lagres elektronisk ved hjælp af distributed ledger-teknologi eller lignende teknologi.

2) Aktivbaseret token: En form for kryptoaktiv, der ikke er en elektronisk pengetoken, og som hævdes at bevare en stabil værdi ved at henvise til en anden værdi eller rettighed eller en kombination heraf, herunder en eller flere officielle valutaer.
3) Elektronisk pengetoken eller e-pengetoken: En form for kryptoaktiv, som hævdes at bevare en stabil værdi ved at henvise til værdien af en officiel valuta.
4) Udsteder af kryptoaktiver: En fysisk eller juridisk person eller en anden virksomhed, der udsteder kryptoaktiver.
5) Udbyder af kryptoaktiver: En fysisk eller juridisk person eller en anden virksomhed, eller udstederen, som udbyder kryptoaktiver til offentligheden.
6) Udbyder af kryptoaktivtjenester: En juridisk person eller en anden virksomhed, hvis erhverv eller forretning består i at levere en eller flere kryptoaktivtjenester til kunder på et erhvervsmæssigt grundlag, og som har tilladelse til at levere kryptoaktivtjenester i overensstemmelse med artikel 59 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

7) Kryptoaktivtjeneste: En af nedenstående tjenester og aktiviteter vedrørende ethvert kryptoaktiv:

a) Levering af deponering og administration af kryptoaktiver på kunders vegne.

b) Drift af en handelsplatform for kryptoaktiver.

c) Veksling mellem kryptoaktiver og midler.

d) Veksling mellem kryptoaktiver og andre kryptoaktiver.

e) Udførelse af ordrer vedrørende kryptoaktiver på vegne af kunder.

f) Placering af kryptoaktiver.

g) Modtagelse og formidling af ordrer vedrørende kryptoaktiver på vegne af kunder.

h) Rådgivning om kryptoaktiver.

i) Porteføljepleje i forbindelse med kryptoaktiver.

j) Levering af tjenester vedrørende overførsel af kryptoaktiver på vegne af kunder.

Inddragelse af tilladelse

§ 332 d. Finanstilsynet kan inddrage en tilladelse til en udsteder af aktivbaserede tokens efter artikel 24 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

§ 332 e. Finanstilsynet kan inddrage en tilladelse til en udbyder af kryptoaktivtjenester efter artikel 64 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Indberetning af oplysninger

§ 332 f. En udsteder af aktivbaserede tokens omfattet af § 361, stk. 1, nr. 11, skal senest den 1. juli hvert år indberette summen af udstederens gennemsnitlige udestående til Finanstilsynet, jf. stk. 2.

Stk. 2. Gennemsnittet af de udestående aktivbaserede tokens beregnes som den samlede markedsværdi af de udestående aktivbaserede tokens, opgjort på baggrund af det daglige udestående ved udgangen af hver dag i de foregående 6 måneder. Opgørelsen foretages den første dag i hver måned. Har virksomheden ikke gennemført 6 måneders drift på datoen for beregningen, anvendes de eventuelt gennemførte måneder med drift og virksomhedens estimater for de gennemsnitlige udestående aktivbaserede tokens for det kommende år som grundlag for beregningen.

§ 332 g. En udbyder af kryptoaktivtjenester omfattet af § 361, stk. 1, nr. 12, skal senest den 1. juli hvert år indberette virksomhedens omkostninger til løn, provision og tantieme til Finanstilsynet.

Tilsyn

§ 332 h. Finanstilsynet, eller hvor kompetencen til at udøve enkelte beføjelser ved lov er tillagt andre danske myndigheder, kan til brug for tilsyn med overholdelsen af Europa-Parlamentets og Rådets forordning (EU)

2023/1114 af 31. maj 2023 om markeder for kryptoaktiver udøve de beføjelser, der følger af forordningens artikel 94. Dette inkluderer til enhver tid mod behørig legitimation uden retskendelse at kunne få adgang til lokaler og lokaliteter tilhørende udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, og personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, udstedere af aktivbaserede tokens, udstedere af e-pengetokens og udbydere af kryptoaktivtjenester, med henblik på indhentelse af oplysninger, herunder ved inspektioner.

Afsnit IX c
Operatører af finansielle digitale infrastrukturer

Udpegning af operatører af finansielle digitale infrastrukturer

§ 333. Finanstilsynet kan udpege virksomheder, der udbyder digital infrastruktur eller forvalter it-tjenester, som nævnt i bilag I, pkt. 8 og 9, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022, og hvis væsentligste aktiviteter består i at drive, administrere eller udvikle tjenester, der er nødvendige for kritiske og vigtige forretningsfunktioner i virksomheder, der er omfattet af Europa-Parlamentets og Rådets forordning (EU) 2022/2254 af 14 december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, som operatører af finansielle digitale infrastrukturer.

Stk. 2. Finanstilsynet skal ved udpegningen af en operatør af finansielle digitale infrastrukturer lægge vægt på følgende:

1) Omfanget og antallet af virksomheder i den finansielle sektor som operatøren varetager kritiske og vigtige opgaver for.
2) Karakteren af de kritiske og vigtige funktioner, som er afhængige af operatørens leverancer.
3) Betydningen af operatørens leverancer for den finansielle stabilitet.
4) Operatørens tilknytning til de virksomheder i den finansielle sektor som modtager operatørens ydelser, herunder koncernforbindelser og ejerskab.

Stk. 3. It-operatører af detailbetalingssystemer og virksomheder, der udfører væsentlig drift eller udvikling for den fælles betalingsinfrastruktur, kan udpeges som operatører af finansielle digitale infrastrukturer efter stk. 1.

Stk. 4. Finanstilsynet skal offentliggøre på sin hjemmeside, hvilke virksomheder der er udpeget som operatører af finansielle digitale infrastrukturer.

Stk. 5. Finanstilsynet kan fastsætte nærmere regler om udpegning af operatører af finansielle digitale infrastrukturer og de kriterier, som Finanstilsynet kan lægge vægt på efter stk. 1 og 2.

Foranstaltninger til styring af it- og cyberrisici

§ 333 a. En operatør af finansiel digital infrastruktur skal have en forvaltnings- og kontrolramme, der sikrer en effektiv og forsigtig styring af it- og cyberrisici.

Stk. 2. En operatør af finansiel digital infrastruktur skal, som led i rammen for styring af it- og cyberrisici, træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risici for sikkerheden i net- og informationssystemer.

Stk. 3. Foranstaltningerne nævnt i stk. 2, skal omfatte
1) politikker for risikoanalyse og informationssystemsikkerhed,
2) håndtering af hændelser,
3) driftskontinuitet, herunder backup-styring og reetablering efter større hændelser og krisestyring,
4) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem operatøren og dens direkte leverandører eller tjenesteudbydere,
5) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder,
6) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici,
7) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse,
8) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering,
9) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver, og
10) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i infrastrukturen, hvor det er relevant.

Stk. 4. En operatør af finansiel digital infrastruktur skal, når den overvejer foranstaltninger nævnt i stk. 3, nr. 4, tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder sikkerheden i deres udviklingsprocedurer. Ved vurderingen skal operatøren desuden tage hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der

foretages i overensstemmelse med artikel 22, stk. 1, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022, hvor det er relevant og hvor resultaterne af sådanne vurderinger foreligger.

Ledelse og organisation

§ 333 b. Bestyrelsen i en operatør af finansiel digital infrastruktur skal fastlægge, godkende, føre tilsyn med og har ansvaret for gennemførelsen af operatørens rammer, foranstaltninger og ordninger for it- og cyberrisikostyring. Bestyrelsen skal godkende en strategi for digital operationel modstandsdygtighed, hvormed rammerne for it- og cyberrisikostyring gennemføres.

Stk. 2. En operatør af finansiel digital infrastrukturs tilsyn med styring af sine it- og cyberrisici skal placeres i uafhængige kontrolfunktioner. Operatøren skal sikre adskillelse og uafhængighed mellem it- og cyberrisikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Stk. 3. Rammen for styring af it- og cyberrisici skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it- eller cyberhændelser, og i overensstemmelse med tilsynsmæssige instrukser eller som følge af observationer efter test eller revisioner. Rammen skal forbedres løbende på grundlag af opnåede erfaringer. En operatør af finansiel digital infrastruktur skal kunne dokumentere sin gennemgang af rammen for it- og cyberrisikostyring i en samlet rapport.

Stk. 4. En operatør af finansiel digital infrastrukturs interne revision skal regelmæssigt revidere rammen for styring af it- og cyberrisici. Den interne revision skal have tilstrækkelig viden, faglig kompetence og ekspertise til udførelsen af denne opgave.

Stk. 5. En operatør af finansiel digital infrastruktur skal oprette en funktion med henblik på overvågning af ordninger, der er indgået med tredjepartsudbydere om it-ydelser, eller udpege et direktionsmedlem som ansvarlig for tilsyn og dokumentation i forbindelse med eksponering for it- og cyberrisici fra tredjepartsudbydere.

Stk. 6. En operatør af finansiel digital infrastruktur skal oprette en funktion til krisestyring, som skal håndtere større it- og cyberhændelser, der medfører aktivering af beredskabsplaner, forretningskontinuitetsplaner eller

genopretningsplaner, og være ansvarlig for kommunikationen i forbindelse hermed.

Stk. 7. Bestyrelsesmedlemmerne af en operatør af finansiel digital infrastruktur skal aktivt vedligeholde den viden og de færdigheder, der er nødvendige for at forstå og vurdere it- og cyberrisici og disses indvirkning på driften af operatøren, herunder ved regelmæssigt at følge undervisning, som er passende i forhold til de it- og cyberrisici, som operatøren og dens kunder er eksponeret for.

Stk. 8. Drives en operatør af finansiel digital infrastruktur som en juridisk person uden en bestyrelse, finder stk. 1, og 7, tilsvarende anvendelse for det øverste ledelsesorgan.

Stk. 9. Drives en operatør af finansiel digital infrastruktur som enkeltmandsvirksomhed eller interessentskab, finder stk. 1, og 7, tilsvarende anvendelse for indehavere.

§ 333 c. En operatør af finansiel digital infrastruktur skal dokumentere anvendelsen af sin ramme for styring af it- og cyberrisici i forhold til leverancer, der er nødvendige for kritiske og vigtige funktioner hos kunder, som er omfattet af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstands-dygtighed i den finansielle sektor.

Styring af it- og cyberrisici

§ 333 d. Den ramme for it- og cyberrisikostyring, som en operatør af finansiel digital infrastruktur skal have, jf. § 333 a, skal omfatte en overordnet strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen skal gennemføres.

Stk. 2. En operatør af finansiel digital infrastruktur skal med passende mellemrum foretage identifikation og vurderinger af alle væsentlige it- og cyberrisici, som operatøren og dennes ydelser er eksponeret for.

Stk. 3. Rammen for it- og cyberrisikostyring skal som minimum omfatte strategier, politikker, procedurer og foranstaltninger, som er nødvendige for at beskytte al fysisk og digital infrastruktur og data i overensstemmelse med de identificerede risici, herunder software, hardware, servere, netværk og relaterede fysiske komponenter og infrastrukturer, såsom lokaler, datacentre og sensitive udpegede områder mod risici.

Stk. 4. En operatør af finansiel digital infrastruktur skal modvirke de potentielle virkninger af it- og cyberrisici ved at indføre passende strategier, politikker, procedurer og foranstaltninger. Operatøren skal efter anmodning forelægge fuldstændige og ajourførte oplysninger om sine it- og cyberrisici og om sin ramme for it- og cyberrisikostyring for Finanstilsynet.

Beskyttelse

§ 333 e. En operatør af finansiel digital infrastrukturs it-systemer, it-protokoller og it-værktøjer skal være pålidelige og med tilstrækkelig kapacitet til rettidigt at håndtere de nødvendige transaktioner m.v. i situationer med spidsbelastning, herunder uventet høje spidsbelastninger.

Stk. 2. En operatør af finansiel digital infrastruktur skal løbende identificere alle kritiske forretningsfunktioner og it-aktiver, herunder it-aktiver, der understøtter kritiske og vigtige forretningsfunktioner for operatørens kunder.

Stk. 3. En operatør af finansiel digital infrastruktur skal identificere alle kritiske eller vigtige forretningsprocesser og tjenester, der er afhængige af eksterne leverandører, og dokumentere egne og kunders afhængigheder af ydelser fra underleverandører.

Stk. 4. En operatør af finansiel digital infrastruktur skal overvåge og kontrollere it-systemernes og it-værktøjernes funktion og sikkerhed og minimere virkningerne af it- og cyberrisici ved at indføre passende sikkerhedsværktøjer, -politikker og -procedurer. Operatøren skal løbende identificere potentielle sårbarheder og single points of failure.

Stk. 5. En operatør af finansiel digital infrastruktur skal udforme og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er egnede til at sikre modstandsdygtighed, stabilitet og tilgængelighed for it-systemer, der understøtter kritiske eller vigtige funktioner og til at opretholde et højt niveau af tilgængelighed, autenticitet, integritet og fortrolighed af data.

Stk. 6. En operatør af finansiel digital infrastruktur skal indføre mekanismer til overvågning og sporing af anormale aktiviteter, trusler og hændelser i relevant infrastruktur og fastsætte tærskler for igangsættelse af indsats- og beredskabsforanstaltninger.

Stk. 7. En operatør af finansiel digital infrastruktur skal have en politik for it-driftsstabilitet.

Stk. 8. En operatør af finansiel digital infrastruktur skal gennemføre politikken for it-driftsstabilitet, jf. stk. 7, ved hjælp af dokumenterede beredskabsplaner, ordninger, procedurer mv., med henblik på
1) at sikre, at operatørens og dennes kunders kritiske eller vigtige funktioner er stabile,
2) hurtigt, passende og effektivt at sætte ind over for og løse alle it-relaterede hændelser på en måde, der begrænser skaden og prioriterer genoptagelsen af aktiviteter og genopretningstiltag,
3) omgående at aktivere planer, der omfatter inddæmningsforanstaltninger, der er passende i forhold til hændelserne og som forhindrer yderligere skade,
4) at anslå foreløbige virkninger, skader og tab, og
5) at indføre kommunikations- og krisestyringstiltag, der sikrer, at ajourførte oplysninger videresendes til al relevant internt personale og eksterne interessenter og indberettes til Finanstilsynet.

Stk. 9. En operatør af finansiel digital infrastruktur skal have politikker og procedurer for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Operatøren skal endvidere have procedurer og metoder for gendannelse og genopretning efter væsentlige hændelser.

Stk. 10. En operatør af finansiel digital infrastruktur skal regelmæssigt teste sine foranstaltninger til beredskab, indsats, genopretning, sikkerhedskopiering og gendannelse.

Stk. 11. En operatør af finansiel digital infrastruktur skal udvikle politikker for en systematisk læring på baggrund af den viden, som operatøren opnår ved opfølgning på sin ramme for risikostyring, trusselsovervågning, testresultater og it- og cyberhændelser. Den opnåede viden skal danne grundlag for en årlig rapportering til ledelsesorganet med anbefalinger til forbedringer i relevant omfang.

Stk. 12. En operatør af finansiel digital infrastruktur skal have beredskab for krisekommunikation og ansvarlig offentliggørelse af oplysninger om større cyberhændelser eller væsentlige sårbarheder til berørte parter, herunder kunder, modparter og offentligheden.

Styring og indberetning af it- og cyberhændelser

§ 333 f. En operatør af finansiel digital infrastruktur skal fastlægge og følge en proces for overvågning, styring og indberetning af it- og cyberhændelser.

Stk. 2. En operatør af finansiel digital infrastruktur skal registrere alle it- og cyberhændelser og væsentlige cybertrusler. Operatøren skal fastlægge passende procedurer, der sikrer en konsekvent og integreret overvågning, håndtering og opfølgning af it- og cyberhændelser og at de grundlæggende årsager identificeres, dokumenteres og håndteres.

Stk. 3. En operatør af finansiel digital infrastruktur skal indberette væsentlige it- og cyberhændelser til Finanstilsynet og CSIRT'en oprettet i medfør af artikel 10, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022. Indberetningen skal indeholde alle oplysninger, der er nødvendige for Finanstilsynet til at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Stk. 4. En hændelse, jf. stk. 3, anses for væsentlig, hvis

1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for operatøren, eller
2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

Stk. 5. Ved indberetning, jf. stk. 3, skal en operatør af digital finansiel infrastruktur:

1) Uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at have fået kendskab til den væsentlige hændelse fremsende en tidlig varsling, som skal angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning.

2) Uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse fremsende en hændelsesunderretning, som skal ajourføre de oplysninger, der er nævnt under nr. 1 og en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger.

3) Efter anmodning fra Finanstilsynet eller fra CSIRT'en fremsende en foreløbig rapport om relevante statusopdateringer.

4) Fremsende en endelig rapport senest en måned efter forelæggelsen af den i nr. 2 nævnte hændelsesunderretning, der skal omfatte følgende:

a) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning.

b) Den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen.
c) Anvendte og igangværende afbødende foranstaltninger.
d) Oplysninger om eventuelle grænseoverskridende virkninger af hændelsen.

5) Forelægge en statusrapport for Finanstilsynet og CSIRT'en senest en måned efter forelæggelsen af den i nr. 2 nævnte hændelsesunderretning, hvis hændelsen fortsat pågår på dette tidspunkt, og en endelig rapport senest en måned efter operatørens håndtering af hændelsen.

Stk. 6. En operatør af finansiel digital infrastruktur skal, hvor det er relevant, uden unødigt ophold underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt.

Stk. 7. En operatør af finansiel digital infrastruktur skal uden unødigt ophold underrette modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller modforholdsregler, som disse modtagere kan træffe som reaktion på den pågældende trussel. Operatøren skal også informere de pågældende modtagere om den konkrete væsentlige cybertrussel, hvor dette er relevant.

Stk. 8. En operatør af finansiel digital infrastruktur kan underrette Finanstilsynet om væsentlige cybertrusler, når den anser truslen for at være relevant for det finansielle system, tjenestebrugere eller kunder.

Trusselsbaseret penetrationstest

§ 333 g. En operatør af finansiel digital infrastruktur skal løbende teste effektiviteten af sine foranstaltninger til sikring mod it- og cyberhændelser, der har eller kan have skadelige virkninger på virksomhedens drift.

Stk. 2. En operatør af finansiel digital infrastruktur skal have et program for test af digital operationel modstandsdygtighed, som er integreret med operatørens ramme for it- og cyberrisikostyring og passende i forhold til de identificerede risici.

Stk. 3. En operatør af finansiel digital infrastruktur kan pålægges at gennemgå trusselsbaserede penetrationstest i overensstemmelse med de regler, der gælder for virksomheder omfattet af kapitel IV i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og retsakter udstedt i medfør heraf. Vurderingen af, i hvilket omfang en

operatør af finansiel digital infrastruktur skal gennemføre disse penetrationstests, skal foretages ud fra

1) virkningsrelaterede faktorer, navnlig i hvilket omfang de tjenester, der leveres, og de aktiviteter, der udføres af operatøren, indvirker på den finansielle sektor,
2) eventuelle betænkeligheder vedrørende finansiel stabilitet, herunder operatørens systemiske karakter, og
3) operatørens specifikke it-risikoprofil, grad af it-modenhed eller de teknologiske kendetegn, der er involveret.

Tredjepartsrisici

§ 333 h. En operatør af finansiel digital infrastruktur skal styre sine it- og cyberrisici, der er relateret til brug af it-tjenester fra tredjeparter som en integreret del af sin ramme for it- og cyberrisikostyring.

Stk. 2. En operatør af finansiel digital infrastruktur, der har overladt driften af en forretningsfunktion til en leverandør, har til enhver tid det fulde ansvar for at overholde og opfylde alle forpligtelser i henhold til denne lov.

Stk. 3. En operatør af finansiel digital infrastruktur skal regelmæssigt gennemgå de risici, der er forbundet med brugen af it-tredjepartsudbydere.

Stk. 4. En operatør af finansiel digital infrastruktur skal vedtage og regelmæssigt gennemgå en strategi for sine it-tredjepartsrisici. Strategien for it-tredjepartsrisici skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere.

Stk. 5. En operatør af finansiel digital infrastruktur skal opretholde og ajourføre et register over oplysninger om alle ordninger for brugen af it-tjenester, der leveres af tredjepartsudbydere. Operatøren skal underrette Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Stk. 6. Inden en operatør af finansiel digital infrastruktur indgår en kontraktlig ordning for brugen af it-tjenester, skal operatøren

1) vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion,
2) vurdere om de tilsynsmæssige betingelser for udlicitering er opfyldt,

3) identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen,
4) foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under udvælgelses- og vurderingsprocessen sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet og
5) identificere og vurdere interessekonflikter, som den kontraktlige ordning kan give anledning til.

Stk. 7. Når en operatør af finansiel digital infrastruktur indgår it-kontrakter, der relaterer sig til kritiske og vigtige funktioner, skal operatøren sikre, at den har passende adgangs-, inspektions- og revisionsrettigheder over for tredjepartsudbyderen af it-tjenester. Operatøren skal, på grundlag af en risikobaseret tilgang, fastsætte hyppigheden af revisioner og inspektioner samt de områder, der skal underkastes revision.

Stk. 8. En operatør af finansiel digital infrastruktur skal sikre, at de kontraktlige ordninger for brugen af it-tjenester som minimum kan opsiges i enhver af følgende situationer:

1) Tredjepartsudbyderen begår en væsentlig overtrædelse af gældende lovgivning eller kontraktvilkår.
2) Operatøren identificerer forhold under overvågningen af it-tredjepartsrisici, som kan ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester.
3) Operatøren dokumenterer svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring.
4) Finanstilsynet ikke længere kan føre effektivt tilsyn med operatøren som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Stk. 9. En operatør af finansiel digital infrastruktur skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner. Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, herunder

1) mulige svigt fra tredjepartsudbyderens side,
2) en forringelse af kvaliteten af de leverede it-tjenester,
3) eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester,
4) eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester, eller

5) opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i stk. 8 anførte situationer.

Stk. 10. En operatør af finansiel digital infrastruktur skal sikre, at den kan opsige kontraktlige ordninger, uden
1) at dens forretningsaktiviteter afbrydes,
2) at efterlevelsen af de lovgivningsmæssige krav begrænses, og
3) at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade.

Stk. 11. Exitstrategierne skal være dokumenterede, proportionale, testet i tilstrækkeligt omfang og gennemgået regelmæssigt.

Stk. 12. En operatør af finansiel digital infrastruktur skal identificere alternative løsninger og udarbejde overgangsplaner, så den kan fratage tredjepartsudbyderen af it-tjenester de relevante it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller indarbejde dem internt.

Stk. 13. En operatør af finansiel digital infrastruktur skal indføre passende beredskabsforanstaltninger for at opretholde driftsstabiliteten i tilfælde af, at de omstændigheder, der er nævnt i stk. 9, nr. 1-5, indtræder.

Risikovurdering ved indgåelse af kontrakter

§ 333 i. Når en operatør af finansiel digital infrastruktur foretager identifikation og vurdering af de risici, der er nævnt i § 333 h, stk. 6, nr. 3, skal operatøren tage hensyn til, hvorvidt den påtænkte indgåelse af en kontraktlig ordning, der understøtter kritiske eller vigtige funktioner for de tilsluttede virksomheder, vil føre til

1) henlæggelse af funktioner til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, eller

2) indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne.

Centrale kontraktsbestemmelser

§ 333 j. Rettigheder og forpligtelser for en operatør af finansiel digital infrastruktur og for tredjepartsudbyderen af it-tjenester skal fordeles klart og fastlægges skriftligt. Den samlede kontrakt skal omfatte

serviceniveauaftaler og dokumenteres i et samlet dokument, som parterne skal have adgang til i et varigt og tilgængeligt format.

Stk. 2. De kontraktlige ordninger for brugen af it-tjenester skal mindst omfatte følgende elementer:
1) En klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen skal levere, med angivelse af om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf, er tilladt, og hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise.
2) En angivelse af de steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og krav om, at tredjepartsudbyderen på forhånd skal underrette operatøren, hvis den har planer om at ændre disse steder.
3) Bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger.
4) Bestemmelser om sikring af adgang, genopretning og tilbagelevering af data i et tilgængeligt format i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen varetager, eller i tilfælde af opsigelse af kontrakten.
5) Beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf.
6) En forpligtelse for tredjepartsudbyderen til at yde bistand til operatøren uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en it-hændelse, der vedrører den it-tjeneste, som leveres til operatøren.
7) En forpligtelse for tredjepartsudbyderen til at samarbejde fuldt ud med Finanstilsynet og afviklingsmyndigheder, herunder personer, som myndighederne har udpeget.
8) Opsigelsesrettigheder og dertil knyttede minimumsfrister for opsigelse af de kontraktlige ordninger.

Stk. 3. De kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, skal ud over de elementer, der er oplistet i stk. 2, mindst omfatte følgende:
1) En fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, så operatøren kan foretage en effektiv overvågning af it-tjenester, og den uden unødigt ophold kan træffe passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes.
2) Opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for operatøren, herunder underretning om enhver

udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer.
3) Krav til tredjepartsudbyderen om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at operatøren kan levere sine tjenester.
4) En forpligtelse for tredjepartsudbyderen til at deltage i og fuldt ud samarbejde om operatørens trusselsbaserede penetrationstest som nævnt i § 333 g, stk. 3.
5) En ret til løbende at overvåge tredjepartsudbyderens opgavevaretagelse og risikostyring, herunder adgangs- og inspektions- og revisionsrettigheder for operatøren, Finanstilsynet eller udpegede tredjeparter og adgang til nødvendig information og dokumentation.
6) Exitstrategier, herunder indførelse af en obligatorisk passende overgangsperiode
a) i løbet af hvilken tredjepartsudbyderen fortsat leverer de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i operatøren eller sikre en effektiv afvikling eller omstrukturering heraf, og

b) som giver operatøren mulighed for at migrere til en anden tredjepartsudbyder, eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Informationsudveksling

§ 333 k. En operatør af finansiel digital infrastruktur kan udveksle oplysninger og efterretninger om cybertrusler i overensstemmelse med reglerne i kapitel VI, i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022, og indgå i ordninger oprettet i henhold forordningens artikel 45, stk. 2. En operatør af finansiel digital infrastruktur kan ligeledes udveksle relevante cybersikkerhedsoplysninger i overensstemmelse med reglerne i kapitel VI, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022, og indgå i ordninger oprettet i overensstemmelse hermed.

Stk. 2. En operatør af finansiel digital infrastruktur skal underrette Finanstilsynet om sin deltagelse i de ordninger, der er nævnt i stk. 1, og i tilfælde af udtrædelse af sådanne ordninger.

Oplysning til Finanstilsynet

§ 333 l. En operatør af finansiel digital infrastruktur skal oplyse Finanstilsynet følgende:

1) Operatørens navn.
2) Adressen på operatørens hovedforretningssted og dens andre retlige forretningssteder i Den Europæiske Union.
.
3) Den relevante sektor og delsektor og typen af enhed, som nævnt i bilag I, i direktiv (EU) 2022/2555 af 14. december 2022.
4) Ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre på operatøren.
5) De medlemsstater, hvor operatøren leverer tjenester.

Stk. 2. Ved ændring af oplysningerne i stk. 1 skal operatøren straks og senest tre måneder efter datoen for ændringen underrette Finanstilsynet herom.

Tilsyn m.v.

§ 333 m. Kapitel 21 og 23 og regler udstedt i medfør af disse kapitler finder anvendelse for operatører af finansielle digitale infrastrukturer med de nødvendige tilpasninger.

§ 333 n. Finanstilsynet har udover de beføjelser, der følger af kapitel 21, beføjelse til at:

1) Pålægge en operatør af finansiel digital infrastruktur regelmæssige og målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed og at afholde udgifterne hertil.
2) Pålægge en operatør af finansiel digital infrastruktur ad hoc-audits, herunder hvor det er berettiget på grund af en væsentlig hændelse eller en overtrædelse af reglerne i denne lov fra den finansielle digitale infrastrukturs side.
3) Pålægge en operatør af finansiel digital infrastruktur sikkerhedsscanninger baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte finansielle digitale infrastruktur.
4) Udstede advarsler om en operatør af finansiel digital infrastrukturs overtrædelse af denne lov.
5) Udpege en person med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med en operatør af finansiel digital infrastrukturs overholdelse af §§ 333 a og 333 f.

§ 333 o. Efterkommer en operatør af finansiel digital infrastruktur ikke Finanstilsynets påbud i medfør af denne lov, og efterkommer operatøren

ikke påbuddet inden en fornyet frist, som Finanstilsynet efterfølgende sætter, kan Finanstilsynet træffe afgørelse om:
1) Midlertidigt at suspendere en myndighedsudstedt certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, operatøren leverer, eller aktiviteter, der udføres af operatøren.
2) Midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller juridisk repræsentant i operatøren at udøve ledelsesfunktioner i denne.

Stk. 2. Midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil operatøren af finansiel digital infrastruktur træffer de nødvendige foranstaltninger til at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne i medfør af stk. 1, blev anvendt.

Stk. 3. En afgørelse efter stk. 1 kan af operatøren af finansiel digital infrastruktur eller den fysiske person, afgørelsen vedrører, forlanges indbragt for domstolene.

Bemyndigelse

§ 333 p. Finanstilsynet kan fastsætte nærmere regler om it- og cyberrisikostyring og kontrol- og sikringsforanstaltninger i en operatør af finansiel digital infrastruktur, herunder om:

1) Indholdet af rammerne for styring af it- og cyberrisici og om indholdet af strategier og politikker på området for digital operationel modstandsdygtighed.
2) Ledelsesorganets opgaver i forbindelse med styringen af it- og cyberrisici.
3) Operatører af finansielle digitale infrastrukturers rapportering af væsentlige hændelser og cybertrusler.
4) Test, herunder eksterne test, af en operatør af finansielle digitale infrastrukturers cybersikkerhed.
5) Krav til testere af en operatør af finansielle digitale infrastrukturers cybersikkerhed.
6) Styring og rapportering af tredjepartsrisici.
7) Obligatorisk brug af særlige sikkerhedscertificerede produkter eller tjenesteydelser.
8) Den interne og eksterne systemrevision i operatører af finansielle digitale infrastrukturer.«

25. *Afsnit X c* ophæves.

26. I *§ 344, stk. 1, 1. pkt.,* indsættes efter »bæredygtige investeringer«: », Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf, Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf«.

27. Efter *§ 344 d* indsættes:

»§ 344 e. Erhvervsministeren kan fastsætte regler, der udpeger en myndighed til at varetage TLPT-relaterede anliggender i henhold til artikel 26, stk. 9, i DORA. Det omfatter også varetagelse af TLPT-relaterede anliggender i forhold til operatører af finansielle digitale infrastrukturer, jf. § 333.«

28. I *§ 348, stk. 2,* ændres »§§ 43 og 57« til: »§ 43«.

29. I *§ 351, stk. 8,* ændres »stk. 5, 3. pkt.« til: »stk. 5, 5. pkt.«

30. I *§ 354, stk. 6,* indsættes som *nr. 50:*

»50) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, under forudsætning af, at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

31. To steder i *§ 354 e, stk. 2, 1. pkt.,* og to steder i *§ 373, stk. 1* og *9,* ændres »§ 125 b, stk. 1-4 og 6« til: »§ 125 b, stk. 3-5 og 8«.

32. I *§ 354 e, stk. 2, 2. pkt.,* indsættes efter »finansielle instrumenter«: »og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

33. *§ 354 h* ophæves.

34. I *§ 355, stk. 1,* indsættes efter »finansielle tjenesteydelser og regler udstedt i medfør heraf«: », Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf«.

35. *§ 361, stk. 1, nr. 4,* affattes således:

» 4) En operatør af finansiel digital infrastruktur betaler 119.000 kr. Har en operatør af finansiel digital infrastruktur i et regnskabsår gennemsnitligt færre end 25 fuldtidsansatte, betaler operatøren af finansiel digital infrastruktur dog 2.200 kr. 1. og 2. pkt. finder ikke anvendelse på en it-operatør af et detailbetalingssystem, der er udpeget som operatør af finansiel digital infrastruktur.«

36. I *§ 361, stk. 1,* indsættes som *nr. 11* og *12:*

»11) En udsteder af aktivbaserede tokens, der er meddelt tilladelse af Finanstilsynet i henhold til artikel 21 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, betaler årligt Finanstilsynet følgende:

a) 35.000 kr., når summen af udstederens gennemsnitlige udestående aktivbaserede tokens i 2. halvår af det foregående kalenderår og 1. halvår af det indeværende kalenderår er mindre end 100 mio. kr.

b) 100.000 kr., når summen af udstederens gennemsnitlige udestående aktivbaserede tokens i 2. halvår af det foregående kalenderår og 1. halvår af det indeværende kalenderår er mellem 100 mio. kr. og 1 mia. kr.

c) 600.000 kr., når summen af udstederens gennemsnitlige udestående aktivbaserede tokens i 2. halvår af det foregående kalenderår og 1. halvår af det indeværende kalenderår er større end 1 mia. kr.

12) En udbyder af kryptoaktivtjenester, der er meddelt tilladelse af Finanstilsynet i henhold til artikel 63 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, betaler årligt et grundbeløb til Finanstilsynet på 12,5 promille af deres omkostninger til løn, provision og tantieme, dog minimum 20.000 kr.«

37. I *§ 361, stk. 6, nr. 1,* udgår »og 22-26«.

38. I *§ 361, stk. 7,* indsættes som nyt *nr. 4:*

»4) Forvaltere af alternative investeringsfonde med registreret hjemsted i et tredjeland, som i henhold til § 130 i lov om forvaltere af alternative investeringsfonde m.v. har tilladelse til markedsføring i Danmark af andele i en alternativ investeringsfond fra et andet land inden for Den Europæiske Union eller et land, som Unionen har indgået aftale med på

det finansielle område, betaler et årligt grundbeløb til Finanstilsynet på 8.000 kr.«

Nr. 4 og 5 bliver herefter nr. 5 og 6.

39. I *§ 361, stk. 12,* ændres »grundbeløb, jf. stk. 1-11,« til: »faste beløb i dette kapitel«.

40. I *§ 368, stk. 1,* indsættes som *4. pkt.:*
»For så vidt angår udstedere af aktivbaserede tokens, foregår beregningen på grundlag af den senest indsendte indberetning efter § 332 f, og for så vidt angår udbydere af kryptoaktivtjenester, foregår beregningen på grundlag af den senest indsendte indberetning efter § 332 g.«

41. I *§ 372, stk. 1,* ændres »erhvervslivet og regler udstedt i medfør heraf og« til: »erhvervslivet og regler udstedt i medfør heraf,«, og efter » investeringer og regler udstedt i medfør heraf,« indsættes: » Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver samt regler udstedt i medfør heraf,«.

42. I *§ 372 a, stk. 1,* ændres » standardiseret securitisering og« til: »«securitisering,«, og efter: » (PEPP-produkt)« indsættes: » Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

43. I *§ 373, stk. 1,* indsættes efter: »for erhvervslivet«: »samt artikel 14, stk. 3, artikel 16, stk. 1, artikel 23, stk. 1 og 4, artikel 36, stk. 1-3 og 5-7, artikel 38, stk. 1 og 3, artikel 39, stk. 2, artikel 40, stk. 1 og 2, artikel 48, stk. 1, artikel 49, stk. 4, artikel 50, stk. 1 og 2, artikel 54, artikel 59, stk. 1, artikel 60, stk. 1-6, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, og artikel 76, stk. 1, 2 og 5-8, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

44. I *§ 373, stk. 2, 1. pkt.,* udgår »§ 71 c, stk. 1, 2. pkt.,«, efter »312 b« indsættes: »§ 333 a, stk. 1-3, § 333 b, stk. 1-6, § 333 d, stk. 1-4, § 333 e, stk. 1-12, § 333 f, stk. 1-8, § 333 g, stk. 1-3, § 333 h, stk. 1-13, § 333 i, stk. 1 og 2, § 333 j, stk. 1-3,«, og »samt artikel 4« ændres til: », artikel

4«, og efter »om europæiske crowdfundingtjenesteudbydere for erhvervslivet« indsættes: », artikel 4, stk. 1, stk. 3, 3. pkt., og stk. 6, artikel 5, stk. 2 og 3, artikel 6, stk. 1-10, artikel 7, stk. 1 og 2, artikel 8, stk. 1-2 og 4-6, artikel 9, artikel 10, artikel 12, stk. 1-4 og 6-9, artikel 13, stk. 2 og 3, artikel 14, artikel 16, stk. 1, 2. afsnit, artikel 17, stk. 1 og 2, artikel 19, stk. 1-9, artikel 22, stk. 1 og 3, artikel 25, stk. 1, 2 og 4, artikel 27, artikel 28, artikel 29, stk. 1-3 og 6, artikel 30, artikel 31, stk. 1-4, artikel 32, stk. 1-4, artikel 33, artikel 34, stk. 1-12, artikel 35, stk. 1, artikel 36, stk. 8-12, artikel 37, stk. 1 og 2, artikel 39, stk. 1, 2. pkt., artikel 41, stk. 1 og 2, artikel 46, stk. 1 og 2, artikel 47, stk. 1-3, artikel 48, stk. 6 og 7, artikel 49, stk. 5, artikel 51, stk. 1-9, 11-13 og stk. 14, 1. pkt., artikel 53 stk. 1-3, 5 og 6, artikel 55, artikel 59, stk. 2, 5 og 8, artikel 64, stk. 8, artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 67, stk. 1, 5 og 6, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9, artikel 76, stk. 3, 4 og 9-15, artikel 77, artikel 78, artikel 79, artikel 80, stk. 1-3, artikel 81, stk. 1-14, artikel 82, stk. 1, artikel 83, stk. 1 og 2, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver samt artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

45. I *§ 373, stk. 9,* indsættes som *2. pkt.:* »Forældelsesfristen er ligeledes 10 år for overtrædelse af artikel 16, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

46. *Bilag 1, nr. 13,* affattes således:
»Udstedelse af elektroniske penge, herunder elektroniske pengetokens, som defineret i artikel 3, stk. 1, nr. 7, i Europa-Parlamentets og Rådets (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

47. I *bilag 1* indsættes som *nr. 14* og *15:*

»14) Udstedelse af aktivbaserede tokens som defineret i artikel 3, stk. 1, nr. 6, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

15) Udbud af kryptoaktivtjenester som defineret i artikel 3, stk. 1, nr. 16, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

48. I *bilag 2* indsættes som *nr. 11-13:*

»11) Udstedelse af elektroniske penge, herunder elektroniske pengetokens som defineret i artikel 3, stk. 1, nr. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.
12) Udstedelse af aktivbaserede tokens som defineret i artikel 3, stk. 1, nr. 6, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.
13) Udbud af kryptoaktivtjenester som defineret i artikel 3, stk. 1, nr. 16, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

§ 2

I lov om betalinger, jf. lovbekendtgørelse nr. 53 af 18. januar 2023, foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »og dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019 om ændring af direktiv 2013/36/EU, for så vidt angår fritagne enheder, finansielle holdingselskaber, blandede finansielle holdingselskaber, aflønning, tilsynsforanstaltninger og -beføjelser og kapitalbevaringsforanstaltninger, EU-Tidende 2019, nr. L 150, side 253 (CRD V)« til: », dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019 om ændring af direktiv 2013/36/EU, for så vidt angår fritagne enheder, finansielle holdingselskaber, blandede finansielle holdingselskaber, aflønning, tilsynsforanstaltninger og -beføjelser og kapitalbevaringsforanstaltninger, EU-Tidende 2019, nr. L 150, side 253 (CRD V) og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

2. *§ 5, stk. 1, nr. 10,* affattes således:

»10) Tjenester leveret af en udbyder af tekniske tjenester, der understøtter udbuddet af betalingstjenester, når udbyderen ikke på noget tidspunkt er i besiddelse af de midler, som skal overføres, og der ikke er tale om tjenester omfattet af bilag 1, nr. 7 og 8, jf. dog § 122.«

3. I *§ 11, stk. 1, nr. 11,* indsættes efter »procedurer«: »samt ordninger for brug af it-tjenester i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

4. I *§ 11, stk. 1, nr. 12,* ændres: »§ 127« til: »kapitel III i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

5. *§ 11, stk. 1, nr. 15,* affattes således:

»15) Virksomhedens beredskabsplan, herunder en klar beskrivelse af de kritiske funktioner, effektive politikker og planer for it-driftsstabilitet og planer for it-indsats- og genopretning og procedurer til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige og effektive i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

6. *§ 11, stk. 1, nr. 17, 2. pkt.,* affattes således:

»Beskrivelsen af foranstaltningerne skal indeholde oplysninger om, hvordan virksomheden sikrer et højt niveau af digital operationel modstandsdygtighed i overensstemmelse med kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, navnlig med hensyn til teknisk sikkerhed og databeskyttelse, herunder vedrørende de software- og it-systemer, der anvendes af ansøgeren eller de virksomheder, som ansøgeren outsourcer alle eller dele af sine aktiviteter til.«

7. I *§ 54, nr. 8, litra c,* ændres: »§§ 126 og 127« til: »§ 126 og kapitel III i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

8. I *§ 60, stk. 3, nr. 5,* indsættes efter »procedurer«: »samt ordninger for brug af it-tjenester i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

9. I *§ 60, stk. 3, nr. 6,* ændres: »§ 126« til: »kapitel III i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december

2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

10. *§ 60, stk. 3, nr. 8,* affattes således:

»8) Virksomhedens beredskabsplan, herunder en klar beskrivelse af de kritiske funktioner, effektive politikker og planer for it-driftsstabilitet og planer for it-indsats og genopretning og procedurer til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige og effektive i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

11. I *§ 126* indsættes efter stk. 1 som nyt stykke:

»*Stk. 2.* Stk. 1, nr. 1 og 2, berører ikke anvendelsen af kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«
Stk. 2-5 bliver herefter stk. 3-6.

12. *§ 127, stk. 1* og *2,* ophæves.

Stk. 3 og 4 bliver herefter stk. 1 og 2.

13. I *§ 127, stk. 4,* der bliver stk. 2, ændres »stk. 1-3« til: »stk. 1«.

14. I *§ 130, stk. 1, 2. pkt.,* ændres »og forordninger udstedt i medfør af Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked« til: », forordninger udstedt i medfør af Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf«.

15. I *§ 130, stk. 1,* indsættes som *3. pkt.:* »Finanstilsynet påser endvidere udstedere af e-pengetokens overholdelse af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf.«

16. I *§ 135, stk. 1, nr. 7,* indsættes efter: »af hvidvaskloven«: »eller Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

17. I *§ 136, stk. 6,* indsættes som *nr. 27:*

»27) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

18. I *§ 138, stk. 1, 8. pkt.,* ændres »og Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro« til: », Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf«.

19. I *§ 138, stk. 1,* indsættes efter 8. pkt. som nyt punktum:

»Reaktioner givet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf, skal offentliggøres på Finanstilsynets hjemmeside med angivelse af virksomhedens navn.«

20. I *§ 138, stk. 1, 9. pkt.,* der bliver 10. pkt., indsættes efter »1. pkt.«: »eller 9. pkt.«

21. I *§ 142, stk. 1,* indsættes efter »regler udstedt i medfør af denne lov«: », forordninger udstedt i medfør af Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked, artikel 3-4 i Europa-Parlamentets og Rådets forordning 924/2009/EF af 16. september 2009 om grænseoverskridende betalinger i Fællesskabet og om ophævelse af forordning (EF) nr. 2560/2001, Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro, Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning nr. 2023/1114 (EU) om markeder for kryptoaktiver og regler udstedt i medfør heraf«.

22. I *§ 143* indsættes efter »udstedt i medfør heraf, « til: »Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf,«.

23. I *§ 144, stk. 1,* indsættes som *3. pkt.:*

»Forbrugerombudsmanden fører også tilsyn med, at virksomheder overfor forbrugere overholder artikel 49, 53 og 55 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

24. I *§ 152, stk. 1,* indsættes efter »og § 60, stk. 1,«: » i denne lov og artikel 48, stk. 1, artikel 49, stk. 4, artikel 50, stk. 1 og 2, artikel 54, artikel 59, stk. 1, artikel 60, stk. 4, artikel 67, stk. 4, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver,«.

25. I *§ 152, stk. 2,* indsættes efter: »(SEPA-forordningen)« », artikel 46, stk. 1 og 2, artikel 47, stk. 1-3, artikel 48, stk. 6 og 7, artikel 49, stk. 5, artikel 51, stk. 1-9, 11-13 og stk. 14, 1. pkt., artikel 53, stk. 1-3, 5 og 6, artikel 55, artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9 og artikel 82, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«

§ 3

I lov om kapitalmarkeder, jf. lovbekendtgørelse nr. 41 af 13. januar 2023, som ændret ved § 6 i lov nr. 243 af 7. marts 2023 og § 5 i lov nr. 480 af 12. maj 2023, foretages følgende ændringer:

1. I *fodnoten* til lovens titel udgår »dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016, EU-Tidende 2016, nr. L 194, side 1,«, og »og dele af Europa-Parlamentets og Rådets direktiv 2019/879/EU af 20. maj 2019 (BRRD II), EU-Tidende 2019, nr. L 150, side 296« ændres til: »dele af Europa-Parlamentets og Rådets direktiv 2019/879/EU af 20. maj 2019 (BRRD II), EU-Tidende 2019, nr. L 150, side 296, og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

2. *§ 58 a* ophæves.

3. I *§ 60, stk. 1, nr. 7,* ændres: »eller pligter efter Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og regler fastsat i medfør heraf.« til: », pligter efter Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og regler fastsat i medfør heraf eller pligter efter Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler fastsat i medfør heraf.«

4. *§ 71, stk. 2, nr. 3,* affattes således:

»3) kunne styre it-risici i overensstemmelse med kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

5. I *§ 114* ændres »have systemer, procedure og ordninger, der sikrer« til: »etablere og opretholde operationel modstandsdygtighed i overensstemmelse med kravene i kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor for at sikre«.

6. I *§ 114, nr. 1,* ændres »fleksible« til: »modstandsdygtige«.

7. I *§ 114, nr. 5,* indsættes efter »driftsstabilitetsordninger,«: »herunder politikker og planer for it-driftsstabilitet og planer for it-indsats og genopretning udarbejdet i overensstemmelse med artikel 11 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december

2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

8. I *§ 118, stk. 2, nr. 1,* indsættes efter »afprøvning af algoritmer«: »i overensstemmelse med kravene til it-risikostyring af informations- og kommunikationsteknologi og til test af digital operationel modstandsdygtighed i kapitel II og IV i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

9. *§ 129, stk. 2,* affattes således:

»*Stk. 2.* Følgende positioner skal ikke medregnes i opgørelsen af en persons nettoposition som nævnt i stk. 1:

1) Positioner, der besiddes af eller på vegne af en ikkefinansiel enhed, og som objektivt kan måles til at reducere de risici, der er direkte knyttet til den ikkefinansielle enheds forretningsmæssige aktivitet.
2) Positioner, der besiddes af eller på vegne af en finansiel enhed, der indgår i en overvejende kommerciel koncern, såfremt den finansielle enhed handler på vegne af en ikkefinansiel enhed i koncernen, og positionerne objektivt kan måles til at reducere de risici, der er direkte knyttet til den pågældende ikkefinansielle enheds forretningsmæssige aktivitet.
3) Positioner, der besiddes af finansielle og ikkefinansielle modparter med hensyn til positioner, som objektivt kan måles til at hidrøre fra transaktioner, der er indgået for at opfylde en forpligtelse til at tilføre en markedsplads likviditet.
4) Værdipapirer som nævnt i § 4, stk. 1, nr. 1, litra c, der vedrører en råvare eller et underliggende aktiv som nævnt i § 4, stk. 1, nr. 10.«

10. *§ 130, stk. 1, nr. 5,* affattes således:
»5) kræve, at en person midlertidigt tilbagefører likviditet til markedspladsen til en aftalt pris og i en aftalt mængde med det udtrykkelige formål at afbøde virkningen af en stor og dominerende position.«

11. I *§ 135, nr. 1, litra a,* ændres »til at håndtere perioder med spidsbelastning« til: »i overensstemmelse med kravene til it-risikostyring i kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

12. *I § 135, nr. 3,* indsættes efter »handelssystemer,«: »herunder planer for it-driftsstabilitet og planer for it-indsats og genopretning i

overensstemmelse med artikel 11 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

13. I *§ 135, nr. 4,* indsættes efter »kravene i nr. 1-3«: »og kravene til it-risikostyring og til test af digital operationel modstandsdygtighed i kapitel II og IV i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

14. I *§ 180 g, stk. 3,* indsættes efter »detailbetalingssystem«: », der ikke er udpeget som operatør af finansiel digital infrastruktur, jf. § 333, stk. 3,«.

15. I *§ 180 h* indsættes efter »detailbetalingssystem«: », der ikke er udpeget som operatør af finansiel digital infrastruktur, jf. § 333, stk. 3,«.

16. I *§ 211, stk. 2,* indsættes som *nr. 15* og *nr. 16:*

»15) Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf.

16) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

17. I *§ 226* indsættes som *nr. 17*:
»17) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, på betingelse af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

18. *§ 236 a* ophæves.

19. I *§ 248* udgår »artikel 27 f, stk. 1-3, artikel 27 g, stk. 1-5, og artikel 27 i, stk. 1-4, når en godkendt offentliggørelsesordning (APA) eller en godkendt indberetningsmekanisme (ARM) har en undtagelse i overensstemmelse med artikel 2, stk. 3,«.

20. I § 248 indsættes som *2. pkt.:* »Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes ligeledes med bøde overtrædelse af artikel 27 b, stk. 1 og 2, artikel 27 f, stk. 1-3, artikel 27 g, stk. 1-5, og

artikel 27 i, stk. 1-4, når en godkendt offentliggørelsesordning (APA) eller en godkendt indberetningsmekanisme (ARM) har en undtagelse i overensstemmelse med artikel 2, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter.«

21. Efter § 251 a indsættes:

»**§ 251 b.** Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde overtrædelse af artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9, artikel 76, stk. 3, 4 og 9-15, artikel 88, stk. 1-3, og artikel 92, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Stk. 2. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder overtrædelse af artikel 59, stk. 1, artikel 60, stk. 2 og 6, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, artikel 76, stk. 1, 2 og 5-8, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Stk. 3. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 1 år og 6 måneder overtrædelser af artikel 89, stk. 1 og 3, artikel 90, stk. 1, og artikel 91, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

§ 251 c. Medmindre højere straf er forskyldt efter den øvrige lovgivning straffes med bøde overtrædelse af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

§ 4

I lov nr. 1155 af 8. juni 2021 om fondsmæglerselskaber og investeringsservice og -aktiviteter, som ændret bl.a. ved § 13 i lov nr. 2382 af 14. december 2021, § 10 i lov nr. 568 af 10. maj 2022, § 3 i lov nr. 409 af 25. april 2023 og senest ved § 7 i lov nr. 480 af 12. maj 2023, foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »og dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019, EU-Tidende 2019, nr. L 150, side 253-293« til: », dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019, EU-Tidende 2019, nr. L 150, side 253-293 og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

2. I *§ 13, stk. 2,* ændres »§§ 15 og 16« til: »§ 13, stk. 6, §§ 15 og 16«.

3. I *§ 13* indsættes som *stk. 6:*

»*Stk. 6.* Et fondsmæglerselskab kan levere tjenester med kryptoaktiver som angivet i artikel 60, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, svarende til de tjenester, som det specifikt er meddelt tilladelse til i henhold til denne lov, hvis selskabet giver Finanstilsynet meddelelse herom mindst 40 arbejdsdage inden disse tjenester leveres første gang. Meddelelsen skal ledsages af de oplysninger, der er anført i artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

4. *§ 95, stk. 1,* affattes således:

»Et fondsmæglerselskab skal inden for rimelighedens grænser, træffe de foranstaltninger, som er nødvendige for at sikre kontinuitet og regelmæssighed i ydelsen af investeringsservice og udførelsen af investeringsaktiviteter. Fondsmæglerselskabet skal med henblik herpå anvende hensigtsmæssige og forholdsmæssigt afpassede systemer, herunder it-systemer, som oprettes og styres i overensstemmelse med artikel 7 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, samt hensigtsmæssige og forholdsmæssigt afpassede ressourcer og procedurer«.

5. I *§ 164, stk. 1, nr. 1,* indsættes som *litra f:*

»f) Europa-Parlamentets og Rådets (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

6. I *§ 214, stk. 1,* indsættes som *stk. 8* og *9:*

»*Stk. 8.* Kapitalejere og kreditorer, hvis krav er blevet nedskrevet eller konverteret i henhold til stk. 1, må ikke lide større tab end ved konkursbehandling af fondsmæglerselskabet.

Stk. 9. Finanstilsynets vurdering efter stk. 8 foretages på baggrund af værdiansættelsen i § 8 i lov om restrukturering og afvikling af visse finansielle virksomheder. Værdiansættelsen foretages af Finansiel Stabilitet efter anmodning fra Finanstilsynet. Konstateres det, at en kapitalejer eller kreditor, herunder Garantiformuen, har lidt større tab, end den ville have gjort ved konkursbehandling af fondsmæglerselskabet, betales forskellen af Afviklingsformuen.«

7. I *§ 214* indsættes som *stk. 8* og *9:*

Stk. 9. Finanstilsynets vurdering efter stk. 8 foretages på baggrund af værdiansættelsen i § 8 i lov om restrukturering og afvikling af visse finansielle virksomheder. Værdiansættelsen foretages af Finansiel Stabilitet efter anmodning fra Finanstilsynet. Konstateres det, at en kapitalejer eller kreditor, herunder Garantiformuen, har lidt større tab, end den ville have gjort ved konkursbehandling af fondsmæglerselskabet, betales forskellen af Afviklingsformuen.«

8. *§ 216, stk. 3,* affattes således:

»Stk. 3. Stk. 1 finder ikke anvendelse, hvis
1) forpligtelsen er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder, eller
2) forpligtelsen er en del af et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, jf. § 2, nr. 19, i lov om restrukturering og afvikling af visse finansielle virksomheder, og overstiger beløbsgrænsen for dækkede indskud, jf. § 9 i lov om en indskyder- og investorgarantiordning, eller
3) forpligtelsen ville være et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, hvis ikke det var foretaget gennem filialer af institutter, der er etableret inden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område, når filialen er beliggende uden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område.«

9. I *§ 217, stk. 1,* indsættes efter »konkurslovens § 97«: », med undtagelse af usikrede obligationer og andre former for omsættelig gæld og instrumenter, er skaber eller anerkender en gæld«.

10. I *§ 219, stk. 2,* indsættes som *nr. 12* og *13:*

»12) Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf.

13) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

11. I *§ 257, stk. 1,* indsættes som nyt *nr. 14:*

»14) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

12. I *§ 259, stk. 1,* ændres »tjenesteydelser og« til: »tjenesteydelser,«, og efter »bæredygtige investeringer« indsættes: » og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

13. I *§ 266, stk. 1,* indsættes som *nr. 5:*

»5) Artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9, artikel 76, stk. 3, 4 og 9-15, artikel 77, artikel 78, artikel 79, artikel 80, stk. 1-3, artikel 81, stk. 1-14, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

14. I *§ 266, stk. 2,* indsættes som *nr. 4* og *5:*

»4) Artikel 59, stk. 1, artikel 60, stk. 3, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, artikel 76, stk. 1, 2 og 5-8, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

5) Artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets

forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

15. I *§ 275, stk. 1,* indsættes som *nr. 8* og *9:*

»8) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.

9) Europa-Parlamentets og Rådets forordning EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

16. I *§ 276, stk. 1,* indsættes som *nr. 9* og *10:*

»9) Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

10) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

§ 5

I lov om forvaltere af alternative investeringsfonde m.v., jf. lovbekendtgørelse nr. 2015 af 1. november 2021, som ændret bl.a. ved § 2 i lov nr. 641 af 19. maj 2020, § 2 i lov nr. 2382 af 14. december 2021, § 9 i lov nr. 568 af 10. maj 2022, og senest ved § 6 i lov nr. 409 af 25. april 2023, foretages følgende ændringer:

1. I *fodnoten* til lovens titel ændres »og dele af Europa-Parlamentets og Rådets direktiv 2019/1160/EU af 20. juni 2019 om ændring af direktiv 2009/65/EF og 2011/61/EU for så vidt angår grænseoverskridende distribution af kollektive investeringsinstitutter, EU-Tidende 2019, nr. L 188, side 106« til: » dele af Europa-Parlamentets og Rådets direktiv 2019/1160/EU af 20. juni 2019 om ændring af direktiv 2009/65/EF og 2011/61/EU for så vidt angår grænseoverskridende distribution af kollektive investeringsinstitutter, EU-Tidende 2019, nr. L 188, side 106, og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

2. I *§ 8* indsættes som *stk. 6:*

»Stk. 6. En forvalter af alternative investeringsfonde kan levere tjenester med kryptoaktiver som angivet i artikel 60, stk. 5, i Europa-Parlamentets

og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, som det specifikt er meddelt tilladelse til i henhold til denne lov, hvis forvalteren giver Finanstilsynet meddelelse mindst 40 arbejdsdage inden disse tjenester leveres første gang. Meddelelsen skal ledsages af de oplysninger, der er anført i artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

3. I *§ 27, stk. 2, nr. 6,* indsættes efter »it-området«: », inklusiv for net- og informationssystemer, der oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

4. I *§ 155, stk. 1,* indsættes som *6. pkt.:*

»Finanstilsynet påser endvidere overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf samt Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf«.

5. I *§ 170, stk. 7,* indsættes som *nr. 29:*

»29) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

6. I *§ 171, stk. 1,* indsættes som *9-11. pkt.*:
»Reaktioner givet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor skal offentliggøres på Finanstilsynets hjemmeside med angivelse af forvalterens navn, jf. dog stk. 4. Indbringes reaktionen, der offentliggøres i henhold til 1. eller 8. pkt., for Erhvervsankenævnet eller domstolene, skal dette fremgå af Finanstilsynets offentliggørelse. Status og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.«

7. I *§ 189* ændres »tjenesteydelser eller« til: »tjenesteydelser, « og efter »bæredygtige investeringer « indsættes », Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver eller Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

8. I *§ 190, stk. 1,* indsættes efter »om europæiske sociale iværksætterfonde«: »og artikel 59, stk. 1, artikel 60, stk. 5, artikel 70, stk. 1-4, og artikel 72, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

9. I *§ 190, stk. 2,* indsættes efter »om pengemarkedsforeninger«: », artikel 64, stk. 8, artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, og artikel 81, stk. 1-14, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

§ 6

I lov om firmapensionskasser, jf. lovbekendtgørelse nr. 355 af 2. april 2020, som ændret bl.a. ved § 4 i lov nr. 409 af 25. april 2023, § 337 i lov nr. 718 af 13. juni 2023 og senest ved § 6 i lov nr. 480 af 12. maj 2023, foretages følgende ændringer:

1. I *§ 3* indsættes som *nr. 28* og *29:*

»28) Variable løndele: Aflønningsordninger, hvor den endelige aflønning ikke er kendt på forhånd, herunder bonusordninger, resultatkontrakter, engangsvederlag og andre lignende ordninger, der ikke er en del af den faste løndel.

29) Kønsneutral lønpolitik: En lønpolitik baseret på lige løn for samme arbejde eller arbejde af samme værdi uanset den ansattes køn.«

2. Efter § 43 d indsættes:

»**§ 43 e.** En firmapensionskasse skal vedtage en skriftlig lønpolitik, der fremmer en sund og effektiv risikostyring.
Stk. 2. Firmapensionskassens lønpolitik skal være kønsneutral.

§ 43 f. Firmapensionskassens øverste organ skal godkende firmapensionskassens lønpolitik, jf. § 43 e, herunder retningslinjer for tildeling af variabel løn og retningslinjer for fratrædelsesgodtgørelser, ved enhver væsentlig ændring og mindst hvert fjerde år. Firmapensionskassens lønpolitik skal hurtigst muligt efter godkendelsen offentliggøres på firmapensionskassens hjemmeside. Lønpolitikken skal forblive offentligt tilgængelig på hjemmesiden, så længe den er gældende.
Stk. 2. Formanden for bestyrelsen skal i sin beretning for firmapensionskassens øverste organ redegøre for aflønningen af firmapensionskassens bestyrelse og direktion. Redegørelsen skal indeholde oplysninger om aflønning i det foregående regnskabsår og om den forventede aflønning i indeværende og det kommende regnskabsår. Formanden for bestyrelsen skal forklare og begrunde lønpolitikkens indhold og dens efterlevelse i sin beretning for virksomhedens øverste organ.
Stk. 3. Firmapensionskassens øverste organ skal godkende aflønningen af firmapensionskassens bestyrelse for det igangværende regnskabsår.
Stk. 4. Bestyrelsen i en firmapensionskasse skal årligt udarbejde og offentliggøre en vederlagsrapport.
Stk. 5. Vederlagsrapporten skal indeholde:
1) Oplysninger om det samlede vederlag, som hvert medlem af bestyrelsen og direktionen som led i dette hverv har optjent fra firmapensionskassen og andre virksomheder inden for samme koncern i de seneste tre år, herunder oplysninger om fastholdelses- og fratrædelsesordningers væsentligste indhold.
2) En redegørelse for sammenhængen mellem ledelsens aflønning og firmapensionskassens strategi og relevante mål herfor.
Stk. 6. Hurtigst muligt efter generalforsamlingens afholdelse skal vederlagsrapporten offentliggøres på firmapensionskassens hjemmeside. Vederlagsrapporten skal forblive offentligt tilgængelig på hjemmesiden i en periode på 10 år. Vederlagsrapporten kan være tilgængelig i en længere periode end 10 år, forudsat at den ikke længere indeholder personoplysninger.

Outsourcing

§ 43 g. Ved en firmapensionskasses outsourcing af aktiviteter til en leverandør skal firmapensionskassen sikre, at aflønning af ledelsen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på

firmapensionskassens risikoprofil, hos leverandøren sker inden for rammerne af firmapensionskassens lønpolitik. Det skal fremgå af aftalen mellem firmapensionskassen og leverandøren, at firmapensionskassens lønpolitik skal overholdes.
Stk. 2. Stk. 1 finder ikke anvendelse, i det omfang leverandøren allerede er underlagt regler om aflønning i den finansielle regulering.

Aflønning i ledelsen og væsentlige risikotagere

§ 43 h. Ved firmapensionskassers aflønning af bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, skal firmapensionskassen sikre sig, at følgende er opfyldt:
1) De variable løndele til et medlem af bestyrelsen eller direktionen må på tidspunktet for beregningen af den variable løndel højst udgøre 50 pct. af henholdsvis honoraret og den faste grundløn inklusive pension.
2) De variable løndele til andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, må på tidspunktet for beregningen af den variable løn højst udgøre 100 pct. af den faste grundløn, inklusive pension.
3) Firmapensionskassens øverste organ kan dog beslutte, at de variable løndele til andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, jf. nr. 2, på tidspunktet for beregningen af den variable løndel kan udgøre op til 200 pct. af den faste grundløn, inklusive pension, forudsat af følgende krav opfyldes:
a) Firmapensionskassen skal senest ved indkaldelse til det øverste organs forsamling orientere det øverste organ om, at der ønskes stillingtagen til benyttelse af et højere maksimalt loft.
b) Det øverste organ skal tage beslutningen om benyttelse af et højere maksimalt loft på baggrund af en detaljeret anbefaling fra firmapensionskassen, der begrunder indstillingen herom, herunder antallet af berørte ansatte, disses arbejdsområder, det nye foreslåede maksimale loft og den forventede indvirkning på firmapensionskassens mulighed for at bevare et sundt kapitalgrundlag. Medlemmerne af det øverste organ skal modtage anbefalingen senest samtidig med indkaldelsen til det øverste organs forsamling.
c) Firmapensionskassen skal senest samtidig med formidling af anbefalingen til medlemmerne af det øverste organ, jf. litra b, informere Finanstilsynet om anbefalingen til det øverste organ, herunder det foreslåede højere maksimale loft og begrundelsen for indstillingen. Firmapensionskassen skal på anmodning fra Finanstilsynet godtgøre, at det foreslåede højere maksimale loft ikke er i strid med firmapensionskassens forpligtelser efter loven og bekendtgørelser

udstedt i medfør af § 43, stk. 2, herunder særligt kapitalgrundlagskravene.

d) Beslutningen om benyttelse af et højere maksimalt loft skal tiltrædes af firmapensionskassens øverste organ med mindst 66 pct. af de afgivne stemmer, forudsat at mindst 50 pct. af de stemmeberettigede medlemmer er repræsenteret på forsamlingen. Er mindre end 50 pct. af de stemmeberettigede medlemmer repræsenteret på forsamlingen, skal beslutningen tiltrædes af mindst 75 pct. af de afgivne stemmer. En ansat, som er medlem af det øverste organ i firmapensionskassen, må ikke deltage i afstemningen herom på det øverste organs forsamling, hvis den ansatte har en væsentlig interesse i beslutningen, der kan være stridende mod firmapensionskassens interesser.

e) Firmapensionskassen skal senest 8 dage efter det øverste organs forsamling informere Finanstilsynet om det øverste organs beslutning, herunder om størrelsen af et eventuelt besluttet højere maksimalt loft.

4) Mindst 50 pct. af en variabel løndel til bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, skal på tidspunktet for beregningen af den variable løn bestå af en balance af efterstillet gæld i firmapensionskassen eller andre instrumenter, som i en passende grad afspejler firmapensionskassens kreditværdighed som en firmapensionskasse, hvis aktivitet formodes at fortsætte. Instrumenterne kan udstedes i firmapensionskassen eller dennes modervirksomhed, der ejer firmapensionskassen fuldt ud.

5) Udbetaling af mindst 40 pct. af en variabel løndel, ved større beløb mindst 60 pct., sker over en periode på mindst fire år, med påbegyndelse ét år efter beregningstidspunktet, dog for bestyrelsen og direktionen mindst fem år. Udbetalingen skal ske med en ligelig fordeling over årene eller med en voksende andel i slutningen af perioden.

6) Firmapensionskassen kan undlade at udbetale en variabel løndel helt eller delvis, såfremt firmapensionskassen på tidspunktet for udbetaling af den variable løndel ikke overholder solvenskapitalkravet i § 54, eller hvis Finanstilsynet vurderer, at der er nærliggende risiko herfor.

7) Firmapensionskassen udbetaler ikke variabel løn til bestyrelsen eller direktionen, såfremt Finanstilsynet i medfør af § 83 kræver, at firmapensionskassen udarbejder en plan for genoprettelse af firmapensionskassens økonomiske stilling.

Stk. 2. For bestyrelsen og direktionen må aktieoptioner i modervirksomheden eller lignende instrumenter højst udgøre 12,5 pct. af henholdsvis honoraret og den faste grundløn inklusive pension på tidspunktet for beregningen heraf.

Stk. 3. En firmapensionskasse skal sikre, at efterstillet gæld, instrumenter m.v., der overdrages til bestyrelsen, direktionen eller andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens

risikoprofil, som en del af den variable løn, som er nævnt i stk. 1, nr. 4, ikke må afhændes af disse personer i en passende periode.

Stk. 4. En firmapensionskasse skal sikre, at udbetaling af den efter stk. 1, nr. 5, udskudte variable løndel til bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, er betinget af, at de kriterier, der har dannet grundlag for beregningen af den variable løndel, fortsat er opfyldt på udbetalingstidspunktet, betinget af, at den pågældende ikke har deltaget i eller været ansvarlig for en adfærd, der har resulteret i betydelige tab for virksomheden, eller ikke har efterlevet passende krav til hæderlighed, samt betinget af, at virksomhedens økonomiske situation ikke er væsentligt forringet i forhold til tidspunktet for beregningen af den variable løndel.

Stk. 5. En firmapensionskasse skal sikre, at bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, og som modtager variabel løn, skal tilbagebetale den variable løn helt eller delvis, hvis den variable løn er udbetalt på grundlag af oplysninger om resultater, som kan dokumenteres at være fejlagtige, og hvis modtageren er i ond tro.

Stk. 6. Tildeler en firmapensionskasse bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, en pensionsydelse, som udgør variabel løn, jf. § 3, nr. 28, skal firmapensionskassen, hvis modtageren forlader firmapensionskassen inden pensionstidspunktet, beholde denne pensionsydelse i form af instrumenter som nævnt i stk. 1, nr. 4, i fem år. Stk. 4 og 5 finder tilsvarende anvendelse på de i 1. pkt. nævnte tilfælde. Hvis modtageren er medlem af bestyrelsen eller ansat i firmapensionskassen ved pensionsalderen, skal firmapensionskassen udbetale den variable del af pensionsydelsen til modtageren i form af de i stk. 1, nr. 4, nævnte instrumenter uden mulighed for afhændelse eller udnyttelse i en periode på 5 år. Stk. 5 finder tilsvarende anvendelse på de i 3. pkt. nævnte tilfælde.

Stk. 7. For personer i ansættelsesforhold, der er omfattet af en kollektiv overenskomst, finder stk. 1-6 kun anvendelse på aftaler om variable løndele, hvis aftalerne om variabel løn ikke er fastsat i overenskomsten.«

3. I *§ 97, stk. 1, 2. pkt.*, ændres »tjenesteydelser og« til: »tjenesteydelser,«, og efter » bæredygtige investeringer« indsættes: » og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

4. I *§ 103, stk. 6,* indsættes som *nr. 30:*

»30) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

5. I *§ 104, stk. 1,* og *§ 112, stk. 1,* indsættes efter »bæredygtige investeringer«: », Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

6. I *§ 105, stk. 1,* indsættes efter 3. pkt. som nyt punktum:

»Reaktioner givet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og forordninger udstedt i medfør heraf, skal offentliggøres på Finanstilsynets hjemmeside med angivelse af firmapensionskassens navn, jf. dog stk. 4.«

7. I *§ 105, stk. 1, 4. pkt.,* der bliver 5. pkt., ændres »1. pkt.« til: »1. eller 4. pkt.«.

8. I *§ 105, stk. 1,* indsættes som *6. pkt.:*

»Indbringes reaktionen, der offentliggøres i henhold til 4. pkt., for Erhvervsankenævnet, skal dette fremgå af Finanstilsynets offentliggørelse, og det efterfølgende resultat af Erhvervsankenævnets afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.«

9. I *§ 117, stk. 2,* indsættes efter »§ 42, stk. 2, jf. stk. 1, nr. 3 og 4,«: »§§ 43 e, 43 f, § 43 g, stk. 1, § 43 h, stk. 1-6,«, og efter »§ 111, stk. 3, 5 og 6,« indsættes: »og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

§ 7

I lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven), jf. lovbekendtgørelse nr. 316 af 11. marts 2022, som ændret ved § 4 i lov nr. 507 af 20. maj 2022 og § 2 i lov nr. 480 af 12. maj 2023, foretages følgende ændringer:

1. *§ 1, stk. 1, nr. 22-26,* ophæves, og i stedet indsættes:

»22) udbydere af kryptoaktivtjenester som defineret i lov om finansiel virksomhed.«

2. *§ 2, nr. 4,* affattes således:

»4) Korrespondentforbindelse:
a) Levering af pengeinstitutydelser fra et pengeinstitut (korrespondenten) til et andet pengeinstitut (respondenten), herunder, men ikke begrænset til, oprettelse af løbende konto eller en anden passivkonto, samt tilknyttede ydelser som likviditetsstyring, internationale overførsler af midler, checkclearing, gennemstrømningskonti og valutatransaktioner.
b) En forbindelse mellem en virksomhed omfattet af § 1, stk. 1, nr. 1-12, 18 eller 22, (korrespondenten) og en virksomhed omfattet af § 1, stk. 1, nr. 1-12, 18 eller 22, (respondenten), herunder hvor der leveres lignende ydelser fra et korrespondentinstitut til et respondentinstitut, og herunder forbindelser indgået med henblik på værdipapirtransaktioner eller overførsler af midler eller forbindelser indgået med henblik på transaktioner med kryptoaktiver eller overførsler af kryptoaktiver.«

3. *§ 2, nr. 15* og *16,* ophæves.

Nr. 17-20 bliver herefter nr. 15-18.

4. I *§ 2* indsættes som *nr. 19:*

»19) Selvhostet adresse: En distributed ledger-adresse som defineret i Europa-Parlamentets og Rådets forordning 2023/1113/EU af 31. maj 2023 om oplysninger, der skal medsendes ved pengeoverførsler og ved overførsler af visse kryptoaktiver og om ændring af direktiv 2015/849/EU.«

5. I *§ 7, stk. 1, 1. pkt.,* indsættes efter »personer«: », der er«.

6. I *§ 7, stk. 2, 1. pkt., § 38, stk. 3* og *6, § 47, stk. 1, 1. pkt.,* og *stk. 3, § 49, stk. 1, 1. pkt., § 51, § 51 a, stk. 1, § 51 b, stk. 1, 1. pkt., §§ 52* og *53* og *§ 54, stk. 1,* udgår: »-26«.

7. I *§ 8, stk. 1, 1. pkt.,* indsættes efter »personer«: », der er«.

8. Et sted i *§ 10, nr. 2, litra c,* og tre steder i *§ 10, nr. 2, litra d,* ændres »virtuel valuta« til: »kryptoaktiver«.

9. Efter § 17 indsættes:

»§ 17 a. Erhvervsministeren kan fastsætte regler om gennemførelse af risikobegrænsende foranstaltninger ved overførsel af kryptoaktiver, der er rettet mod eller stammer fra en selvhostet adresse.«

10. I *§ 19* indsættes efter stk. 1 som nyt stykke:

»Stk. 2. Inden gennemførelse af kryptoaktivtjenester, skal korrespondenten fastslå, om respondenten er godkendt eller registreret i det pågældende land.«
Stk. 2 bliver herefter stk. 3.

11. I *§ 33, 1. pkt.,* ændres »udbydere af betalingstjenester og udstedere af elektroniske penge« til: »udbydere af betalingstjenester, udstedere af elektroniske penge og udbydere af kryptoaktivtjenester«.

12. I *§ 35, stk. 1, 1. pkt.,* og *§ 36, stk. 1, 1. pkt.,* ændres »og 21-26« til: », 21 og 22«.

13. *§ 48, stk. 2,* ophæves.

Stk. 3-7 bliver herefter stk. 2-6.

14. I *§ 48, stk. 3, 6* og *7,* udgår: »og 2«.

15. I *§ 48, stk. 5,* ændres »stk. 3 og 4« til: »stk. 2 og 3«.

16. I *§ 48, stk. 6,* ændres »stk. 3« til: »stk. 2« og »stk. 4« ændres til: »stk. 3«.

17. I *§ 54, stk. 2,* ændres: »1-13, 19 og 23-27« til: »1-12, 18 og 22«.

18. I *§ 78, stk. 1, 2. pkt.,* ændres »§ 48, stk. 1 og 2,« til: »§ 48, stk. 1,«.

19. I *§ 85* indsættes som *stk. 4:*

»Stk. 4. De dele af §§ 59 og 60, som i medfør af stk. 1 er sat i kraft for Grønland, kan ved kongelig anordning sættes helt eller delvis i kraft på

ny for Grønland med de ændringer, som de grønlandske forhold tilsiger.«

§ 8

I lov nr. 718 af 13. juni 2023 om forsikringsvirksomhed, foretages følgende ændringer:

1. I *§ 2, stk. 1,* ændres »139,« til: »138,«.

2. *Overskriften* før § 2 ophæves.

3. *§ 8* ophæves.

4. *§ 9, stk. 1, nr. 13,* ophæves.

Nr. 14-43 bliver herefter nr. 13-42.

5. I *§ 107, stk. 2,* ændres »balancesum på over 4 mia. kr.« til: »bruttopræmieindtægt på over 4. mia. kr.,«

6. I *§ 123, stk. 2,* udgår »Landbrugets FinansieringsBank A/S,«.

7. I *§ 193, stk. 13,* udgår »og om systemrevisionens gennemførelse i fælles datacentraler«.

8. I *§ 195, stk. 6,* udgår »§ 274, stk. 3,« og »§ 294, stk. 3,«.

9. I *§ 259, stk. 2,* indsættes efter nr. 7 som nyt nummer*:*

»8) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

Nr. 8 og 9 bliver herefter nr. 9 og 10.

10. I *§ 280, stk. 7, 1. pkt.,* ændres »stk. 2, 3 eller 5« til: »stk. 2 eller 3 eller stk. 4, 3. pkt.«

11. I *§ 289, stk. 1,* indsættes som *nr. 14:*

»14) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle

sektor, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

12. I *§ 302, stk. 1*, ændres »jf. dog stk. 2 og 3, og Europa-Parlamentets og Rådets forordning 2019/2088/EU af 27. november 2019 om bæredygtighedsrelaterede oplysninger i sektoren for finansielle tjenesteydelser og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning 2020/852/EU af 18. juni 2020 om fastlæggelse af en ramme til fremme af bæredygtige investeringer og regler udstedt i medfør heraf« til: », Europa-Parlamentets og Rådets forordning 2019/2088/EU af 27. november 2019 om bæredygtighedsrelaterede oplysninger i sektoren for finansielle tjenesteydelser og regler udstedt i medfør heraf, Europa-Parlamentets og Rådets forordning 2020/852/EU af 18. juni 2020 om fastlæggelse af en ramme til fremme af bæredygtige investeringer og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf, jf. dog stk. 2 og 3«.

13. I *§ 309, stk. 1,* indsættes som *nr. 9:*

»9) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

14. I *§ 310* indsættes som *nr. 9:*

»9) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

15. I *§ 312, stk. 1,* indsættes som *nr. 3:*

»3) Artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

16. I *§ 312, stk. 2, nr. 1,* indsættes efter »§ 105, stk. 5, jf. stk. 1, nr. 3 og 4,«: »§ 125,«.

17. I *§ 313, stk. 1,* ændre »§ 275, stk. 2« til: »§ 275«.

§ 9

I lov om forsikringsformidling, jf. lovbekendtgørelse nr. 337 af 11. marts 2022, som ændret ved § 10 i lov nr. 570 af 10. maj 2022, § 4 i lov nr. 480 af 12. maj 2023 og § 338 i lov nr. 718 af 13. juni 2023, foretages følgende ændringer:

1. I *§ 22, stk. 1, 2. pkt.,* ændres »og Europa-Parlamentets og Rådets forordning 2019/2088/EU af 27. november 2019 om bæredygtighedsrelaterede oplysninger i sektoren for finansielle tjenesteydelser« til: », Europa-Parlamentets og Rådets forordning 2019/2088/EU af 27. november 2019 om bæredygtighedsrelaterede oplysninger i sektoren for finansielle tjenesteydelser, Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

2. I *§ 31, stk. 6,* indsættes som *nr. 18:*

»18) Myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.«

3. I *§ 33, stk. 1,* indsættes som *8. pkt.:*

»Reaktioner givet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og forordninger udstedt i medfør heraf, skal offentliggøres på Finanstilsynets hjemmeside med angivelse af virksomhedens navn.«

4. I *§ 33, stk. 1, 8. pkt.,* der bliver 9. pkt., indsættes efter »af loven «: », Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf«.

5. I *§ 33, stk. 1, 9. pkt.,* der bliver 10. pkt., indsættes efter »1. pkt.«: »eller 8. pkt.«

6. I *§ 36, stk. 1,* indsættes efter »Europa-Parlamentets og Rådets forordning 2019/2088/EU af 27. november 2019 om bæredygtighedsrelaterede oplysninger i sektoren for finansielle tjenesteydelser«: », Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

7. I *§ 37* ændres »eller i henhold« til: »,«, og efter »tjenesteydelser« indsættes: », Europa-Parlamentets og Rådets forordning 2019/2088/EU af 27. november 2019 om bæredygtighedsrelaterede oplysninger i sektoren for finansielle tjenesteydelser eller i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

8. I *§ 42, stk. 2,* ændres »(PRIIP'er) og« til: »(PRIIP'er),«, og efter »(PEPP-Produkt)« indsættes: », og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

§ 10

I lov om en garantifond for skadesforsikringsselskaber, jf. lovbekendtgørelse nr. 2067 af 12. november 2021, som ændret ved § 1 i lov nr. 480 af 12. maj 2023 og ved § 339 i lov nr. 718 af 13. maj 2023, foretages følgende ændringer:

1. Efter § 12 indsættes:

»**§ 12 a.** Fondens bestyrelse skal, som en del af at antage fornøden medhjælp efter § 12, stk. 1, indgå aftale med et forsikringsselskab som administrationsselskab, jf. dog stk. 3.

Stk. 2. Fonden skal skriftligt orientere Finanstilsynet, når en aftale efter stk. 1 er indgået. Fonden skal ligeledes skriftligt orientere Finanstilsynet, hvis Fonden ikke kan indgå en aftale efter stk. 1.

Stk. 3. Kan Fondens bestyrelse ikke indgå aftale med et forsikringsselskab som administrationsselskab, skal Finanstilsynet udnævne et administrationsselskab for Fonden, der opfylder kriterierne fastsat i stk. 4, nr. 1-5, og i overensstemmelse med stk. 5 og 6.

Stk. 4. Finanstilsynet udnævner et forsikringsselskab efter stk. 3, jf. dog stk. 5 og 6, som administrationsselskab for Fonden, når forsikringsselskabet
1) har fået Finanstilsynets tilladelse til at drive forsikringsvirksomhed uden begrænsninger til forsikringsklasse 1-3, 6, 8-10, 12, 13, 16, 17 og 18 i bilag 1 i lov om forsikringsvirksomhed,
2) i henhold til seneste godkendte årsrapport har haft en årlig bruttopræmieindtægt på minimum 2. mia. kr.,
3) i de to seneste regnskabsår på balancetidspunktet i gennemsnit har haft 125 eller flere fuldtidsansatte,
4) overholder det for forsikringsselskabet fastsatte solvenskapitalkrav,
5) minimum har en markedsandel i Danmark på 3 pct. målt på bruttopræmie.

Stk. 5. Opfylder flere forsikringsselskaber kriterierne i stk. 4, skal Finanstilsynet udnævne et administrationsselskab for Fonden på baggrund af en rotationsordning. Finanstilsynet skal dog i sin afgørelse inddrage relevante forhold relateret til de omfattede forsikringsselskaber i sin vurdering af, hvilket forsikringsselskab, der skal udnævnes som administrationsselskab.

Stk. 6. Finanstilsynet kan, medmindre særlige forhold taler herfor, ikke udnævne et forsikringsselskab som administrationsselskab i to af hinanden efterfølgende perioder.

Stk. 7. Finanstilsynet skal udnævne et forsikringsselskab efter stk. 3, for en periode på 48 måneder, jf. dog stk. 8.

Stk. 8. Hvis der i løbet af de 48 måneder, hvor et forsikringsselskab er udnævnt af Finanstilsynet som administrationsselskab, opstår en konkurs i et forsikringsselskab, skal Fondens bestyrelse indgå aftale med et nyt forsikringsselskab som administrationsselskab, jf. stk. 1, jf. dog stk. 3. Det forsikringsselskab, der på tidspunktet for konkursens indtræden er udnævnt som administrationsselskab, skal bistå Fonden indtil sagsbehandlingen af konkursen er afsluttet, uanset om perioden på 48 måneder i mellemtiden måtte være ophørt.

Stk. 9. Indgår Fondens bestyrelse aftale efter stk. 1, med et forsikringsselskab om at varetage opgaven som administrationsselskab for Fonden efter udløb af en periode, jf. stk. 7, og indtræder der en konkurs i et forsikringsselskab inden den igangværende periode, jf. stk. 7, udløber, skal forsikringsselskabet, som Fondens bestyrelse har indgået aftale med, overtage opgaven som administrationsselskab på tidspunktet for konkursens indtræden.

Stk. 10. Fonden skal betale vederlag til et administrationsselskab udnævnt af Finanstilsynet. Vederlaget fastlægges efter vilkårene i Fondens udbudsmateriale eller andet dokument indeholdende Fondens specificering af opgaverne. Er det ikke muligt for parterne at blive enig om størrelsen på vederlaget, skal Finanstilsynet fastsætte vederlagets størrelse på baggrund af et oplæg fra Fonden.

Stk. 11. Det af Finanstilsynet udnævnte administrationsselskab, jf. stk. 3, skal varetage de opgaver, der fremgår af Fondens udbudsmateriale eller andet dokument indeholdende Fondens specificering af opgaverne.«

2. Efter § 17 a indsættes i *kapitel 10*:

»§ 17 b. Afgørelser truffet af Finanstilsynet i medfør af § 12 a, stk. 3 og 10, 3. pkt., kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt det pågældende forsikringsselskab.**«**

§ 11

I lov nr. 405 af 25. april 2023 om Kreditforeningen af kommuner og regioner i Danmark, foretages følgende ændringer:

1. I *§ 21, stk. 1,* indsættes som *2. pkt.:*
»Finanstilsynet påser endvidere overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

2. I *§ 22* indsættes som *stk. 2* og *3:*

»Stk. 2. § 354 e i lov om finansiel virksomhed finder tilsvarende anvendelse på foreningen for sager om overtrædelse af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.
Stk. 3. § 372 a i lov om finansiel virksomhed finder tilsvarende anvendelse på foreningen for regler, som er nødvendige for at anvende

eller gennemføre de afgørelser eller retsakter, som vedtages af Europa-Kommissionen i medfør af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

3. I *§ 25, stk. 2,* indsættes efter »§ 199, stk. 2 og 6, i lov om finansiel virksomhed,«: »og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

§ 12

I lov om et skibsfinansieringsinstitut, jf. lovbekendtgørelse nr. 646 af 18. maj 2022, foretages følgende ændringer:

1. I *§ 14, stk. 1, 1. pkt.,* indsættes efter »§ 3, 2. pkt.,«: »og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

§ 13

I lov om Danmarks Eksport- og Investeringsfond, jf. lov nr. 871 af 21. juni 2022, foretages følgende ændringer:

1. I *§15* indsættes efter stk. 1 som nyt stykke:
»Stk. 2. Europa-Parlamentets og Rådets forordning (EU) 2022/2254 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor finder ikke anvendelse for Danmarks Eksport- og Investeringsfond og dennes selvstændige offentlige dattervirksomheder og øvrige datterselskaber samt enheder forvaltet af Danmarks Eksport- og Investeringsfond eller Danmarks Eksport- og Investeringsfonds selvstændige offentlige dattervirksomheder, jf. artikel 2, stk. 4, i Europa-

Parlamentets og Rådets forordning (EU) 2022/2254 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«

Stk. 2 og 3 bliver herefter stk. 3 og 4.

§ 14

I straffeloven, jf. lovbekendtgørelse nr. 1360 af 28. september 2022, som ændret ved § 2 i lov nr. 409 af 25. april 2023, § 3 i lov nr. 486 af 13. maj 2023, § 3 i lov nr. 486 af 13. maj 2023, § 1 i lov nr. 741 af 13. juni 2023 og § 32 i lov nr. 753 af 13. juni 2023, foretages følgende ændring:

1. I *§ 299 d, stk. 1*, indsættes før nr. 1 som nyt nummer:

»1) overtrædelse af artikel 89, stk. 2, eller artikel 91, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver,«.
Nr. 1-3 bliver herefter nr. 2-4.

§ 15

Stk. 1. Loven træder i kraft den 1. juli 2024, jf. dog stk. 2-5.
Stk. 2. §§ 332 b, 332 c, 332 e, 332 f, 332 g og 332 h, som affattet ved denne lovs § 1, nr. 24, træder i kraft den 30. juli 2024.
Stk. 3. §§ 332, 332 a og 332 d i lov om finansiel virksomhed, som affattet ved denne lovs § 1, nr. 24, § 1, nr. 37, og § 7 træder i kraft den 30. december 2024.
Stk. 4. § 1, nr. 6, 23, afsnit IX c som affattet ved denne lovs § 1, nr. 24, § 1, nr. 33, og § 3, nr. 2 og 18, træder i kraft den 18. oktober 2024.
Stk. 5. § 1, nr. 5, 7 og 8, § 2, nr. 1 og 3-13, § 3, nr. 4-8 og 11-13, § 4, nr. 1 og 4, og § 5, nr. 1 og 3, træder i kraft den 17. januar 2025.
Stk. 6. Udbydere af kryptoaktivtjenester, der inden den 30. december 2024 udbyder kryptoaktivtjenester, kan fortsætte med at udbyde kryptoaktivtjenester her i landet uden en tilladelse efter den 30. december 2024 i op til 18 måneder eller indtil virksomheden er meddelt tilladelse eller afslag i henhold til § 332 b, stk. 1, såfremt virksomheden indsender en ansøgning efter § 332 b, stk. 1, til Finanstilsynet senest den 30. december 2024.
Stk. 7. § 43 h, stk. 1, nr. 5, i lov om firmapensionskasser som affattet ved denne lovs § 6, nr. 2, finder ikke anvendelse for variabel løn optjent for optjeningsperioder før lovens ikrafttræden. For variabel løn optjent i optjeningsperioder før lovens ikrafttræden finder de hidtil gældende regler anvendelse i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og

aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser.
Stk. 8. Regler fastsat i medfør af § 199, stk. 12, 2. pkt., i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 406 af 29. marts 2022, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 333 a, stk. 1, som affattet ved § 1, nr. 24.

§ 16

Stk. 1. Loven gælder ikke for Færøerne og Grønland, jf. dog stk. 2 og 3.

Stk. 2. Lovens §§ 1-10 og 12 kan ved kongelig anordning helt eller delvis sættes i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger.

Stk. 3. §§ 1-5, 7 og 12 kan ved kongelig anordning helt eller delvis sættes i kraft for Færøerne med de ændringer, som de færøske forhold tilsiger.

Bemærkninger til lovforslaget
Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Cyberangreb mod den finansielle sektor kan have alvorlige konsekvenser for Danmark. Længevarende it-nedbrud i sektoren kan true den finansielle stabilitet og tilliden til den finansielle sektor. Det er derfor afgørende, at hele den finansielle sektor har et stærkt og robust cybersikkerhedsniveau.

Med Europa-Parlamentets og Rådets forordning 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) og Europa-Parlamentets og Rådets direktiv 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen mv. (NIS 2-direktivet) sker der en nødvendig modernisering af reglerne for tilsyn med it- og cybersikkerhed i den finansielle sektor.

DORA-forordningen kommer til at gælde direkte for virksomheder på det finansielle område og erstatter en række nationale regler om kontrol- og sikringsforanstaltninger på it-området. DORA-forordningen fastsætter bl.a. krav om it-risikostyring, indberetning af større it-relaterede hændelser til myndighederne, test af cybertrusler, styring af it-tredjepartsrisici i virksomhederne og krav til kontrakter mellem virksomhederne og it-leverandører. Med lovforslaget foreslås det, at Finanstilsynet udpeges som kompetent myndighed til at påse virksomhedernes overholdelse af bestemmelserne i DORA-forordningen, og at der fastsættes hjemmel til at sanktionere overtrædelser af forordningen.

En række leverandører af it-tjenester på det finansielle område, omfattes ikke af DORA-forordningen. Det drejer sig primært om fælles datacentraler på det finansielle område og it-operatører af detailbetalingssystemer. Disse virksomheder omfattes af NIS 2-direktivet, der fastsætter krav til it-sikkerheden også for andre aktører på tværs af sektorer. Det foreslås derfor at implementere NIS 2-direktivets krav for disse virksomheder på det finansielle område.

For at sikre et ensartet og stærkt cybersikkerhedsniveau i hele den finansielle sektor og undgå svage led i den finansielle infrastruktur foreslås det herudover at fastsætte supplerende nationale regler for virksomheder, der udpeges som operatører af finansielle digitale infrastrukturer, hvilket vil omfatte de fælles datacentraler på det finansielle område og it-operatører af detailbetalingssystemer. Det foreslås, at disse regler afspejler relevante krav i DORA-forordningens, som gælder for de øvrige virksomheder på det finansielle område.

Med lovforslaget gennemføres dermed ændringer af den finansielle lovgivning, der er nødvendige for at sikre implementering af fælleseuropæisk regulering på cybersikkerhedsområdet.

Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) harmoniserer reguleringen af markedet for kryptoaktiver på tværs af medlemsstaterne i EU og understøtter innovation samt beskytter forbrugere, investorer og den finansielle stabilitet. Med lovforslaget udpeges Finanstilsynet som kompetent myndighed til at påse overholdelsen af MiCA og gives hjemmel til at opkræve afgifter fra de nye virksomheder, som kommer under tilsyn som følge af forordningen.

Lovforslaget indfører krav for firmapensionskasser om kønsneutral lønpolitik, og forlænger udskydelsesperioderne for udbetaling af variable løndele. Lovforslaget gennemfører også anbefalingerne om transparens på aflønningsområdet fra Komitéen for god Selskabsledelse i overensstemmelse med betænkning nr. 1575 om skærpet ansvarsvurdering for ledelsesmedlemmer m.v. i finansielle virksomheder for firmapensionskasserne.

Lovforslaget giver derudover Finanstilsynet mulighed for at udnævne et forsikringsselskab til at varetage opgaven som administrationsselskab for Garantifonden for skadesforsikringsselskaber i en periode af op til fire år, mod vederlag, dog maksimalt til administration af ét konkursramt forsikringsselskab. Lovforslaget sikrer, at garantifonden altid kan løfte den samfundsmæssigt væsentlige opgave, der består i bl.a. at foretage udbetalinger til forsikringstagere i tilfælde af deres forsikringsselskabs konkurs.

Lovforslaget indeholder ændringer til regler om kapitalgrundlag i lov om finansiel virksomhed, der præciserer, at det ikke-gearingsrelaterede søjle II-tillæg og vejledende kapitalniveau opgøres i forhold til de risikovægtede eksponeringer. Gearingsrelaterede søjle II-tillæg og vejledende kapitalniveau opgøres derimod i forhold til de uvægtede eksponeringer. Præciseringen har til formål at tydeliggøre gældende retspraksis. Lovforslaget indeholder også en ændring af opgørelse af et vejledende niveau af yderligere kapitalgrundlag (P2G) og en ændring, så det gearingsbaserede vejledende niveau af yderligere kapitalgrundlag (P2G-LR) kan opfyldes med kernekapital. Ændringen har til formål at bringe den danske tilgang til opgørelse af P2G samt den danske tilgang til opfyldelse af P2G-LR i overensstemmelse med den europæiske tilgang.

2. Lovforslagets hovedpunkter

2.1. Ændringer som følge af DORA-forordningen

2.1.1. Gældende ret

De gældende regler om it- og cybersikkerhed for virksomheder på det finansielle område findes i de virksomhedsspecifikke hovedlove, og er nærmere udmøntet i tilknyttede bekendtgørelser.

Banker, realkreditinstitutter, investeringsforvaltningsselskaber og fondsmæglerselskaber skal have betryggende kontrol- og sikringsforanstaltninger på it-området. Kravene hertil er nærmere udmøntet i bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.v. (ledelsesbekendtgørelsen), herunder særligt bekendtgørelsens bilag 5, der omhandler den it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik, som en virksomhed skal udarbejde.

På samme vis skal også forsikringsselskaber og firmapensionskasser have betryggende kontrol og sikringsforanstaltninger på it-området. Kravene hertil er nærmere udmøntet i bilag 4 i henholdsvis bekendtgørelse nr. 1723 af 16. december 2015 om ledelse og styring af forsikringsselskaber m.v. og bekendtgørelse nr. 7 af 4. januar 2019 om ledelse og styring af firmapensionskasser.

På kapitalmarkedsområdet er der fastsat krav til operatører af markedspladser, som den danske børs Nasdaq Copenhagen, der skal sikre, at markedspladsen drives på en betryggende og hensigtsmæssig måde. Kravene herom er nærmere udmøntet i lov om kapitalmarkeder. Derudover er der fast nærmere krav til markedspladserne i Kommissionens delegerede forordning (EU) 2017/584 af 14. juli 2016 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2014/65/EU for så vidt angår reguleringsmæssige tekniske standarder om præcisering af organisatoriske krav til markedspladser.

E-pengeinstitutter og betalingsinstitutter skal også have betryggende kontrol- og sikkerhedsforanstaltninger på it-området. Kravene hertil er nærmere udmøntet i lov om betalinger.

2.1.2. Erhvervsministeriets overvejelser og den foreslåede ordning

DORA-forordningen moderniserer og harmoniserer reglerne indenfor it- og cybersikkerhed på tværs af den finansielle sektor.

Den finansielle sektor er blevet væsentlig mere digitaliseret og cybertruslen mod sektoren er høj. En modernisering og harmonisering af reglerne om it-

og cybersikkerhed er derfor nødvendig, da en cyberhændelse kan forstyrre tilgængeligheden af finanssektorens ydelser og dermed udgøre en risiko for den finansielle stabilitet. Den fælles europæiske regulering på det finansielle område har ikke fulgt med denne udvikling. Den overordnede hensigt med DORA-forordningen er derfor at bidrage til at skabe en mere sikker og effektiv digital finansiel sektor i EU.

Forordningen fastsætter bl.a. regler, der skal styrke den operationelle modstandsdygtighed i virksomhedernes it-teknologi og hermed mindske risikoen for navnlig cyberangreb, begrænse skaden og prioritere genoptagelsen af aktiviteter i tilfælde af et cyberangreb. Forordningen finder anvendelse fra den 17. januar 2025.

Forordningen finder anvendelse på finansielle enheder. Ved finansielle enheder forstås penge- og realkreditinstitutter, betalingsinstitutter, e-pengeinstitutter, herunder betalings- eller e-pengeinstitutter med en begrænset tilladelse, udbydere af kontooplysningstjenester, fondsmæglerselskaber, forsikrings- og genforsikringsvirksomheder, større forsikringsformidlere og arbejdsmarkedspensionsselskaber, forvaltere af alternative investeringsfonde, udbydere af kryptoaktivtjenester, markedspladser, værdipapircentraler, centrale modparter (CCP), udbydere af dataindberetningstjenester, crowdfundingtjenesteudbydere, transaktionsregistre, administratorer af kritiske benchmarks, securitiseringsregistre og kreditvurderingsbureauer. For betalings- og e-pengeinstitutter med en begrænset tilladelse, arbejdsmarkedsrelateret pensionskasser, der forvalter pensionsordninger, som tilsammen har mindre end 100 medlemmer i alt og små og ikke indbyrdes forbundne fondsmæglerselskaber, gælder dog kun forenklede krav til it-risikostyring.

Forordningen indeholder regler om it-risikostyring, indberetning af større it-relaterede hændelser til myndighederne, test af cybersikkerhed, udveksling af oplysninger og efterretninger om cybertrusler og sårbarheder, styring af it-tredjepartsrisici i virksomhederne. Desuden indeholder forordningen regler om de kontrakter, der indgås mellem en it-leverandør og finansielle enheder, en ny ordning om overvågning af it-leverandører, som er kritiske for den finansielle sektor på EU-niveau.

Reglerne i forordningen erstatter de gældende regler på it-området i den finansielle sektor, samtidig med at den fastsætter en række nye og skærpede krav til de omfattede virksomheder. Det indebærer bl.a., at de regler i den danske regulering, der i dag regulerer de områder, som bliver omfattet af DORA-forordningen, skal ophæves. Det drejer sig særligt om den regulering, der i dag er udmøntet i it-bilagene til ledelsesbekendtgørelserne indenfor de forskellige virksomhedsområder i den finansielle sektor.

DORA-forordningen kommer til at gælde direkte i Danmark og skal derfor ikke implementeres i national lovgivning. Som følge af forordningen, er det dog nødvendigt at indføre regler i den danske lovgivning, der sikrer et effektivt tilsyn med overholdelsen af forordningen.

For at sikre et effektivt tilsyn med DORA-forordningen foreslås det, at Finanstilsynet udpeges som kompetent myndighed til at påse overholdelsen af forordningen. Finanstilsynet fører også i dag it-tilsynet med virksomhederne på det finansielle område og vil derfor kunne tilpasse og anvende den tilsynsramme, der allerede er etableret på området. Finanstilsynet har bl.a. mulighed for at indhente alle relevante oplysninger hos virksomhederne og deres underleverandører, samt at benytte de reaktionsmuligheder der allerede udgør et led i Finanstilsynets almindelige tilsynsudøvelse.

Udpegelsen af Finanstilsynet som kompetent myndighed for tilsynet med overholdelsen af DORA-forordningen nødvendiggør en række tilpasninger af tilsyns-, delegations- og klagebestemmelser i de finansielle hovedlove, hvor der er behov for at tilføje forordningen til oplistningerne i bestemmelserne.

Det foreslås derfor, at Finanstilsynet skal føre tilsyn med virksomhedernes overholdelse af DORA-forordningen på tværs af den finansielle regulering.

DORA-forordningen indeholder en række regler om TLPT-test. Et område, der ikke hidtil har været reguleret ved lov, men er blevet drevet af Danmarks Nationalbank i henhold til TIBER-DK. Det vurderes, at det er væsentligt, at der er mulighed for, at TLPT-opgaven kan forblive hos den myndighed, der i dag har ekspertisen og erfaringen med at løse den. Danmarks Nationalbank har opbygget erfaring med at vejlede de testede virksomheder i alle elementer af testprocessen.

Udpegelse af en anden myndighed end Finanstilsynet er ligeledes i overensstemmelse med forudsætningerne i præamblen til DORA-forordningen, der fastslår, at det vil være hensigtsmæssigt at gøre det muligt at udpege en anden offentlig myndighed, end den kompetente myndighed, til at varetage TLPT-opgaven for derigennem at kunne trække på den ekspertise, som visse kompetente myndigheder allerede har erhvervet med hensyn til gennemførelse af TIBER-EU-rammen.

Som i Danmark har det været praksis i de andre lande i EU, at TLPT-opgaven er placeret hos centralbanker. Dette har baggrund i centralbankernes operationelle fokus, der modsvarer tilgangen til TLPT,

hvor formålet er at skabe læring, både vedrørende styrker og svagheder i cyberforsvaret. Testene adskiller sig således fra klassisk tilsynsvirksomhed, der har fokus på overholdelse af regulering.

Det foreslås derfor, at erhvervsministeren bemyndiges til at fastsætte regler, der udpeger en myndighed til at varetage TLPT-relaterede anliggender i henhold til artikel 26, stk. 9, i DORA.

Derudover er det nødvendigt at strafbelægge overtrædelser af forordningens artikler i de danske hovedlove på det finansielle område. Det foreslås derfor i overensstemmelse med forordningen, at en række overtrædelser af forordningen strafbelægges med bøde ved at tilføje disse bestemmelser til opregninger i strafbestemmelserne i de relevante hovedlove.

Sammen med DORA-forordningen blev også Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022 vedtaget. Direktiv indeholder konsekvensændringer til en række direktiver på det finansielle område som følge af DORA-forordningen. Derfor foreslås tilsvarende konsekvensændringer i de bestemmelser i den danske lovgivning, der implementerer de ændrede direktivbestemmelser.

2.2. Udpegelse af operatører af finansielle digitale infrastrukturer og implementering af NIS 2-direktivet

2.2.1. Gældende ret

Finanstilsynet fører i dag tilsyn med it-sikkerheden hos fælles datacentraler og it-operatører af detailbetalingssystemer. Tilsynet er med til at sikre it-sikkerheden i de virksomheder, der står for it-driften i finansielle virksomheder, som har en central samfundsmæssig betydning. Tilsynet er desuden med til at sikre, at it-driften af et detailbetalingssystem, der er afgørende for, at bl.a. udbetaling af løn og pension, betaling for køb af varer og betaling af regninger kan foretages uden væsentlige forsinkelser.

Fælles datacentraler er reguleret i afsnit X c i lov om finansiel virksomhed. Ved fælles datacentraler forstås virksomheder, hvis væsentligste aktiviteter omfatter it-drifts- eller udviklingsopgaver for flere finansielle virksomheder, finansielle holdingvirksomheder, forsikringsholdingvirksomheder eller sådanne virksomheders dattervirksomheder, og som overvejende er ejet af disse virksomheder eller en eller flere foreninger, hvis medlemmer overvejende udgøres af disse virksomheder.

Reglerne for fælles datacentraler gælder også for datacentraler, der udfører væsentlige it-drift og it-udvikling for den fælles betalingsinfrastruktur,

medmindre datacentralen har tilladelse som it-operatør af et detailbetalingssystem.

En virksomhed automatisk omfattet af reglerne om fælles datacentraler, hvis f.eks. virksomhedens væsentligste aktiviteter netop er it-drifts- eller udviklingsopgaver for flere finansielle virksomheder, og virksomheden samtidig overvejende er ejet af flere finansielle virksomheder. Det kræver derfor ikke tilladelse fra Finanstilsynet at drive en fælles datacentral.

Reglerne for fælles datacentraler afspejler de regler, der også gælder finansielle virksomheders kontrol- og sikringsforanstaltninger på it-området, ligesom tilsynsrammen for tilsynet med datacentraler også afspejler det it-tilsyn, som Finanstilsynet fører med de finansielle virksomheder.

Det følger af lov om finansiel virksomhed, at reglerne om betryggende kontrol- og sikringsforanstaltninger på it-området finder tilsvarende anvendelse for fælles datacentraler.

Disse regler findes i ledelsesbekendtgørelsen, herunder særligt bekendtgørelsens bilag 5, der bl.a. fastsætter nærmere krav til den it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik, som en datacentral skal have.

Derudover følger det af lov om finansiel virksomhed, at reglerne om outsourcing finder tilsvarende anvendelse for fælles datacentraler. Reglerne om outsourcing er nærmere udmøntet i bekendtgørelse nr. 949 af 22. juni 2022 om outsourcing for kreditinstitutter m.v. og omfatter således i dag også de fælles datacentraler.

Herudover følger det af lov om finansiel virksomhed, at Finanstilsynet kan fastsætte bestemmelser om intern revision og om systemrevisionens gennemførelse i fælles datacentraler. Bemyndigelsen er udnyttet i bekendtgørelse nr. 1581 af 22. december 2022 om systemrevisionens gennemførelse i fælles datacentraler m.fl.

Endelig følger det af i lov om finansiel virksomhed, at kapitel 21 og 23 i lov om finansiel virksomhed og regler udstedt i medfør af disse kapitler finder tilsvarende anvendelse for fælles datacentraler med de fornødne tilpasninger. Det indebærer bl.a., at tilsynsrammen for tilsynet med finansielle virksomheder også gælder for finansielle datacentraler, herunder bl.a. reglerne om Finanstilsynets tavshedspligt, offentliggørelse, partsbestemmelser og klageadgang.

Finanstilsynet fører også tilsyn med it-operatører af detailbetalingssystemer, dvs. virksomheder, der er meddelt tilladelse til it-drift af et detailbetalingssystem efter i lov om kapitalmarkeder. It-operatører af detailbetalingssystemer er reguleret i kapitel 32 a i lov om kapitalmarkeder.

Et detailbetalingssystem er et betalingssystem, hvormed der i væsentligt omfang udføres clearing af betalinger i danske kroner mellem fysiske personer, virksomheder og offentlige myndigheder og mellem disse personer indbyrdes.

Reglerne om it-operatører af detailbetalingssystemers kontrol- og sikringsforanstaltninger på it-området afspejler ligesom for datacentraler det it-tilsyn, som Finanstilsynet fører med de finansielle virksomheder.

Det følger af lov om kapitalmarkeder, at it-operatører af detailbetalingssystemer skal have betryggende kontrol- og sikringsforanstaltninger på it-området. I forlængelse heraf følger det, at Finanstilsynet kan fastsætte nærmere regler om de foranstaltninger, som en it-operatør af et detailbetalingssystem skal træffe for at have betryggende kontrol- og sikringsforanstaltninger på it-området. Bemyndigelsen er ligesom for datacentraler, udnyttet i ledelsesbekendtgørelsen, herunder særligt bekendtgørelsens bilag 5, der bl.a. fastsætter nærmere krav til den it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik, som it-operatører af detailbetalingssystemer skal have.

Det følger også af lov om kapitalmarkeder, at Finanstilsynet fastsætter bestemmelser om intern it-revision og om systemrevisionens gennemførelse for en it-operatør af et detailbetalingssystem. Bemyndigelsen er udnyttet i bekendtgørelse nr. 1581 af 22. december 2022 om systemrevisionens gennemførelse i fælles datacentraler m.fl.

Endelig følger det af lov om kapitalmarkeder, at Finanstilsynet kan fastsætte nærmere regler om it-operatører af detailbetalingssystemers outsourcing. Reglerne om outsourcing er nærmere udmøntet i bekendtgørelse nr. 949 af 22. juni 2022 om outsourcing for kreditinstitutter m.v. og omfatter således i dag også it-operatører af detailbetalingssystemer.

2.2.2. Erhvervsministeriets overvejelser og den foreslåede ordning

I januar 2023 trådte NIS2-direktivet i kraft sammen med DORA-forordningen. NIS2-direktivet finder anvendelse fra den 18. oktober 2024 og DORA-forordningen fra den 17. januar 2025.

Hensigten med lovpakken er bl.a. at styrke it- og cybersikkerheden i den finansielle sektor ved at gennemføre en væsentlig udvidelse, harmonisering og modernisering af de juridiske rammer på tværs af medlemslandene.

Hvor DORA-forordningen alene finder anvendelse på virksomheder på det finansielle område, så fastsætter NIS 2-direktivet mere generelle regler om it-sikkerhed for kritiske infrastrukturer på tværs af sektorer og offentlige myndigheder. Direktivets regler gælder derfor, udover for dele af den finansielle sektor, også for bl.a. energi-, transport-, sundheds-, og forsyningssektoren, og for den offentlige forvaltning.

For så vidt angår forholdet mellem NIS 2-direktivet og DORA-forordningen, så følger det af præambelen i NIS 2-direktivet, at DORA-forordningens regler finder anvendelse i stedet for NIS 2-direktivets regler på de områder, som DORA-forordningen regulerer. Da DORA-forordningens regler favner kravene til virksomhedernes it- og cybersikkerhed i NIS 2-direktivet, og hertil fastsætter mere omfattende krav, er der ikke behov for at implementere direktivets regler for de virksomheder på det finansielle område, der er omfattet af forordningen.

DORA-forordningen omfatter stort set alle de virksomheder, der er reguleret i den finansielle lovgivning og underlagt Finanstilsynets tilsyn. Enkelte virksomhedstyper er dog ikke omfattet. Det gælder de fælles datacentraler, der står for it-drift og it-udvikling i finansielle virksomheder og den fællesbetalingsinfrastruktur, samt it-operatører af detailbetalingssystemer. Fælles datacentraler og it-operatører af detailbetalingssystemer omfattes dog af NIS2-direktivets mere generelle regler, der bl.a. finder anvendelse på digital infrastruktur og forvaltning af it-tjenester. Derfor skal reglerne i NIS2-direktivet implementeres for fælles datacentraler og it-operatører af detailbetalingssystemer.

For at sikre, at Finanstilsynet kan føre tilsyn med it- og cybersikkerheden i alle relevante virksomheder på det finansielle område, der udbyder digital infrastruktur og forvaltning af it-tjenester indenfor den finansielle sektor, og som omfattes af NIS 2-direktivets regler, foreslås det, at Finanstilsynet kan udpege disse virksomheder som operatører af finansielle digitale infrastrukturer. Det foreslås i den forbindelse, at det alene er virksomheder, hvis væsentligste aktiviteter består i at drive, administrere eller udvikle tjenester, som er nødvendige for finansielle virksomheders kritiske og vigtige forretningsfunktioner, der kan udpeges som operatører finansielle digitale infrastrukturer. Det vil bl.a. indebære, at Finanstilsynet kan udpege fælles datacentraler og it-operatører af detailbetalingssystemer som operatører af finansielle digitale infrastrukturer.

Det foreslås i forlængelse heraf, at der fastsættes regler i lov om finansiel virksomhed, der implementerer NIS 2-direktivets krav, for disse virksomheder, som udpeges som operatører af digitale finansielle infrastrukturer. Kravene, der foreslås implementeret fra NIS 2-direktivet, er overordnede og indebærer, at virksomhederne skal træffe tekniske, operationelle og organisatoriske foranstaltninger for at styre deres cyberrisici. Det omfatter bl.a. krav om politikker for risikoanalyse og informationssystemsikkerhed, krav om foranstaltninger til håndtering af it-sikkerhedshændelser og krav om foranstaltninger til grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse. Herudover foreslås det at implementere rapporteringsforpligtelser til Finanstilsynet om væsentlige hændelser og underretningspligt overfor modtagerne af virksomhedens tjenester. Det foreslås også at fastsætte enkelte supplerende tilsyns- og håndhævelsesforanstaltninger i overensstemmelse med direktivets krav, og at strafbelægge de relevante bestemmelser, der implementerer direktivets krav.

Kravene i NIS2-direktivet er overordnede og ikke sektorspecifikke. Implementeringen af NIS2-direktivet alene vil derfor isoleret set indebære en lempelse af kravene til cybersikkerheden for fælles datacentraler og it-operatører af detailbetalingssystemer, der i dag er omfattet af mere uddybende krav i ledelsesbekendtgørelsen, fordi disse gældende krav skal udgå fra bekendtgørelsen, når DORA-forordningen finder anvendelse.

Datacentraler har en særlig rolle i Danmark, hvor navnlig de små og mellemstore institutter i vid udstrækning anvender datacentraler til drift af kerneforretninger, og er derfor centrale for den danske finansielle sektor. Ligesom de fælles datacentraler er it-operatører af detailbetalingssystemer centrale for den danske finansielle sektor. Næsten alle betalinger sker i dag digitalt. Et cyberangreb mod betalingsinfrastrukturen kan have væsentlige systemiske konsekvenser.

For at bevare og sikre et ensartet højt cybersikkerhedsniveau i hele finanssektoren, herunder for fælles datacentraler og it-operatører af detailbetalingssystemer, foreslås det, at reglerne, som implementerer NIS 2-direktivet for de virksomheder, der bliver udpeget som operatører af finansielle digitale infrastrukturer, suppleres med nationale regler, der afspejler relevante krav fra DORA-forordningen. Herved vil der fortsat gælde ensartede krav for fælles datacentraler og it-operatører af detailbetalingssystemer, som også gælder for øvrige virksomheder på det finansielle område omfattet af DORA-forordningen. Det vil også være med til at understøtte de virksomheder, der benytter sig af levering af it-tjenesteydelser fra operatørerne af finansielle digitale infrastrukturer, i at overholde DORA-forordningen.

På den baggrund foreslås det konkret at fastsætte uddybende krav til operatører af digitale finansielle infrastrukturers ramme for styring af cyberrisici, herunder med krav til strategier, politikker, procedurer, og foranstaltninger på en række områder indenfor it- og cybersikkerheden. Det omfatter bl.a. krav til operatørernes beskyttelse i form af løbende overvågning af og kontrol med it-systemer og it-værktøjer, samt krav til beredskab og genopretning. Det omfatter også uddybende krav til styring og indberetning af it- og cyberhændelser, håndtering af tredjepartsrisici og krav til kontrakter med tredjepartsudbydere af it-tjenester.

Med reglerne foreslås også ledelsesmæssige og organisatoriske krav. Det gælder bl.a. krav om at ledelsen skal godkende, føre tilsyn med og gennemføre rammen for it- og cyberrisikostyring, at rammen regelmæssigt er genstand for intern revision og at det interne tilsyn med styring af it- og cyberrisici placeres i uafhængige kontrolfunktioner.

Det foreslås herudover at Finanstilsynet bemyndiges til at fastsætte nærmere regler for operatører af finansielle digitale infrastrukturer. Det gælder bl.a. for indholdet af rammerne for styring af it- og cyberrisici, herunder for strategier og politikker, ledelsens opgaver, rapportering af hændelser, tredjepartsrisici samt intern og ekstern systemrevision. Bemyndigelsen vil sikre, at reglerne for operatører af finansielle digitale infrastrukturer kan opfylde krav, der eventuelt bliver fastsat i medfør af delegerede retsakter til NIS 2-direktivet, eller som udspringer af DORA-forordningen, og som bør gælde tilsvarende.

Det foreslås i øvrigt at udnytte Finanstilsynets eksisterende tilsynsramme, der følger af lov om finansiel virksomhed i kapitel 21 og 23 i lov om finansiel virksomhed, og som også i dag gælder for datacentraler, ved at lade disse regler finde tilsvarende anvendelse for operatører af finansielle digitale infrastrukturer.

2.3. Ophævelse af reglerne om udpegning af væsentlige tjenester og indberetning af væsentlige hændelser til Finanstilsynet – tilbagerulning af NIS-direktivet

2.3.1. Gældende ret

I dag udpeger Finanstilsynet mindst hvert andet år de penge- og realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester efter henholdsvis lov om finansiel virksomhed eller lov om kapitalmarkeder. Ved udpegning skal Finanstilsynet bl.a. lægge vægt på om, de tjenester, der leveres, er

væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, leveringen af tjenesten afhænger af net- og informationssystemer, og en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Når en virksomhed er udpeget som operatør af væsentlige tjenester skal virksomheden rapportere hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, til Finanstilsynet og Center for Cybersikkerhed. Center for Cybersikkerhed er udpeget som CSIRT (Computer Security Incident Response Team), dvs. den kompetente myndighed der bl.a. håndterer it-sikkerhedshændelser.

Reglerne om operatører af væsentlige tjenester og rapportering af hændelser gennemfører dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

Som et eksempel på en hændelse, som en operatør af en væsentlig tjeneste skal rapportere om, kunne bl.a. være en bank, der bliver ramt af et hackerangreb, som betyder, at mange systemer, der normalt anvendes af både privatkunder i hele Danmark og interne i banken, ikke længere kan anvendes. Et andet eksempel kunne være en hændelse, der har væsentlige konsekvenser for kontinuiteten af driften af markedspladsen og den multilaterale handel med finansielle instrumenter, såsom en hændelse hvormed markedspladsens handelssystem svigter i en længere periode.

Desuden følger det af henholdsvis i lov om finansiel virksomhed og i lov om kapitalmarkeder, at Finanstilsynet kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Finanstilsynets ansatte er underlagt en særlig tavshedspligt efter lov om finansiel virksomhed. Finanstilsynet kan i nærmere angivne tilfælde videregive fortrolige oplysninger, uanset den særlige tavshedspligt, til bl.a. andre myndigheder i Danmark, indenfor EU/EØS eller udenfor EU/EØS. Finanstilsynet kan ikke videregive oplysninger til Den Fælles Afviklingsmyndighed (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Tilsvarende bestemmelser om Finanstilsynets tavshedspligt og undtagelser hertil fremgår også af de øvrige hovedlove på det finansielle område.

I dag udpeger Finanstilsynet mindst hvert andet år de penge- og realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester efter henholdsvis lov om finansiel virksomhed eller lov om kapitalmarkeder. Ved udpegning skal Finanstilsynet bl.a. lægge vægt på om, de tjenester, der leveres, er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, leveringen af tjenesten afhænger af net- og informationssystemer, og en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesten.

Når en virksomhed er udpeget som operatør af væsentlige tjenester skal virksomheden rapportere hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, til Finanstilsynet og Center for Cybersikkerhed. Center for Cybersikkerhed er udpeget som CSIRT (Computer Security Incident Response Team), dvs. den kompetente myndighed der bl.a. håndterer it-sikkerhedshændelser.

Reglerne om operatører af væsentlige tjenester og rapportering af hændelser gennemfører dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

Som et eksempel på en hændelse, som en operatør af en væsentlig tjeneste skal rapportere om, kunne bl.a. være en bank, der bliver ramt af et hackerangreb, som betyder, at mange systemer, der normalt anvendes af både privatkunder i hele Danmark og interne i banken, ikke længere kan anvendes. Et andet eksempel kunne være en hændelse, der har væsentlige konsekvenser for kontinuiteten af driften af markedspladsen og den multilaterale handel med finansielle instrumenter, såsom en hændelse hvormed markedspladsens handelssystem svigter i en længere periode.

Desuden følger det af henholdsvis i lov om finansiel virksomhed og i lov om kapitalmarkeder, at Finanstilsynet kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

Finanstilsynets ansatte er underlagt en særlig tavshedspligt efter lov om finansiel virksomhed. Finanstilsynet kan i nærmere angivne tilfælde videregive fortrolige oplysninger, uanset den særlige tavshedspligt, til bl.a. andre myndigheder i Danmark, indenfor EU/EØS eller udenfor EU/EØS. Finanstilsynet kan ikke videregive oplysninger til Den Fælles Afviklingsmyndighed (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Tilsvarende bestemmelser om Finanstilsynets tavshedspligt og undtagelser hertil fremgår også af de øvrige hovedlove på det finansielle område.

2.3.2. Erhvervsministeriets overvejelser og den foreslåede ordning

Med NIS2-direktivet sker der bl.a. en ophævelse af det første NIS-direktiv fra 2016. Ophævelsen af NIS-direktivet vil betyde, at bestemmelserne om udpegning af operatører af væsentlige tjenester bliver ophævet. Det gælder også kravet om indrapportering af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer. Endvidere sker der en ophævelse af Finanstilsynet mulighed for at oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge en hændelse eller håndtere en igangværende hændelse.

For fortsat at sikre et høj it- og cybersikkerhedsniveau i EU ved bl.a. at sikre, at kompetente myndigheder fortsat får overblik over it-hændelser og hermed kan imødegå it-risici i den finansielle sektor bliver reglerne om hændelsesrapportering i NIS-direktivet erstattet af et krav om indberetning af større it-relaterede hændelser og frivillig underretning om væsentlige cybertrusler til de kompetente myndigheder i artikel 19 i DORA-forordningen. DORA-forordningen finder bl.a. anvendelse på penge- og realkreditinstitutter, operatører af markedspladser og centrale modparter (CCP'er), jf. artikel 2, stk. 1, litra a, h og i. Når de kompetente myndigheder modtager en underretning om en større it-relateret hændelse, skal den kompetente myndighed bl.a. rettidigt forelægge nærmere oplysninger herom til CSIRT'er, jf. artikel 19, stk. 6, litra c. I Danmark vil Finanstilsynet blive udpeget som kompetent myndighed, jf. pkt. 2.2. ovenfor om DORA-forordningen og Erhvervsministeriets overvejelser og den foreslåede ordning. Center for Cybersikkerhed vil blive udpeget som CSIRT i henhold til NIS 2-direktivet.

Desuden vil virksomhederne blive underlagt et krav om at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter, hvad der er relevant, jf. artikel 14, stk. 1, i DORA-forordningen.

De kompetente myndigheder vil bl.a. også skulle orientere Den Europæiske Banktilsynsmyndighed (EBA), Den Europæiske Værdipapir- og Markedstilsynsmyndighed (ESMA) eller Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger (EIOPA) om indberetning af større it-relaterede hændelser, som de modtager fra virksomhederne, jf. artikel 19, stk. 6, litra a, i DORA.

Som noget nyt vil det også blive relevant for Finanstilsynet at dele oplysninger med ENISA. Det vil bl.a. være relevant for Finanstilsynet at videreformidle hændelsesindberetninger i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB, og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Det foreslås derfor, at Finanstilsynet skal kunne videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

2.4. Ny regulering af kryptoaktiver og kryptoaktivtjenester, mv. (supplering af dele af MiCA-forordningen)

2.4.1. Gældende ret

Et kryptoaktiv er en digital repræsentation af et aktiv (f.eks. en aktie eller valuta) eller en rettighed (f.eks. en forkøbsret til en vare eller en tjenesteydelse), der kan opbevares og handles digitalt ved brug af distribueret hovedbog-teknologi, hvilket betyder at transaktioner kan verificeres decentralt mellem parter i stedet for f.eks. at være afhængig af en bank til at udføre transaktioner.

I dag er udstedere af kryptoaktiver og udbydere af kryptoaktivtjenester som udgangspunkt ikke omfattet af den finansielle lovgivning. Kryptoaktiver er i dag kun omfattet af den finansielle lovgivning i det omfang, at kryptoaktiverne udgør finansielle instrumenter eller andre former for regulerede aktiver, såsom elektroniske penge.

Størstedelen af de kryptoaktiver, der eksisterer i dag, udgør ikke finansielle instrumenter eller andre regulerede aktiver. De er derfor ikke omfattet af den gældende finansielle lovgivning. Udstedere og udbydere af disse kryptoaktiver og tjenester forbundet hermed er derfor som udgangspunkt ikke omfattet af nogen tilladelseskrav under den finansielle lovgivning. Det betyder samtidig, at investorer og forbrugere, der handler med kryptoaktiver i dag, ikke er omfattet af den investor- og forbrugerbeskyttelse, som den gældende finansielle lovgivning fastsætter.

I særlige tilfælde vil et kryptoaktiv kunne udgøre finansielle instrumenter, såsom aktier eller e-penge, der er reguleret gennem den finansielle lovgivning. Udstedere af sådanne kryptoaktiver og udbydere af

kryptoaktivtjenester med sådanne kryptoaktiver er omfattet af den finansielle lovgivning. Det er eksempelvis tilfældet, hvis en virksomhed yder skønsmæssig porteføljepleje med kryptoaktiver, der udgør aktier. I det tilfælde skal virksomheden have tilladelse af Finanstilsynet som fondsmæglerselskab.

Hvidvaskloven regulerer i dag, at udbydere af tjenester med virtuelle valutaer skal registreres i Finanstilsynets hvidvaskregister efter hvidvasklovens § 48, stk. 2. Det betyder eksempelvis, at en virksomhed, der tilbyder en platform, hvor forbrugere kan handle bitcoins og lignende kryptoaktiver, i dag er omfattet af registreringspligten i hvidvaskloven.

De omfattede udbydere af tjenester med virtuel valuta er udbydere af veksling mellem virtuelle valutaer og fiatvalutaer (lovlige betalingsmidler udstedt af centralbanker, f.eks. DKK), udbydere af virtuelle tegnebøger, udbydere af veksling mellem en eller flere typer af virtuel valuta, udbydere af overførsel af virtuel valuta og udbydere af finansielle tjenester relateret til en udsteders udbud eller salg af virtuel valuta.

Europa-Parlamentets og Rådets forordning (EU) 2015/847 af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler (pengeoverførselsforordningen) regulerer i dag, hvilke oplysninger der skal medsendes ved overførsel af fiatvaluta.

2.4.2. Erhvervsministeriets overvejelser og den foreslåede ordning

Den 30. december 2024 træder Europa-Parlamentets og Rådets forordning 2023/1113/EU af 31. maj 2023 om oplysninger, der skal medsendes ved pengeoverførsler og ved overførsler af visse kryptoaktiver og om ændring af direktiv 2015/849/EU, (herefter "den omarbejdede pengeoverførselsforordning") i kraft. Den omarbejdede pengeoverførselsforordning udvider forordningens anvendelsesområde til også at omfatte oplysninger, som skal medsendes ved overførsler af kryptoaktiver.

For at sikre de lovgivningsmæssige rammer for bekæmpelse af hvidvask af penge og finansiering af terrorisme og for at tilpasse EU-retten til internationale henstillinger, ændredes dele af 4. hvidvaskdirektiv i forordningen i overensstemmelse med MiCA. 4. hvidvaskdirektivs anvendelsesområde udvides således til at omfatte alle kategorier af udbydere af kryptoaktivtjenester i overensstemmelse med MiCA, som dækker et bredere spektrum af virksomheder og personer, end de udbydere af tjenester med virtuelle valutaer, som er omfattet i dag.

Udbydere af kryptoaktivtjenester dækker over de samme virksomheder og personer, som fremgår af FATF's anbefaling nr. 15 om udbydere af tjenester med virtuel valuta. Da Danmark har gennemført FATF's anbefaling nr. 15 dækker udbydere af kryptoaktivtjenester, som defineret i MiCA, ligeledes over de samme virksomheder og personer, som er omfattet af hvidvasklovens anvendelsesområde.

Ligeledes fastsættes en række krav til udbydere af kryptoaktivtjenester, når disse etablerer korrespondentforbindelser med andre udbydere af kryptoaktivtjenester. Endeligt fastsættes en række krav til udbydere af kryptoaktivtjenester, når disse gennemfører overførsler af kryptoaktiver, som er rettet mod eller stammer fra selvhostede adresser.

Markedet for kryptoaktiver er vokset globalt de seneste år, også i Danmark. I Danmark har virksomheder, der er involveret i udstedelse og udbud af kryptoaktiver som udgangspunkt ikke været omfattet af den finansielle lovgivning. Kun i særlige tilfælde, hvor kryptoaktiver falder ind under definitionen af "finansielle instrumenter" eller "andre regulerede aktiver", er de omfattet af den finansielle lovgivning i Danmark.

Reguleringen af virksomheder, der er involveret i udstedelse og udbud af kryptoaktiver er fragmenteret på tværs af EU. Enkelte EU-medlemslande har indført deres egne nationale regler for virksomheder, der er involveret i udstedelse og udbud af kryptoaktiver, der falder udenfor anvendelsesområdet for den finansielle lovgivning i EU, med henblik på at regulere udstedere og udbydere af kryptoaktivtjenester med disse kryptoaktiver. Andre EU-medlemslande overvejer, om de nationalt skal lovgive på området for kryptoaktiver.

Den fragmenterede og ofte manglende regulering af kryptoaktiver, der ikke udgør finansielle instrumenter betyder generelt, at indehavere af disse kryptoaktiver er udsat for risici, navnlig på områder, der ikke er omfattet af investor- eller forbrugerbeskyttelsesreglerne i den finansielle lovgivning. Det vil eksempelvis være tilfældet for de mange investorer og forbrugere, der handler med kryptoaktiver som bitcoin. Det kan også skabe risici for markedsintegriteten, bl.a. ved markedsmisbrug og økonomisk kriminalitet.

MiCA har til formål at skabe en særlig og harmoniseret ramme for markedet for kryptoaktiver i EU ved at fastsætte specifikke bestemmelser for kryptoaktiver og dermed forbundne aktiviteter og tjenester, der endnu ikke er omfattet af den finansielle lovgivning. Det skal støtte innovation og fair konkurrence samtidig med, at der sikres et højt beskyttelsesniveau. Det skal give kunderne fordele i form af adgang til billigere, hurtigere og sikrere finansielle tjenesteydelser og forvaltning af midler. Det er

Erhvervsministeriets forventning, at en samlet regulering i EU vil afhjælpe de eksisterende hindringer for et velfungerende marked for kryptoaktiver og sikre investorer, erhvervsdrivende og forbrugere et højt beskyttelsesniveau gennem fastsættelse af et regelsæt i EU.

MiCA finder direkte anvendelse i Danmark, og det er samtidig nødvendigt, at der med lovforslaget indføres regler i lov om finansiel virksomhed og en række andre love på det finansielle område. Det er samtidig vigtigt, at der udpeges en kompetent myndighed i Danmark til at håndhæve reglerne overfor de relevante aktører.

Finanstilsynet udpeges i henhold til artikel 93, stk. 1, i MiCA, som den kompetente myndighed i Danmark, der er ansvarlig for at udføre de i forordningen fastsatte funktioner og opgaver. MiCA skal sikre harmoniserede tilsynsmæssige rammer i EU, eksempelvis ved at stille ensartede krav til bl.a. udstedere af kryptoaktiver og udbydere af kryptoaktivtjenester med henblik på at sikre investor- og forbrugerbeskyttelse, markedsintegritet og den finansielle stabilitet i EU.

Det foreslås blandt andet, at Finanstilsynet tillægges beføjelser til at meddele og inddrage tilladelse til udstedere af aktivbaserede tokens, udstedere af e-pengetokens og udbydere af kryptoaktivtjenester. Som konsekvens heraf foreslås det at ophæve krav om registrering efter hvidvaskloven, jf. lovforslaget § 7, nr. 13. En række virksomheder, der allerede har tilladelse under den finansielle lovgivning, skal ikke søge om tilladelse til eksempelvis at udbyde kryptoaktivtjenester. Det er virksomheder, som fremgår af artikel 60, stk. 1-6, i MiCA. Disse virksomheder skal alene underrette den kompetente myndighed i hjemlandet om deres aktiviteter med kryptoaktiver. Det foreslås, at Finanstilsynet udpeges som den kompetente myndighed til at modtage disse underretninger.

Det foreslås, at udstedere af aktivbaserede tokens og udbydere af kryptoaktivtjenester skal betale en årlig afgift til Finanstilsynet. Afgiftsbetalingerne har til formål at dække omkostningerne til Finanstilsynets virksomhed. Den foreslåede afgiftsbetaling er fastsat under hensyntagen til, at de aktiviteter og udbydere, som Finanstilsynet skal føre tilsyn med efter MiCA, er et komplekst og nyt område. I udmålingen er der også taget hensyn til Finanstilsynets risikobaserede tilsyn samt afgiftsbetalingen for sammenlignelige virksomheder under Finanstilsynets tilsyn. Finanstilsynets tilsynsvirksomhed vil blandt andet bestå i at give og inddrage tilladelse til udstedere af aktivbaserede tokens og udbydere af kryptoaktivtjenester samt føre tilsyn med disse, herunder gennemføre inspektioner og varetage øvrige løbende tilsynsopgaver. Hertil kommer

forpligtelser overfor øvrige tilsynsmyndigheder, EBA og ESMA, herunder bl.a. samarbejds- og notifikationsforpligtelser samt oplysnings- og vejledningsforpligtelser.

Virksomheder, der ikke skal have selvstændig tilladelse af Finanstilsynet for at kunne udbyde aktivbaserede tokens til offentligheden eller anmode om optagelse til handel eller udbyde kryptoaktivtjenester, vil ikke blive opkrævet yderligere afgifter som konsekvens af MiCA. Disse udbydere fremgår af artikel 16, stk. 1, litra b, samt artikel 60, stk. 1-6, i MiCA. Det er f.eks. pengeinstitutter og fondsmæglerselskaber.

Det foreslås, at Finanstilsynet tillægges undersøgelses- og tilsynsbeføjelser, herunder mulighed for at indhente oplysninger og gennemføre inspektioner samt gribe ind over for overtrædelse af forordningen, så der kan føres et effektivt tilsyn med overholdelsen af forordningen. I tillæg hertil foreslås det, at Finanstilsynet gives beføjelse til at give påbud og påtaler for overtrædelser af MiCA, samt at gribe ind med en række målrettede foranstaltninger. Finanstilsynet gives eksempelvis beføjelse til at kræve, at en udbyder af kryptoaktivtjenester suspenderer leveringen af kryptoaktivtjenester, eller helt forbyde leveringen af kryptoaktivtjenester, hvis Finanstilsynet finder, at forordningen er blevet overtrådt, eller hvis der er rimelig mistanke om, at den vil blive overtrådt.

Medlemslandene kan beslutte, at en række artikler i MiCA skal kunne underlægges strafferetlige sanktioner gennem national ret. Det foreslås som konsekvens heraf, at overtrædelser af en række artikler i MiCA enten kan straffes med bøde, fængsel indtil 4 måneder eller fængsel indtil 1 år og 6 måneder i tilfælde af eksempelvis markedsmisbrug.

Endeligt foreslås det at ændre hvidvaskloven, så loven vil finde anvendelse på samme aktører og anvende samme definitioner som MiCA og den omarbejdede pengeoverførselsforordning.

Den foreslåede ændring af hvidvaskloven vil medføre, at alle udbydere af tjenester med virtuel valuta fremover vil blive samlet under betegnelsen udbydere af kryptoaktivtjenester. Virksomheder og personer, som udbyder kryptoaktivtjenester, vil fortsat være omfattet af de forpligtelser, der gælder i hvidvaskloven, med undtagelse af registreringskravet i hvidvaskloven, som foreslås ophævet, jf. ovenfor i afsnit 2.1.2, og erstattet af en tilladelsesordning i henhold til MiCA.

Der henvises i øvrigt til lovforslagets § 1. nr. 2-4, 24, 26, 34, 36, 41-43, og 46-48, (ændringer til lov om finansiel virksomhed) § 2, nr. 15, 16, og 21-24, (ændringer til lov om betalinger), § 3, nr. 3, 16, (ændringer lov om

kapitalmarkeder), § 4, nr. 2, 3, 5, 10, 13, 10-16, (ændringer til lov om fondsmæglerselskaber og investeringsservice og -aktiviteter), § 5, nr. 2, 4, 8 og 9, (ændringer til lov om forvaltere af alternative investeringsfonde m.v.), § 7 (ændringer til hvidvaskloven), samt de specielle bemærkninger hertil.

2.5. Aflønningsregler for firmapensionskasser

2.5.1. Gældende ret

Aflønningsreglerne har overordnet set til formål at sikre, at firmapensionskasser fører en forsvarlig lønpolitik, som fremmer en sund og forsvarlig virksomhedsledelse, og som ikke tilskynder til overdreven risikotagen, der kan undergrave den pågældende virksomheds risikostyring. Aflønningsreglerne gælder på tværs af den finansielle sektor og sikrer et ensartet beskyttelsesniveau for kunder, indskydere og investorer indenfor de forskellige delsektorer.

Aflønningsreglerne er en udmøntning af den politiske aftale om forsvarlig aflønningspolitik i den finansielle sektor af 31. august 2010 mellem den daværende regering (Venstre og Det Konservative Folkeparti), Socialdemokraterne, Dansk Folkeparti, Socialistisk Folkeparti, Radikale Venstre og Liberal Alliance og den politiske aftale om regulering af systemisk vigtige finansielle institutter (SIFI) samt krav til alle banker og realkreditinstitutter om mere og bedre kapital og højere likviditet af 10. oktober 2013 mellem den daværende regering (Socialdemokraterne, Radikale Venstre og Socialistisk Folkeparti), Venstre, Dansk Folkeparti, Liberal Alliance og Det Konservative Folkeparti. Med aftalerne blev bestemmelserne fra Europa-Parlamentets og Rådets direktiv 2010/76/EU af 24. november 2010 (CRD III) og Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 (CRD IV) gennemført på tværs af den finansielle sektor sammen med enkelte nationale skærpelser.

De gældende regler om lønpolitik og aflønning af bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil, såkaldte væsentlige risikotagere, er nærmere fastsat i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser (aflønningsbekendtgørelsen), som ændret ved bekendtgørelse nr. 360 af 23. marts 2022. Aflønningsbekendtgørelsen er, for så vidt angår firmapensionskasser udstedt med hjemmel i § 43 i lov om firmapensionskasser.

De gældende aflønningsregler foreskriver, at firmapensionskasser skal have en skriftlig lønpolitik. Aflønningspolitikken skal godkendes af

firmapensionskassens generalforsamling, og bestyrelsesformanden skal i sin formandsberetning for generalforsamlingen redegøre for aflønningen af firmapensionskassens bestyrelse og direktion.

En firmapensionskasse skal ved outsourcing af aktiviteter sikre, at lønpolitikken overholdes af den virksomhed, som firmapensionskassen har outsourcet aktiviteterne til, i det omfang aflønningen relaterer sig til arbejde, som er outsourcet firmapensionskassen. Det følger af § 19 i aflønningsbekendtgørelsen.

Bestyrelsen, direktionen og andre væsentlige risikotagere i firmapensionskasser er underlagt en række regler om udbetalingsbegrænsninger af variable løndele, eksempelvis et forholdsmæssigt loft for den variable løndels størrelse set i forhold til den faste løndels størrelse. Det følger således af de gældende regler, at de variable løndele til et medlem af bestyrelsen eller direktionen i en firmapensionskasse højst må udgøre 50 pct. af vedkommendes faste løndel. De væsentlige risikotagere i firmapensionskassen må modtage op til 100 pct. af deres faste løn i variabel løn, dog kan firmapensionskassens øverste organ beslutte, at dette loft hæves til 200 pct., hvis visse betingelser er opfyldt. Det følger af § 18, stk. 1, nr. 1-3, i den gældende aflønningsbekendtgørelse.

Endvidere indeholder de gældende aflønningsregler krav om, at en vis minimumsandel af de variable løndele skal udgøres af en balance af finansielle instrumenter, og at den skal omfatte en fleksibel, udskudt løndel, som tager højde for den pågældende firmapensionskasses virksomhedsart og tidshorisont. Det følger af § 18, stk. 1, nr. 4, i den gældende aflønningsbekendtgørelse. Herudover foreskriver de gældende aflønningsregler, at udbetalingen sker over en periode på mindst tre år for væsentlige risikotagere og fire år for medlemmer af direktionen og bestyrelsen med påbegyndelse et år efter beregningstidspunktet, og som tilpasses den pågældende virksomhed og risici samt de pågældende ansattes aktiviteter. Det følger af § 18, stk. 1, nr. 5, i den gældende aflønningsbekendtgørelse. Anvendelsen af aktieoptioner er for bestyrelsen og direktionen begrænset således, at andelen heraf højst må udgøre 12,5 pct. af vedkommendes faste løndel, jf. § 18, stk. 2, i aflønningsbekendtgørelsen.

Firmapensionskasser skal også sikre, at finansielle instrumenter, som tildeles bestyrelsen, direktionen eller andre væsentlige risikotagere som en del af en variabel løndel, ikke må afhændes i en passende periode, og at disse personer forpligter sig til ikke at benytte personlige afdækningsstrategier eller løn- og ansvarsrelaterede forsikringer til at

undergrave de risikotilpasningsvirkninger, der er indbygget i deres aflønningsvilkår. Det følger af § 18, stk. 3, og § 9, stk. 2, nr. 7, i den gældende aflønningsbekendtgørelse.

Derudover skal firmapensionskasser sikre, at udbetalingen af en udskudt variabel løndel betinges af, at de kriterier, der har dannet grundlag for beregningen af den variable løndel, fortsat er opfyldt på udbetalingstidspunktet, samt at firmapensionskassens og vedkommendes personlige forhold m.v. ikke har ændret sig væsentligt i forhold til beregningstidspunktet. Er firmapensionskassens økonomiske situation eksempelvis væsentligt forringet i udskydelsesperioden, skal den variable løndel reduceres herefter. Uanset udskydelsesperiode kan en variabel løndel kræves tilbagebetalt, hvis denne er udbetalt til et medlem af bestyrelsen eller direktionen eller en væsentlig risikotager på grundlag af fejlagtige oplysninger, og modtageren er i ond tro herom. Kravene om reduktion og tilbagebetaling af en variabel løndel følger af § 18, stk. 4 og 5, i aflønningsbekendtgørelsen, og virksomhedens disposition skal desuden opfylde kravene i § 9, stk. 2, nr. 1 og 5, i aflønningsbekendtgørelsen.

Det følger endvidere af de gældende regler, at hvis et medlem af bestyrelsen eller direktionen eller en væsentlig risikotager, der modtager en variabel pensionsydelse, forlader firmapensionskassen inden pensionstidspunktet, skal virksomheden tilbageholde den variable del af pensionsydelsen i fem år i form af finansielle instrumenter. Både kravet om betinget udbetaling af den variable pensionsydelse og muligheden for at kræve tilbagebetaling af en allerede udbetalt pensionsydelse finder anvendelse i et sådant tilfælde. Hvis modtageren derimod er medlem af bestyrelsen eller ansat i firmapensionskassen ved pensionsalderen, skal firmapensionskassen udbetale den variable del af pensionsydelsen til modtageren i form af finansielle instrumenter uden mulighed for afhændelse eller udnyttelse i en femårig periode. I et sådant tilfælde finder muligheden for at kræve tilbagebetaling af en allerede udbetalt pensionsydelse anvendelse. Det følger af § 18, stk. 6, i den gældende aflønningsbekendtgørelse.

Overtrædelser af visse aflønningsregler straffes med bøde, jf. § 29 i aflønningsbekendtgørelsen.

2.5.2. Erhvervsministeriets overvejelser og den foreslåede ordning

Aflønningsreglerne sikrer, at firmapensionskasser fører en forsvarlig lønpolitik, som fremmer en sund og effektiv risikostyring. Med lovforslaget videreføres en række gældende aflønningskrav med redaktionelle ændringer i overensstemmelse med de politiske aftaler, jf. afsnit 2.5.1. Med lovforslaget samles de væsentligste bestemmelser om lønpolitik og variabel

aflønning af bestyrelsen, direktionen og andre væsentlige risikotagere i firmapensionskasser på lovniveau, som det er tilfældet i den øvrige finansielle lovgivning. Det indebærer, at §§ 8, 14, 18, og 19 i aflønningsbekendtgørelsen videreføres i de foreslåede §§ 43 e-43 h i lov om firmapensionskasser med de fornødne redaktionelle ændringer. Der vil samtidig ske en tilpasning af den gældende aflønningsbekendtgørelse.

Lovforslaget viderefører visse bestemmelser for firmapensionskasser, som er fastsat i Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'er) aktiviteter og tilsynet hermed. De pågældende bestemmelser har hidtil været implementeret i aflønningsbekendtgørelsen.

Udover at lovforslaget viderefører gældende ret, indfører lovforslaget også enkelte nye krav. Lovforslaget indfører et krav om, at firmapensionskassers lønpolitik skal være kønsneutral, baseret på princippet om lige løn for samme arbejde eller arbejde af samme værdi uanset den ansattes køn.

Lovforslaget forlænger desuden minimumskravene til udskydelses-perioderne for variabel aflønning. Ifølge de gældende aflønningsregler om udskydelse af udbetaling af variable løndele skal udbetalingen af mindst 40 pct., ved større beløb mindst 60 pct., ske over en periode på mindst tre år med påbegyndelse et år efter beregningstidspunktet, dog for bestyrelsen og direktionen mindst fire år, med en ligelig fordeling over årene eller med en voksende andel i slutningen af perioden, jf. § 18, stk. stk. 1, nr. 5, i aflønningsbekendtgørelsen. Det forslås at skærpe udskydelsesperioden, som fremgår af aflønningsbekendtgørelsen for at ensrette kravene på tværs den finansielle sektor. Udskydelsesperioden foreslås på den baggrund fastsat til mindst fire år for væsentlige risikotagere og mindst fem år for medlemmer af bestyrelse og direktion. Reglerne udspringer af Europa-Parlamentets og Rådets direktiv (EU) 2019/878 af 20. maj 2019 (CRD V) på kreditinstitutområdet og er gennemført for øvrige finansielle virksomheder, i dele af den finansielle regulering ved lov nr. 2110 af 22. december 2020 og lov nr. 2382 af 14. december 2021. Hensigten med at indføre kravet er at opretholde ensartede aflønningsregler i den finansielle sektor i overensstemmelse med de politiske aftaler på området.

Herudover foreslås det at indføre gennemførelsen af anbefalingerne fra Komitéen for god Selskabsledelse (2017), afsnit 4.2., oplysninger om vederlag, om vederlagspolitik og vederlagsrapporter, som ved seneste revision i 2020 udgik i forbindelse med implementeringen af aktionærrettighedsdirektivet i selskabsloven. Anbefalinger fra Komitéen for god Selskabsledelse finder anvendelse for selskaber, som har aktier optaget

til handel på et reguleret marked i Danmark efter et følg eller forklar-princip, jf. årsregnskabslovens § 107 b. Med den politiske aftale af 31. august 2010 om forsvarlig aflønningspolitik i den finansielle sektor opfordres finansielle virksomheder til at følge anbefalingerne efter følg eller forklar-princippet – også selvom virksomheden ikke er børsnoteret. Det forslås også at implementere Ansvarsudvalgets anbefalinger til transparens på aflønningsområdet i betænkning nr. 1575 om skærpet ansvarsvurdering for ledelsesmedlemmer m.v. i finansielle virksomheder.

Det foreslås på den baggrund at indføre krav om godkendelse og offentliggørelse af lønpolitikker i firmapensionskasser. En lønpolitik skal godkendes ved enhver væsentlig ændring og mindst hvert fjerde år, og den skal forblive offentligt tilgængelig på virksomhedens hjemmeside, så længe politikken er gældende.

Det foreslås desuden at indføre krav om, at formanden for bestyrelsen skal forklare og begrunde lønpolitikkens indhold og dens efterlevelse i sin beretning for virksomhedens øverste organ samt krav om det øverste organs godkendelse af bestyrelsens aflønning for det indeværende år.

Herudover foreslås det at indføre en pligt til årligt at udarbejde og offentliggøre en vederlagsrapport over de enkelte ledelsesmedlemmers samlede aflønning. Vederlagsrapporten skal indeholde oplysninger om det samlede vederlag, som hvert medlem af bestyrelsen og direktionen, som led i dette hverv, har optjent fra firmapensionskassen og andre virksomheder indenfor samme koncern i de seneste tre år, herunder oplysninger om fastholdelses- og fratrædelsesordningers væsentligste indhold samt en redegørelse for sammenhængen mellem ledelsens aflønning og virksomhedens strategi og relevante mål herfor. Vederlagsrapporten skal hurtigst muligt efter det øverste organs forsamling offentliggøres på firmapensionskassens hjemmeside og forblive offentligt tilgængelig på den pågældende firmapensionskasses hjemmeside i en periode på 10 år. Vederlagsrapporten kan være tilgængelig i en længere periode, forudsat at den ikke længere indeholder personoplysninger.

Det findes hensigtsmæssigt at indføre krav til offentliggørelse af lønpolitik og udarbejdelse af vederlagsrapport for firmapensionskasser til lov om firmapensionskasser af hensyn til at sikre ensartede regler om aflønning på tværs af den finansielle sektor samt større transparens om aflønningen af ledelsen i firmapensionskasser.

2.6. Opgørelse af søjle II-tillæg og det vejledende kapitalgrundlag

2.6.1. Gældende ret

Lov om finansiel virksomheds kapitel 10 indeholder regler om pengeinstitutters og realkreditinstitutters solvens, herunder regler om solvensbehov og det vejledende kapitalgrundlag.

Det følger af § 124, stk. 2, i lov om finansiel virksomhed, at pengeinstitutter og realkreditinstitutter skal opgøre deres individuelle solvensbehov, efter instituttets vurdering af det tilstrækkelige kapitalgrundlag, mens § 124, stk. 3, angiver, at Finanstilsynet kan fastsætte solvenskrav, som er udtryk for Finanstilsynets vurdering af instituttets tilstrækkelige kapitalgrundlag.

Det følger af § 124 a, at Finanstilsynet årligt fastsætter et vejledende niveau af yderligere kapitalgrundlag for de individuelle kreditinstitutter og meddeler dette til kreditinstitutterne. Finanstilsynet meddeler ved afgørelse institutterne det yderligere kapitalgrundlag, som instituttet skal opretholde, ud over det kombinerede kapitalbufferkrav, for at kunne tåle det hårde stressscenarie i Finanstilsynets tilsynsmæssige stresstest uden at bryde med det individuelle solvensbehov eller solvenskrav, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 94.

§ 125 fastsætter regler for de oplysninger, penge- og realkreditinstitutter skal indsende til Finanstilsynet ved brud på det kombinerede kapitalbufferkrav.

Det kombinerende kapitalbufferkrav består af kapitalbevaringsbufferen, den kontracykliske buffer, SIFI-bufferen og den systemiske buffer, jf. § 5, stk. 1, nr. 36, i lov om finansiel virksomhed.

2.6.2. Erhvervsministeriets overvejelser og den foreslåede ordning

Det gearingsbaserede solvensbehov og solvenskrav og det gearingsbaserede vejledende niveau af yderligere kapitalgrundlag (Leverage ratio pillar 2 guidance - P2G-LR) knytter sig til gearingsgradskavet som blev indført den 28. juni 2021. Gearingsgradskravet adskiller sig fra de risikobaserede kapitalkrav ved at eksponeringerne ikke vægtes efter en vurdering af, hvor risikofyldte de er. Gearingsgradskravet bestemmer således, hvor meget kapital institutterne skal have i forhold til deres uvægtede eksponeringer, mens de risikobaserede kapitalkrav bestemmer, hvor meget kapital institutterne skal have i forhold til deres risikovægtede eksponeringer.

I § 124, stk. 2 og 3, i lov om finansiel virksomhed fremgår det, at solvensbehovet og solvenskravet opgøres i procent af den risikovægtede eksponering. Ligeledes fremgår det af § 124 a stk. 1, at det vejledende niveau af yderligere kapitalgrundlag (Pillar 2 guidance – P2G) opgøres i procent af den risikovægtede eksponering. Det fremgår imidlertid ikke,

hvordan det gearingsbaserede solvensbehov og solvenskrav samt P2G-LR opgøres.

Det fremgår dog af bemærkningerne til § 124 a i lov om finansiel virksomhed, at der sondres mellem P2G-LR, og P2G, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 94. Denne sondring er også relevant for opgørelsen af solvensbehovet og solvenskravet. Den nuværende formulering af reglerne kan derfor give anledning til tvivl om opgørelsen af solvensbehov og solvenskrav samt P2G-LR.

Det foreslås derfor at præcisere, at det risikobaserede solvensbehov og solvenskrav samt P2G opgøres i forhold til den risikovægtede eksponering, mens det gearingsbaserede solvensbehov og solvenskrav samt P2G-LR opgøres i forhold til den ikke-risikovægtede eksponering.

Det foreslås derfor at præcisere i § 124, stk. 2 og 3, og § 124 a, stk. 1, at det risikobaserede solvensbehov og solvenskrav samt P2G opgøres i forhold til den risikovægtede eksponering, mens det gearingsbaserede solvensbehov og solvenskrav samt P2G-LR opgøres i forhold til den ikke-risikovægtede eksponering.

Det foreslåede vil medføre, at der skabes klarhed om retstilstanden vedrørende opgørelse af henholdsvis det gearingsbaserede solvensbehov og solvenskrav og P2G-LR.

Den Europæiske Banktilsynsmyndighed (EBA) har udstedt retningslinjer for opgørelse af det vejledende niveau af kapitalgrundlag, jf. EBA/GL/2022/03.

Den nuværende danske praksis med opgørelse af P2G i henhold til bemærkningerne til § 124 a, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 94-95, er imod hensigten ikke i overensstemmelse med de europæiske retningslinjer.

Med forslaget bringes opgørelsen af P2G i overensstemmelse med europæiske retningslinjer, hvilket betyder, at P2G vil blive højere end ved den nuværende danske praksis.

Institutterne fastsætter i praksis i dag en målsætning for størrelsen af deres kapitalgrundlag, som sikrer, at institutterne opererer efter en kapitalmålsætning, som i udgangspunktet vil være på niveau med eller højere end P2G. Dette vil som udgangspunkt fortsat være tilfældet ved den justerede metode for opgørelse af P2G.

På denne baggrund vurderes forslaget ikke at have videre betydning for institutternes overordnede kapitalstyring, medmindre institutterne ikke fastsætter en hensigtsmæssig kapitalmålsætning. I de tilfælde vil Finanstilsynet dog allerede være i dialog med institutterne om fastsættelse af en hensigtsmæssig kapitalmålsætning.

Det fremgår yderligere af EBA's retningslinjer, at det gearingsbaserede vejledende niveau af yderligere kapital (P2G-LR) kan opfyldes af kernekapital. Det fremgår imidlertid af § 124 a stk. 3, i lov om finansiel virksomhed, at P2G-LR skal opfyldes af en højere kvalitet af kapital – nemlig egentlig kernekapital.

Det foreslås derfor, at det i § 124 a, stk. 3, i lov om finansiel virksomhed angives, at institutterne også kan benytte anden kernekapital end egentligt kernekapital til at opfylde P2G-LR.

Det foreslåede vil medføre, at den danske tilgang til opfyldelse af P2G-LR bringes i overensstemmelse med den europæiske tilgang, jf. EBA/GL/2022/03.

2.7. Administrationsselskab for garantifonden for skadesforsikringsselskaber

2.7.1. Gældende ret

Garantifonden for skadesforsikringsselskaber (Fonden) blev oprettet ved lov om en garantifond for skadesforsikringsselskaber, jf. lov nr. 457 af 10. juni 2003, der trådte i kraft den 1. oktober 2003.

Fonden sikrer på forbrugerskadeforsikringsområdet, at der ydes dækning til berørte forsikringstagere i tilfælde af et skadesforsikringsselskabs konkurs.

Fonden administreres af et sekretariat, der dog ikke bistår ved skadesbehandlingen som følge af et skadesforsikringsselskabs konkurs, da Fonden ikke har kapacitet til at udføre denne opgave. For at være i stand til at påtage sig en betydelig administrativ byrde, i det øjeblik der skal udbetales erstatninger m.v. fra Fonden, antager bestyrelsen for Fonden fornøden medhjælp, f.eks. i form af et administrationsselskab, jf. § 12, stk. 1, 1. led, i lov om en garantifond for skadesforsikringsselskaber.

2.7.2. Erhvervsministeriets overvejelser og den foreslåede ordning

Fondens administration vil, så længe der ikke sker udbetalinger fra Fonden, kunne bestrides med beskeden bistand til bestyrelsen. Samtidig skal Fonden dog uden varsel være i stand til at påtage sig en betydelig administrativ byrde, i det øjeblik der skal udbetales erstatninger m.v. fra Fonden. Det er

derfor en forudsætning for Fondens virke, at Fondens bestyrelse træffer de nødvendige beredskabsmæssige foranstaltninger, så Fonden kan løse de opgaver, den bliver stillet overfor.

Fonden har tidligere indgået aftale med et forsikringsselskab til løsning af Fondens administrative opgaver i forbindelse med udbetaling af erstatninger m.v.

Det har i en årrække vist sig vanskeligt for Fonden at indgå aftale med et forsikringsselskab som administrationsselskab for Fonden. Fonden har haft opgaven som administrationsselskab i udbud, men det har vist sig, at der ikke er egnede forsikringsselskaber, der har ønsket at påtage sig opgaven som administrationsselskab for Fonden.

På den baggrund har Fonden taget kontakt til Erhvervsministeriet for at oplyse om problematikken med, at der ikke er egnede forsikringsselskaber, der byder på opgaven. Fonden har oplyst, at de bl.a. har været i dialog med Forsikring & Pension og i den forbindelse har de forslået en rotationsordning, der indebærer, at de største skadesforsikringsselskaber på skift påtager sig opgaven som administrationsselskab. Den foreslåede rotationsordning vil være subsidiær til udbudsmodellen, og rotationsordningen vil derfor først blive bragt i spil, såfremt der ikke er nogen egnede forsikringsselskaber, der har ønsket at byde på opgaven som administrationsselskab for Fonden.

Derfor er det nødvendigt gennem en ændring af lov om en garantifond for skadesforsikringsselskaber at sikre, at Fonden til alle tider har et administrationsselskab tilknyttet. Dette skal sikre, at forsikringstagerne i et konkursramt forsikringsselskab får den nødvendige hurtige og effektive sagsbehandling ved udbetaling af erstatninger og skadebehandling fra Fonden.

Det foreslås derfor med lovforslaget § 10, nr. 1, at Fondens bestyrelse, som en del af at antage medhjælp, skal forsøge at indgå aftale med et forsikringsselskab som administrationsselskab.

Den foreslåede ændring af vil medføre, at Fonden får pligt til at forsøge at indgå aftale med et forsikringsselskab som administrationsselskab.

Det foreslås desuden med lovforslagets § 10, nr. 1, at Finanstilsynet bliver tillagt beføjelse til på baggrund af objektive kriterier fastsat i loven at udnævne et forsikringsselskab som administrationsselskab for Fonden, hvis det ikke er muligt for Fondens bestyrelse at indgå aftale med et forsikringsselskab som administrationsselskab evt. som følge af et offentligt

udbud. Et forsikringsselskab, der opfylder kriterierne fastsat i loven, vil indgå i en rotationsordning. Derudover vil et forsikringsselskab, der bliver udnævnt af Finanstilsynet som administrationsselskab for Fonden, modtage vederlag for arbejdet forbundet hermed af Fonden.

På nuværende tidspunkt er der tre forsikringsselskaber, der opfylder de forslåede kriterier i den foreslåede § 12 a, stk. 4, nr. 1-5.

Det foreslås derudover med lovforslagets § 10, nr. 2, at der fastsættes en klageadgang for adressaten af Finanstilsynets afgørelser i forbindelse med den foreslåede bestemmelse om, at Finanstilsynet skal tillægges beføjelse til at udnævne et forsikringsselskab som administrationsselskab for Fonden, samt at Finanstilsynet på baggrund af oplæg fra Fonden kan fastsætte størrelsen af vederlaget, som Fonden skal betale til administrationsselskabet, hvis parterne ikke kan blive enige herom.

2.8. Reaktionsmuligheder for Erhvervsstyrelsen i hvidvaskloven, som sat i kraft for Grønland

2.8.1. Gældende ret

Ved anordning nr. 956 af 17. maj 2021 om ikrafttræden for Grønland af lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) blev hvidvaskloven, jf. lov nr. 651 af 8. juni 2017, sat i kraft for Grønland.

Det følger af hvidvaskloven, jf. lovbekendtgørelse nr. 316 af 11. marts 2022, at Erhvervsstyrelsen blandt andet påser overholdelse af hvidvaskloven for visse revisorer og revisionsvirksomheder, visse kunsthandlere samt virksomheder og personer, der erhvervsmæssigt leverer samme ydelser som visse advokater samt visse revisorer og revisionsvirksomheder.

Hvidvaskloven, som sat i kraft for Grønland, indeholder ikke Erhvervsstyrelsens tilsynskompetence for så vidt angår virksomheder og personer, der erhvervsmæssigt leverer samme ydelser som visse advokater samt visse revisorer og revisionsvirksomheder, herunder revisorer, der ikke er godkendt i henhold til revisorloven, skatterådgivere og eksterne bogholdere. Derfor er der ved lov nr. 480 af 12. maj 2023 om ændring af lov om en garantifond for skadesforsikringsselskaber, hvidvaskloven, lov om finansiel virksomhed og forskellige andre love, indsat en ny anordningshjemmel i den danske hvidvasklov, der skal sikre, at de angivne virksomheder og personer ved anordning kan underlægges Erhvervsstyrelsens tilsyn.

Det følger videre af § 59 i den danske hvidvasklov, at disse virksomheder og personer omfattet af Erhvervsstyrelsens tilsynskompetence skal give

Erhvervsstyrelsen de oplysninger, som er nødvendige for styrelsens virksomhed. Herudover følger det af § 60 i den danske hvidvasklov, at Erhvervsstyrelsen, hvis formålet tilsiger det, til enhver tid mod behørig legitimation uden retskendelse, kan få adgang til disse virksomheder og personer, med henblik på indhentelse af oplysninger, herunder ved kontrolbesøg. Disse reaktionsmuligheder er ved en fejl ikke blevet sat i kraft for Grønland.

2.8.2. Erhvervsministeriets overvejelser og den foreslåede ordning

For at sikre, at Erhvervsstyrelsen har tilstrækkelige beføjelser til at sikre overholdelsen af hvidvaskloven, som sat i kraft for Grønland, så bør Erhvervsstyrelsen have samme tilsynsbeføjelser, som de har i henhold til hvidvaskloven i Danmark.

Det foreslås derfor at indsætte et nyt stk. 4 i anordningshjemlen i den danske hvidvasklov. Den foreslåede ændring vil medføre, at anordningshjemlen kan anvendes på ny med henblik på at indsætte en henvisning til § 1, stk. 1, nr. 17, i hvidvasklovens §§ 59 og 60, som sat i kraft for Grønland. Erhvervsstyrelsen får derved de samme beføjelser, når de fører tilsyn efter hvidvaskloven, som sat i kraft for Grønland, som efter den danske hvidvasklovs §§ 59 og 60.

3. Økonomiske og implementeringskonsekvenser for det offentlige

Lovforslagets del om supplerende bestemmelser til forordningen om markeder for kryptoaktiver indeholder ikke skønsbaserede kriterier. Lovforslagets definitioner er i overensstemmelse med definitionerne i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, som lovforslaget supplerer. Denne del af lovforslaget vurderes ikke at have implementeringsmæssige konsekvenser for det offentlige.

Lovforslagets § 10, nr. 2, hvorefter forsikringsselskaber, der er udpeget i henhold til bestemmelserne i lovforslagets § 10, nr. 1, kan klage over udpegelsen eller vederlaget, kan medføre, at Erhvervsankenævnet skal behandle flere klager.

Lovforslaget efterlever princip nr. 1, 4 og 5 for digitaliseringsklarlovgivning.

Lovforslaget efterlever princip nr. 1 og 4, da lovforslaget sikrer sig, at kravene fra DORA-forordningen gælder ensartet for hele finanssektoren. Dette gøres

ved at supplere med nationale regler, der til svarer DORA-reglerne, for de få virksomheder, der ikke er omfattet af DORA-forordningen. Ensretningen er ligeledes i tråd med princip nr. 4 om at skabe sammenhæng på tværs af lovgivningen ved at bruge ensartede begreber.

I forlængelse heraf indebærer lovforslaget desuden, i overensstemmelse med princip nr. 5 om tryg og sikker datahåndtering, at man sikrer et ensartet højt cybersikkerhedsniveau i hele finanssektoren. Implementeringen af DORA-forordningen i sig selv, kan desuden ses som at fremme en tryg og sikker datahåndtering.

4. Økonomiske og administrative konsekvenser for erhvervslivet mv.

OBR vurderer, at lovforslaget medfører administrative konsekvenser for erhvervslivet. Disse konsekvenser vurderes at være under 4 mio. kr., hvorfor de ikke kvantificeres nærmere.

OBR bemærker, at lovforslaget giver hjemmel til udstedelse af bekendtgørelser, som indebærer administrative konsekvenser for erhvervslivet. Disse konsekvenser kan ikke kvantificeres på nuværende tidspunkt, da kravene ikke er endeligt fastlagt.

5. Administrative konsekvenser for borgerne

Lovforslaget vurderes ikke at have administrative konsekvenser for borgerne.

6. Klimamæssige konsekvenser

Lovforslaget har ikke klimamæssige konsekvenser.

7. Miljø- og naturmæssige konsekvenser

Lovforslaget har ikke miljø- og naturmæssige konsekvenser.

8. Forholdet til EU-retten

Lovforslaget implementerer eller supplerer følgende EU-retsakter:

- Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

- Europa-Parlamentets og Rådets forordning af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr.

600/2014, (EU) nr. 909/2014 og (EU) 2016/1011) (DORA-forordningen).

- Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet).

- Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor.

- Lovforslagets § 1, nr. 18-22, implementerer dele af Europa-Parlamentets og Rådets direktiv af 20. maj 2019 om ændring af direktiv 2014/59/EU for så vidt angår kreditinstitutters og investeringsselskabers tabsabsorberings- og rekapitaliseringskapacitet og af direktiv 98/26/EF.

DORA-forordningen forudsætter, at der i national lovgivning vedtages straffebestemmelser for overtrædelse af visse af forordningens bestemmelser og bestemmelser om tvangsbøder for kritiske tredjepartsudbydere, som er omfattet af forordningens kapitel V, 2. afd. Der indføres desuden bestemmelser i den danske lovgivning om kompetente myndigheder og håndhævelse af forordningen i Danmark.

Operatører af finansielle digitale infrastrukturer bliver omfattet af NIS 2-direktivet, som stiller en række krav til de forpligtelser medlemslandene skal skabe hjemmel til i deres nationale lovgivning. Lovændringerne tager sigte på at opfylde disse krav i NIS 2-direktivet. NIS 2-direktivet stiller endvidere en række yderligere krav til medlemslandenes myndigheder. Disse krav opfyldes som udgangspunkt med forretningsgange mv.

De foreslåede bestemmelser i afsnit IX c, jf. lovforslagets § 1, nr. 24, om operatører af finansielle digitale infrastrukturer går videre end NIS 2-direktivets bestemmelser.

9. Hørte myndigheder og organisationer mv.

[Afventer offentlig høring.]

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter	Negative konsekvenser/merudgifter
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Lovforslaget medfører, at Finanstilsynet skal påse overholdelsen af en række nye regler. Dette vil medføre økonomiske konsekvenser for Finanstilsynet.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Ingen
Økonomiske konsekvenser for erhvervslivet	Ingen	Lovforslaget forventes at medføre mindre økonomiske konsekvenser for erhvervslivet.
Administrative konsekvenser for erhvervslivet	Ingen	Lovforslaget forventes at medføre mindre administrative konsekvenser for erhvervslivet.
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslagets § 1, nr. 2-4, 24, 26, 34, 36, 41-43, og 46-48, (ændringer til lov om finansiel virksomhed) § 2, nr. 15, 16, og 21-24, (ændringer til lov om betalinger), § 3, nr. 3, 16, (ændringer lov om kapitalmarkeder), § 4, nr. 2, 3, 5, 10, 13, 10-16, (ændringer til lov om fondsmæglerselskaber og investeringsservice og -aktiviteter), § 5, nr. 2, 4, 8 og 9, (ændringer til lov om forvaltere af alternative investeringsfonde m.v.), § 7 (ændringer til hvidvaskloven), supplerer MiCA. Lovforslagets § 3, nr. 19 og 20, implementerer dele af artikel 1, nr. 5, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2019/2177 af 18. december 2019 om ændring af direktiv 2009/138/EF om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II), direktiv 2014/65/EU om markeder for finansielle instrumenter og af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme (omnibusdirektivet). Lovforslaget implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2021/338 af 16. februar 2021 om	

	ændring af direktiv 2014/65/EU, for så vidt angår oplysningskrav, produktstyring og positionslofter, og af direktiv 2013/36/EU og (EU) 2019/878, for så vidt angår deres anvendelse på investeringsvirksomheder, med henblik på at bidrage til genopretningen efter COVID-19 pandemien. Lovforslagets § 1, nr. 38, supplerer artikel 9 i for 2019/1156/EU om lettere grænseoverskridende distribution af kollektive investeringsinstitutter. Lovforslagets supplerer dele af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor. Lovforslaget implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet). Lovforslaget implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor. Lovforslagets § 7 implementerer ændringer til det 4. hvidvaskdirektiv, jf. den omarbejdede pengeforordning artikel 40.
Er i strid med de principper for implementering af erhvervsrettet EU-regulering/ Går videre end minimumskrav i EU-regulering	Ja X	Nej

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Til nr. 1 (fodnoten i lov om finansiel virksomhed)
Lov om finansiel virksomhed gennemfører i dag dele af NIS-direktivet, herunder bestemmelser om identifikation af operatører af væsentlige tjenester, jf. afsnit VIII i loven, og bestemmelser om Finanstilsynets og Center For Cybersikkerheds orientering af offentligheden om hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere igangværende hændelser, jf. § 354 h.

Det foreslås i *fodnoten* at »dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016 (NIS-direktivet), EU-Tidende 2016, nr. L 194, side 1,« udgår, og at »og dele af Europa-Parlamentets og Rådets direktiv (EU) 2019/2162 af 27. november 2019 om udstedelse af dækkede obligationer og offentligt tilsyn med dækkede obligationer og om ændring af direktiv 2009/65/EF og 2014/59/EU, EU-Tidende 2019, nr. L 328, side 29« ændres til: »dele af Europa-Parlamentets og Rådets direktiv (EU) 2019/2162 af 27. november 2019 om udstedelse af dækkede obligationer og offentligt tilsyn med dækkede obligationer og om ændring af direktiv 2009/65/EF og 2014/59/EU, EU-Tidende 2019, nr. L 328, side 29 og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

Det foreslåede vil medføre, at NIS-direktivet udgår fra fodnoten. Dette foreslås, da dette lovforslag implementerer dele af NIS 2-direktivet, der ophæver NIS-direktivet.

Det foreslåede vil endvidere medføre, at der i fodnoten indsættes en henvisning til, at der med denne lov foretages en gennemførelse af dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor. Denne henvisning tilføjes, idet lovforslaget gennemfører artikel 1 i direktivet, der fastsætter ændringer til Europa-Parlamentets og Rådets direktiv af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer, og artikel 4 i direktivet, der fastsætter ændringer til Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og

investeringsselskaber. Direktivet er et følgedirektiv til DORA-forordningen.

Til nr. 2 (§ 1, stk. 14, i lov om finansiel virksomhed)

Den gældende § 1 i lov om finansiel virksomhed fastsætter lovens anvendelsesområde. Den gældende lov om finansiel virksomhed finder som udgangspunkt ikke anvendelse på udstedere af aktivbaserede tokens, udstedere af e-pengetokens og udbydere af kryptoaktivtjenester.

Det foreslås at indsætte et nyt *stk. 14* i § 1 i lov om finansiel virksomhed, hvorefter kapitel 19 b, som indsat ved lovforslagets § 1, nr. 24, finder anvendelse på fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester.

Den foreslåede bestemmelse fastlægger hvilke bestemmelser i lov om finansiel virksomhed, der skal finde anvendelse på fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester. Visse andre virksomheder kan eksempelvis være enkeltmandsvirksomheder, der i visse sammenhænge ikke betragtes som juridiske personer i dansk ret.

Den foreslåede bestemmelse vil omfatte fysiske og juridiske personer, der udbyder andre kryptoaktiver end aktivbaserede tokens og e-pengetokens til offentligheden eller anmoder om optagelse af disse til handel i EU, udstedere af aktivbaserede tokens, som udbyder disse til offentligheden eller anmoder om optagelse af disse til handel i EU, udstedere af e-pengetokens, som udbyder disse til offentligheden eller anmoder om optagelse af disse til handel i EU og udbydere af kryptoaktivtjenester.

De tilsynsmæssige krav og rammer for disse aktører er i øvrigt fastsat i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og vil finde direkte anvendelse fra de tidspunkter, hvor de relevante bestemmelser i MiCA finder anvendelse.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Til nr. 3 (§ 10, stk. 1, 2. pkt., i lov om finansiel virksomhed)

Det gældende § 10, stk. 1, i lov om finansiel virksomhed fastsætter, hvilke aktiviteter et investeringsforvaltningsselskab må udføre. Afgrænsningen i

bestemmelsen indebærer, at investeringsforvaltningsselskaber efter gældende ret ikke må udføre investeringstjenester eller accessoriske tjenesteydelser med kryptoaktiver.

Det foreslås, at der i *§ 10, stk. 1, 2. pkt.*, efter »§ 10 a« indsættes », § 10 b«.

Den foreslåede ændring vil medføre, at investeringsforvaltningsselskaber fremadrettet må udbyde aktiviteter som nævnt i dette lovforslags § 1, nr. 4, hvorefter der foreslås indført en ny § 10 b, i lov om finansiel virksomhed. Forslaget vil medføre, at et investeringsforvaltningsselskab fremadrettet vil kunne udføre investeringstjenester eller accessoriske tjenesteydelser med kryptoaktiver, hvis de lever op til betingelserne i § 10 b, i lov om finansiel virksomhed.

Ændringen er en konsekvens af, at det i artikel 60, stk. 5, i MiCA, bestemmes, at et investeringsforvaltningsselskab skal kunne udføre disse aktiviteter, såfremt betingelserne angivet i bestemmelsen er opfyldt. Der henvises i øvrigt til bemærkningerne til lovforslagets § 1, nr. 4.

Til nr. 4 (§ 10 b i lov om finansiel virksomhed)

Efter den gældende bestemmelse i § 10, stk. 1, 1. pkt., i lov om finansiel virksomhed, skal en virksomhed have tilladelse som investeringsforvaltningsselskab for at udføre den daglige ledelse af investeringsforeninger og administrere andre UCITS, jf. bilag 6 til lov om finansiel virksomhed. Investeringsforvaltningsselskaber må efter afgrænsningen i § 10, stk. 1, 2. pkt., derudover kun udføre virksomhed som nævnt i § 10, stk. 2, § 10 a og § 28.

Den gældende retstilstand indebærer, at investeringsforvaltningsselskaber ikke kan udføre investeringstjenester eller accessoriske tjenesteydelser med kryptoaktiver.

Det foreslås at indsætte en ny bestemmelse i *§ 10 b*, hvorefter et investeringsforvaltningsselskab kan levere tjenester med kryptoaktiver som angivet i artikel 60, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, svarende til de tjenester, som det specifikt er meddelt tilladelse til i henhold til § 10, hvis selskabet giver Finanstilsynet meddelelse mindst 40 arbejdsdage, inden disse tjenester leveres første gang, sammen med de oplysninger, der er anført i artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Den foreslåede bestemmelse skal sikre, at der ikke i dansk ret er hindringer for, at investeringsforvaltningsselskaber, såfremt de lever op til betingelserne i artikel 60, stk. 7, i MiCA, vil kunne udøve virksomhed som forudsat efter artikel 60, stk. 5, i MiCA. De efter lovforslaget omfattede investeringsforvaltningsselskaber, omfatter administrationsselskaber for investeringsinstitutter efter artikel 60, stk. 5, i MiCA.

Den foreslåede bestemmelse er samtidig en konsekvens af, at udbydere af kryptoaktivtjenester vil blive underlagt Finanstilsynets tilsyn i henhold til MiCA, hvorfor underretning om, at et investeringsforvaltningsselskab påtænker at udøve virksomhed efter § 10 b skal ske til Finanstilsynet.

Den foreslåede bestemmelse fastlægger, at Finanstilsynet er den kompetente myndighed til at vurdere en underretning efter artikel 60, stk. 8, i MiCA.

Et investeringsforvaltningsselskab må ikke begynde at levere kryptoaktivtjenester, så længe underretningen er ufuldstændig.

Investeringsforvaltningsselskaber vil ikke være forpligtede til at ansøge om særskilt tilladelse til at udbyde kryptoaktivtjenester, jf. artikel 59, stk. 1, litra b, i MiCA.

Retten til at levere kryptoaktivtjenester ophæves ved inddragelsen af den tilladelse, der gav virksomheden mulighed for at levere kryptoaktivtjenester uden at skulle indhente en tilladelse i henhold til artikel 59 i MiCA, jf. artikel 60, stk. 11, i MiCA.

Bestemmelsen supplerer artikel 60, stk. 5, i MiCA.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Til nr. 5 (§ 71, stk. 1, nr. 8, i lov om finansiel virksomhed)

§ 71, stk. 1, indeholder nærmere regler om de former for virksomhedsstyring en finansiel virksomhed og en finansiel holdingvirksomhed skal have, herunder eksempelvis betryggende kontrol- og sikringsforanstaltninger på it-området, jf. § 71, stk. 1, nr. 8.

§ 71, stk. 1, gennemfører bl.a. artikel 12, stk. 1, 2. afsnit, litra a, i Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer og artikel 74, stk. 1, i Europa-Parlamentets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed

som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber (CRD IV).

Det foreslås i *§ 71, stk. 1, nr. 8,* at tilføje net- og informationssystemer, der oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede bestemmelse vil medføre, at et investeringsforvaltningsselskab og et penge- og realkreditinstitut skal have betryggende kontrol- og sikringsforanstaltninger hvad angår net- og informationssystemer, der oprettes og styres i overensstemmelse med DORA-forordningen.

DORA-forordning fastsætter ensartede krav til sikkerheden i de net- og informationssystemer, der understøtter finansielle enheders forretningsprocesser.

Ved net- og informationssystem forstå elektronisk kommunikationsnet i form af radiofrekvens- eller kabelbaseret teleinfrastruktur, der anvendes til formidling af tjenester, enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse, jf. § 2, nr. 1, i lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester.

Bestemmelsen er ny og gennemfører dele af artikel 1, nr. 1, og artikel 4, nr. 2, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022, der er et følgedirektiv til DORA, der ændrer i henholdsvis i artikel 12, stk. 1, 2. afsnit, litra a, i Europa-Parlamentets og Rådets direktiv af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer og artikel 74, stk. 1, i CRD.

Til nr. 6 (§ 71, stk. 2, 2. pkt., i lov om finansiel virksomhed)

Det følger af § 71, stk. 2, 2. pkt., at Finanstilsynet kan fastsætte nærmere regler om hændelsesrapportering for de virksomheder, der udpeges som operatører af væsentlige tjenester i medfør af § 307 a i lov om finansiel virksomhed, herunder om, at Finanstilsynet og Center for Cybersikkerhed underrettes ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer.

Bestemmelsen gennemfører artikel 14, stk. 3, i Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer (NIS-direktivet), hvorefter en operatør af væsentlige tjenester hurtigst muligt skal foretage en underretning til den kompetente myndighed eller CSIRT, af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer. En hændelse forstås som værende enhver begivenhed, der har en negativ indvirkning på sikkerheden i en virksomheds net- og informationssystemer. Ved CSIRT forstås en national it-beredskabsenhed, der håndterer hændelser, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU, jf. definitionen heraf i § 2, nr. 17, i lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester. I Danmark er det Forsvarets Efterretningstjeneste, herunder Center for Cybersikkerhed, der er udpeget som CSIRT.

Der henvises i det hele til de specielle bemærkningerne til § 19, nr. 2, i Folketingstidende 2017-18, tillæg A, L 144 som fremsat, side 29-31.

Det foreslås at ophæve *§ 71, stk. 2, 2. pkt.*

Med det foreslåede ophæves den danske implementering af kravene i NIS-direktivets artikel 14, stk. 3, om underretning af hændelser til den kompetente myndighed eller CSIRT. Dette foreslås, da NIS 2-direktivet ophæver NIS-direktivet.

Kravet om underretning af hændelser i artikel 14, stk. 3, i NIS-direktivet bliver erstattet af kravet om indberetning af større it-hændelser til den kompetente myndighed, dvs. Finanstilsynet, jf. § 1, nr. 24, i nærværende lovforslag, i medfør af artikel 19, stk. 1, i DORA-forordningen. DORA-forordningen gælder for finansielle enheder, herunder penge- og realkreditinstitutter, jf. artikel 2, stk. 1, litra a. Når Finanstilsynet modtager en underretning om en større it-hændelse, skal Finanstilsynet rettidigt forelægge nærmere oplysninger om hændelsen for andre myndigheder, for hvem hændelsen er relevant, jf. artikel 19, stk. 6, i DORA-forordningen. Artikel 19, stk. 6, nævner de myndigheder, som Finanstilsynet kan forelægge en hændelse for, herunder CSIRT, dvs. Center for Cybersikkerhed.

Til nr. 7 (§ 72 a, stk. 4, i lov om finansiel virksomhed)

§ 72 a i lov om finansiel virksomhed fastsætter regler om outsourcing for pengeinstitutter, sparevirksomheder, realkreditinstitutter og investeringsforvaltningsselskaber.

Det fremgår af stk. 1, at Pengeinstitutter, sparevirksomheder, realkreditinstitutter og investeringsforvaltningsselskaber kan outsource en proces, en tjenesteydelse eller en aktivitet, som virksomheden ellers selv ville udføre, til en leverandør.

Af stk. 2 følger det, at Finanstilsynet kan træffe afgørelse om, at outsourcingvirksomheders outsourcing skal bringes til ophør inden for en af Finanstilsynet nærmere fastsat frist, hvis outsourcingkontrakten eller dennes parter ikke opfylder reglerne fastsat i medfør af stk. 3.

I henhold til stk. 3, kan erhvervsministeren fastsætte nærmere regler om outsourcing for disse virksomheder, herunder bl.a. vedrørende outsourcingvirksomheders ledelsesordninger, ansvar, risikostyring, overvågning, kontrol og rapportering i tilknytning til outsourcing til en leverandør samt vedrørende krav til indholdet af kontrakten. Bemyndigelsen er udnyttet til at udstede bekendtgørelse nr. 973 af 22. juni 2022 om outsourcing for kreditinstitutter m.v.

Når DORA-forordningen finder anvendelse, vil der ikke længere være beføjelse til at fastsætte nationale regler om styring af tredjepartsrisici på det digitale operationelle område, herunder regler om outsourcing.

Det foreslås derfor at indsætte *§ 72 a, stk. 4,* i lov om finansiel virksomhed, hvorefter stk. 1-3 ikke skal finde anvendelse på det digitale operationelle område.

Den foreslåede bestemmelse vil indebære, at reglerne om outsourcing i § 72 a, stk. 1 og 2, samt bemyndigelsesbestemmelsen til at erhvervsministeren kan fastsætte nærmere regler i medfør af stk. 3, ikke længere vil omfatte outsourcing på det digitale operationelle område. Outsourcing på det digitale operationelle område vil i stedet fremover blive reguleret i kapitel V, afdeling I, i DORA-forordningen.

Bestemmelsen vil også indebære behov for, at Finanstilsynet ændrer bekendtgørelse nr. 973 af 22. juni 2022 om outsourcing for kreditinstitutter m.v., så bekendtgørelsen ikke kommer til at omfatte outsourcing på det digitale operationelle område.

Til nr. 8 (§ 72 c i lov om finansiel virksomhed)

Det fremgår af § 72 c, at regler fastsat i medfør af § 72 a, stk. 3, ikke gælder for virksomhedernes autentifikation af brugere ved anvendelse af MitID-løsningen, jf. lov om MitID og NemLog-in.

I henhold til § 72 a, stk. 3, kan erhvervsministeren fastsætte nærmere regler for pengeinstitutter, sparevirksomheder, realkreditinstitutter og investeringsforvaltningsselskaber om outsourcing, herunder bl.a. vedrørende outsourcingvirksomheders ledelsesordninger, ansvar, risikostyring, overvågning, kontrol og rapportering i tilknytning til outsourcing til en leverandør samt vedrørende krav til indholdet af kontrakten. Bemyndigelsen er udnyttet til at udstede bekendtgørelse nr. 973 af 22. juni 2022 om outsourcing for kreditinstitutter m.v.

Når DORA-forordningen finder anvendelse, vil der ikke længere være beføjelse til at fastsætte nationale regler om styring af tredjepartsrisici på det digitale operationelle område, herunder regler om outsourcing.

Det foreslås derfor at ophæve *§ 72 c* i lov om finansiel virksomhed.

Virksomhedernes outsourcing af autentifikation af brugere ved anvendelse af MitID-løsningen angår det digitale operationelle område og vil derfor fremadrettet skulle følge DORA-forordningens regler. Det foreslåede skal ses i denne sammenhæng.

Til nr. 9 (§ 80, stk. 5, i lov om finansiel virksomhed)

§ 80, stk. 4, i lov om finansiel virksomhed indeholder et eksponeringsforbud.

§ 80, stk. 5, fastsætter, at eksponeringsforbuddet i stk. 1 ikke finder anvendelse i forbindelse med deltagelse i bestyrelserne i en række angivne virksomheder, herunder i Landbrugets FinansieringsBank A/S

Landbrugets FinansieringsBank A/S er ophørt i 2017.

Det foreslås at ændre i *§ 80, stk. 5*, så henvisningen til »Landbrugets FinansieringsBank A/S« udgår.

Den foreslåede ændring vil medføre, at Landbrugets FinansieringsBank A/S ikke længere vil fremgå af § 80, stk. 5.

Til nr. 10 (§ 124, stk. 2, i lov om finansiel virksomhed)

Det følger af § 124, stk. 2, i lov om finansiel virksomhed, at solvensbehovet opgøres som det tilstrækkelige kapitalgrundlag i procent af den samlede risikoeksponering.

Penge- og realkreditinstitutter er i dag underlagt krav om at opretholde et individuelt solvensbehov, jf. § 124, stk. 2-8, samt et kombineret kapitalbufferkrav, jf. § 125 a. Solvensbehovet består af søjle-I kapitalgrundlagskravet i artikel 92, stk. 1, litra a-c, og minimumskapitalkravet i artikel 93 i CRR, samt et eventuelt søjle II-tillæg, hvis instituttets risici ikke er tilstrækkelig dækket af søjle I-kravet. Parallelt med de risikobaserede krav gælder gearingsgradskravet på 3 pct., jf. artikel 92, stk. 1, litra d, i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 (CRR). Gearingsgraden opgøres som kernekapital i forhold til den ikke risikovægtede eksponering, jf. artikel 429-429g i CRR. Et eventuelt tillæg som følge af risiko for overdreven gearing skal lægges til gearingsgradskravet og ikke de risikobaserede kapitalgrundlagskrav.

Det foreslås i *§ 124, stk. 2,* at indsætte som *3. pkt.:* »Den del af solvensbehovet, der vedrører overdreven risiko for gearing opgøres i procent af den samlede ikke-risikovægtede eksponering.«, og i *§ 124, stk. 2, 3. pkt.,* der bliver 4. pkt., at indsætte efter »i artikel 93«: »eller gearingsgradskravet efter artikel 92, stk. 1, litra d,«.

Det foreslåede præciserer, hvordan den del af solvensbehovet, der vedrører risiko for overdreven gearing, opgøres. Formålet er at tydeliggøre gældende retspraksis, så ordlyden af bestemmelsen ikke giver anledning til tvivl.

Til nr. 11 (§ 124, stk. 3, i lov om finansiel virksomhed)

Det følger af § 124, stk. 3, i lov om finansiel virksomhed, at Finanstilsynet kan fastsætte et individuelt solvenskrav i form af et tillæg til kapitalgrundlagskravet, der fremgår af artikel 92, stk. 1, litra c, i CRR. Dette solvenskrav vil være et udtryk for Finanstilsynets vurdering af instituttets tilstrækkelige kapitalgrundlag i procent af den samlede risikoeksponering.

Det foreslås i *§ 124, stk. 3, 1. pkt.,* efter: »92, stk. 1, litra c,« at indsætte: »eller til gearingsgradskravet, der fremgår af artikel 92, stk. 1, litra d,«, og i *§ 124, stk. 3, 2. pkt.,* efter »samlede risikoeksponering« at indsætte: »og i procent af den ikke-risikovægtede eksponering, hvis solvenskravet vedrører risiko for overdreven gearing«.

Det foreslåede præciserer, at den del af solvensbehovet der vedrører risiko for overdreven gearing skal opgøres som det tilstrækkelige kapitalgrundlag i procent af den samlede ikke-risikovægtede eksponering, jf. de foreslåede

tilpasninger til § 124, stk. 2, og § 124 a, stk. 1, 2. pkt., jf. lovforslagets § 1, nr. 10 og 13. Det foreslåede har til formål at tydeliggøre gældende retspraksis, så ordlyden af bestemmelsen ikke giver anledning til tvivl.

Til nr. 12 (§ 124 a, stk. 1, 1. pkt., i lov om finansiel virksomhed)

Det følger af § 124 a, stk. 1, i lov om finansiel virksomhed, at Finanstilsynet årligt fastsætter et vejledende niveau af yderligere kapitalgrundlag for de individuelle kreditinstitutter og meddeler dette til kreditinstitutterne.

Finanstilsynet meddeler ved afgørelse institutterne det yderligere kapitalgrundlag, som instituttet skal opretholde, ud over det kombinerede kapitalbufferkrav, jf. § 125 a, for at kunne tåle det hårde stressscenarie i Finanstilsynets tilsynsmæssige stresstest uden at bryde med det individuelle solvensbehov, jf. § 124, stk. 2, eller med det individuelle solvenskrav, jf. § 124, stk. 3.

Det kombinerende kapitalbufferkrav består af kapitalbevaringsbufferen, den kontracykliske buffer, SIFI-bufferen og den systemiske buffer.

Det fremgår af bemærkningerne til § 124 a, stk. 1, at det vejledende niveau af yderligere kapitalgrundlag godt kan være nul, såfremt instituttets kombinerede kapitalbufferkrav overstiger kapitaleffekten af Finanstilsynets hårde stressscenarie, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 94.

Dette er imod hensigten imidlertid ikke i overensstemmelse med de europæiske retningslinjer vedrørende opgørelse af P2G – SREP (Supervisory Review and Evaluation Process), jf. EBA/GL/2022/03.

Det fremgår af de europæiske SREP-retningslinjer, at kun kapitalbevaringsbufferen, jf. 125 a, stk. 2, modregnes kapitaleffekten af det tilsynsmæssige hårde stressscenarie. Baseret på en case-by-case vurdering kan den kontracykliske buffer, jf. §125 a stk. 3, undtagelsesvist også modregnes kapitaleffekten. SIFI-bufferen og den systemiske buffer skal imidlertid ikke modregnes ved opgørelsen af kapitaleffekten.

Det foreslås i *§ 124 a, stk. 1, 1. pkt.*, at ændre »meddeler« til: »informerer«.

Der er alene tale om en sproglig ændring af lovteksten, som har til formål at give mulighed for at korrigere de tidligere bemærkningerne om opgørelse af P2G.

Det forslåede, hvor P2G fremover som udgangspunkt vil blive opgjort som kapitaleffekten i stress fratrukket kapitalbevaringsbuffer, er en ændring af dansk praksis vedrørende fastsættelse af det vejledende niveau. I overensstemmelse med SREP kan der derudover være særlige tilfælde, hvor mere kvalitative justeringer til opgørelsen af P2G er nødvendige. Det kan f.eks. være som følge af udformningen af stresstest eller institutionsspecifikke karakteristika. Den foreslåede ændring af bemærkningerne vil medføre, at dansk praksis fremover vil være i overensstemmelse med de europæiske retningslinjer.

Finanstilsynet har og vil fortsat i vurderingen af institutternes kapitalgrundlag inddrage, om institutternes kapitalmålsætning sættes på et fornuftigt niveau, som også sikrer, at institutterne ikke forventes at bryde med kapital- og bufferkravene i perioder med stress. Finanstilsynet indleder en dialog med institutterne, hvis ikke institutternes kapitalmålsætning vurderes at være fastsat på et fornuftigt niveau. Implementeringen af det vejledende niveau af yderligere kapitalgrundlag i 2020 har ikke ændret ved denne tilsynspraksis, da kapitalmålsætningen har udgjort et øvre mål, som institutterne har navigeret efter. Det skyldes, at kapitalmålsætningen ikke inkluderer den kontracykliske buffer, dvs. den buffer kan modregnes den stresseffekt, som kapitalmålsætningen opgøres ud fra. Den kontracykliske buffer har i perioden ligget på et niveau mellem 0-2,5 procentpoint. Dermed har kapitalmålsætningen udgjort et højere eller som minimum det samme mål som P2G, hvor det er kapitalbevaringsbufferen på 2,5 pct., der modregnes i stresseffekten. Den ændring af praksis, som forslås her i forhold til opgørelsen af P2G, ville dermed ikke historisk have haft nogen reel betydning. De nuværende niveauer for den kontracykliske buffer og kapitalbevaringsbufferen medfører, at P2G-målsætningen og kapitalmålsætningen kommer tæt på hinanden, men forskellen imellem dem varierer med størrelsesforholdet mellem de to buffere.

Det vil fortsat være sådan, at Finanstilsynet alene meddeler et institut et vejledende niveau af yderligere kapitalgrundlag, hvis instituttets faktiske kapitalisering eller kapitalmålsætning er utilstrækkelig.

Til nr. 13 (§ 124 a, stk. 1, 2. pkt., i lov om finansiel virksomhed)

Det følger af § 124 a, stk. 1, i lov om finansiel virksomhed, at Finanstilsynet årligt fastsætter et vejledende niveau af yderligere kapitalgrundlag for de individuelle kreditinstitutter og meddeler dette til kreditinstitutterne. Det vejledende niveau af yderligere kapitalgrundlag baseres på en tilsynsmæssig stresstest og opgøres i procent af den samlede risikoeksponering.

Det fremgår af bemærkningerne til bestemmelsen, at der i § 124 a sondres mellem risici, der angår risikoen for overdreven gearing og risici, der ikke angår risikoen for overdreven gearing. Jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 94.

Det foreslås det i *§ 124 a, stk. 1, 2. pkt.*, efter: »risikoeksponering« at indsætte: »og i procent af den samlede ikke-risikovægtede eksponering«

Det foreslåede har til formål at tydeliggøre gældende retspraksis, så ordlyden ikke giver anledning til tvivl, jf. også de foreslåede tilpasninger til § 124, stk. 2 og 3, jf. lovforslagets § 1, nr. 10 og 11.

Til nr. 14 (§ 124 a, stk. 3, i lov om finansiel virksomhed)

Det følger af § 124 a, stk. 3, i lov om finansiel virksomhed, at den del af det vejledende niveau af yderligere kapitalgrundlag, som er fastsat for at tage højde for risikoen for overdreven gearing, skal opfyldes med egentlig kernekapital.

Det følger af EBA's retningslinjer for fælles procedurer og metoder for tilsyns- og evalueringsprocessen (SREP), at den del af det vejledende niveau af yderligere kapitalgrundlag, der dækker risikoen for overdreven gearing, bør kunne opfyldes med kernekapital, jf. EBA/GL/2022/03. Retningslinjerne angiver derfor en lempeligere tilgang end § 124 a, stk. 3.

Det foreslås i *§ 124 a, stk. 3*, at »egentlig« og »egentlige« udgår.

Det foreslåede vil medføre, at den del af det vejledende niveau af yderligere kapitalgrundlag, der dækker risikoen for overdreven gearing, skal opfyldes med kernekapital, og ikke udelukkende egentlig kernekapital. Ændringen bringer den danske praksis til opfyldelse af den del af det vejledende niveau af yderligere kapitalgrundlag, der dækker risikoen for overdreven gearing, i overensstemmelse med de europæiske retningslinjer.

Til nr. 15 (§ 125 d, stk. 1, i lov om finansiel virksomhed)

Det følger af § 125 d, stk. 1, i lov om finansiel virksomhed, at penge- og realkreditinstitutterne skal sende en række oplysninger til Finanstilsynet, når det pågældende institut agter at foretage en handling omfattet af § 125 d, stk. 3, nr. 1-3.

§ 125 d, stk. 3, nr. 1-3, er ved lov nr. 2110 af 22. december 2020 rykket til § 125 d, stk. 5, nr. 1-3. Ved samme lov blev der i § 125 b, stk. 3, der blev stk. 5, indsat en forpligtelse for penge- og realkreditinstitutter til ikke at

foretage en række handlinger, hvis de bryder med gearingsbufferkravet, førhen at virksomheden har opgjort det maksimale udlodningsbeløb og underrettet Finanstilsynet i medfør af § 125 d. Der blev ikke samtidig foretaget en konsekvensrettelse af § 125 d, stk. 1, der fastsætter for hvilke oplysninger, der skal sendes til Finanstilsynet i sådanne tilfælde.

Det foreslås i *§ 125 d, stk. 1,* efter »§ 125 a, stk. 1,« at indsætte: »eller gearingsgradbufferkravet, jf. artikel 92 stk. 1, litra a, hvis gearingsgradsbufferkravet finder anvendelse,«, og at ændre »§ 125 b, stk. 3,« til: »§ 125 b, stk. 5,«.

Med det foreslåede tager henvisningen til § 125 b højde for de ændringer, der blev foretaget af ved § 1, nr. 39 og 42, i lov nr. 2110 af 22. december 2020.

Til nr. 16 (§ 199, stk. 12, 2. pkt., i lov om finansiel virksomhed)

Det fremgår af § 199, stk. 12, 2. pkt., i lov om finansiel virksomhed, at Finanstilsynet kan fastsætte bestemmelser om intern revision og om systemrevisionens gennemførelse i fælles datacentraler. Finanstilsynet har i dag fastsat regler herom i bekendtgørelse nr. 1581 af 22. december 2022 om systemrevisionens gennemførelse i fælles datacentraler m.fl.

Ved systemrevision forstås intern og ekstern revision af, om de generelle it-kontroller fungerer betryggende. Ved de generelle it-kontroller forstås styringen af den grundlæggende it-sikkerhed, men ikke sikkerheden i specifikke it-systemer.

Det foreslås at ophæve *§ 199, stk. 12, 2. pkt.,* i lov om finansiel virksomhed.

Bestemmelsen er en konsekvens af, at Finanstilsynet med lovforslagets § 1, nr. 24, foreslås nye regler i § 333 – 333 p, i lov om finansiel virksomhed for operatører af finansielle digitale infrastrukturer, der fremover vil omfatte og regulere fælles datacentraler. De gældende regler for fælles datacentraler foreslås derfor ophævet.

Finanstilsynets bemyndigelsen til at fastsætte nærmere regler om den interne og eksterne systemrevision i operatører af finansielle digitale infrastrukturer, herunder for fælles datacentraler, foreslås med lovforslaget fremover at følge af § 333 p, stk. 1, litra d, i lov om finansiel virksomhed.

Til nr. 17 (§ 224, stk. 1, nr. 1, i lov om finansiel virksomhed)

Det gældende § 224, stk. 1, nr. 1, i lov om finansiel virksomhed fastsætter, at Finanstilsynet kan inddrage en virksomheds tilladelse som pengeinstitut, realkreditinstitut, investeringsforvaltningsselskab og forsikringsselskab, hvis virksomheden gør sig skyldig i grove eller gentagne overtrædelser af lov om finansiel virksomhed samt en række andre love og EU-retsakter på det finansielle område.

Det foreslås i *§ 224, stk. 1, nr. 1,* efter »om markeder for finansielle instrumenter« at indsætte »og Europa-Parlamentets og Rådets (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

Den foreslåede bestemmelse vil medføre, at Finanstilsynet vil kunne inddrage en virksomheds tilladelse som pengeinstitut eller investeringsforvaltningsselskab, hvis virksomheden gør sig skyldig i grove eller gentagne overtrædelser af MiCA.

Der forudsættes en høj grad af væsentlighed, hvis inddragelse af tilladelse skal finde sted med henvisning hertil. Vurderingen skal foretages på baggrund af overtrædelsens grovhed og de risici, det medfører for forbrugere, samfundet og den finansielle stabilitet. Der må tages hensyn til overtrædelsens karakter, omfang, tidsmæssige aspekt osv. En afgørelse om inddragelse af en virksomheds tilladelse er af indgribende karakter for virksomheden Medmindre forholdet er af meget væsentlig karakter, eller inddragelsen sker efter anmodning fra virksomheden, forudsættes det derfor, at inddragelse af tilladelse typisk kun bliver aktuel, efter der har været givet frist til berigtigelse af forholdet, og at berigtigelse ikke er sket.

Til nr. 18 (§ 267 a, stk. 2, i lov om finansiel virksomhed)

Den gældende § 267 a, stk. 2, fastsætter, at en afviklingsenhed, der er et globalt systemisk vigtigt finansielt institut (G-SIFI) eller en væsentlig dattervirksomhed af et G-SIFI i et tredjeland, skal opfylde krav om nedskrivningsegnede passiver med kapitalgrundlag, supplerende kapitalinstrumenter og nedskrivningsegnede forpligtelser, der er omfattet af § 267 a, stk. 1, nr. 2-4, og som opfylder kravene i artikel 92 a eller 92 b i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter (CRR).

Bestemmelsen implementerer artikel 45 b, stk. 1, 2. afsnit, i BRRD, jf. Folketingstidende 2021-21, Tillæg A, L 109 som fremsat, side 152.

Efter § 267 a, stk. 2, skal de nedskrivningsegnede passiver dog opfylde kravene i artikel 92 a og artikel 92 b. Disse artikler indeholder krav til selve

virksomhederne og ikke de nedskrivningsegnede forpligtelser. Bestemmelsen implementerer derfor ikke direktivet korrekt.

Det foreslås derfor i *§ 267 a, stk. 2,* at ændre »der er omfattet af stk. 1, nr. 2-4, og som opfylder kravene i artikel 92 a eller 92 b i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter«, til: »forpligtelser, der opfylder betingelserne i artikel 72 a, artikel 72 b, artikel 72 c og artikel 72 d i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter som opgjort efter de fradrag, som er angivet i artikel 72 e i nævnte forordning, eller forpligtelser, der er omfattet af stk. 1, nr. 3 og 4, dog således at forpligtelserne skal opfylde samme krav som efter dette stykke med undtagelse af betingelsen i artikel 72 a, stk. 2, litra l«.

Den foreslåede ændring vil medføre, at henvisningen til artikel 92 a og 92 b i CRR udgår.

Den foreslåede ændring vil endvidere medføre, at nedskrivningsegnede passiver skal opfylde de krav, som er fastsat i artikel 72 a-72 d i CRR, og at der ved opgørelsen af de nedskrivningsegnede forpligtelser skal ske de fradrag, der er nævnt i CRR artikel 72 e.

De omfattede virksomheder vil fortsat kunne anvende forpligtelser, der er omfattet af § 267 a, stk. 1, nr. 3 og 4, hvis forpligtelserne lever op til kravene i artikel 72 a-72 d, med undtagelse af artikel 72 a, stk. 2, litra l, da forpligtelserne i § 267 a, stk. 1, nr. 3 og 4, har derivatkomponenter.

Til nr. 19 (§ 269 a, stk. 3, nr. 2, i lov om finansiel virksomhed)

Den gældende § 269 a, stk. 3, nr. 2, fastsætter, at Finanstilsynet ved sin vurdering af, hvorvidt en virksomheds udlodning skal begrænses, jf. § 269, stk. 1, sammen med de øvrige hensyn i § 269, stk. 3, skal tage hensyn til udviklingen i virksomhedens økonomiske situation og sandsynligheden for, at virksomheden inden for en overskuelig fremtid opfylder betingelserne for afvikling.

Bestemmelsen implementerer artikel 16 a, stk. 2, 1. afsnit, i BRRD, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 184-185. Artiklen 16 a, stk. 2, 1. afsnit i BRRD indeholder dog en betingelse om, at virksomheden indenfor en overskuelig fremtid bliver nødlidende eller forventeligt nødlidende, hvilket ikke følger af formuleringen i den gældende § 259 a, stk. 3, nr. 2.

Det foreslås derfor i *§ 269 a, stk. 3, nr. 2,* at ændre »opfylder betingelserne for afvikling« til: »bliver nødlidende eller forventeligt nødlidende, jf. § 224 a«.

Den foreslåede ændring vil medføre, at Finanstilsynet fremadrettet skal tage hensyn til sandsynligheden for, at virksomheden inden for en overskuelig fremtid bliver nødlidende eller forventeligt nødlidende, jf. § 224 a, fremfor om virksomheden opfylder betingelserne for afvikling.

Det foreslåede har til formål at sikre en tekstnær implementering, således at hensynet i § 269 a, stk. 3, nr. 3, svarer til hensynet i artikel 32, stk. 2, 1. afsnit, litra b, i BRRD.

Bliver virksomhedens økonomiske situation forværret af den manglende opfyldelse, taler det for, at Finanstilsynet begrænser virksomhedens udlodning til det maksimale udlodningsbeløb. Er det ikke tilfældet, taler det for, at Finanstilsynet ikke begrænser virksomhedens udlodning til det maksimale udlodningsbeløb.

Vil virksomheden inden for en overskuelig fremtid blive nødlidende eller forventeligt nødlidende, taler det for, at Finanstilsynet begrænser virksomhedens udlodning til det maksimale udlodningsbeløb. Er det ikke tilfældet, taler det for, at Finanstilsynet ikke begrænser virksomhedens udlodning til det maksimale udlodningsbeløb. Betingelserne for, hvornår en virksomhed er nødlidende eller forventeligt nødlidende fremgår af § 224 a og omfatter overordnet følgende tre tilfælde: Når instituttet ikke kan opretholde sin tilladelse, herunder ikke opfylder sit kapitalkrav, når instituttet har alvorlige likviditetsproblemer, eller når instituttet modtager ekstraordinær finansiel støtte fra det offentlige.

Det er Finanstilsynet, der vurderer om virksomhedens økonomiske situation og sandsynligheden for, at virksomheden inden for en overskuelig fremtid opfylder betingelserne for afvikling, taler for eller imod en begrænsning af virksomhedens udlodning til det maksimale udlodningsbeløb.

Til nr. 20 (§ 272, stk. 8 og 9, i lov om finansiel virksomhed)

Det foreslås i *§ 272, stk. 8,* at kapitalejere og kreditorer, hvis krav er blevet nedskrevet eller konverteret i henhold til § 272, stk. 1, ikke må lide større tab end ved konkursbehandling af virksomheden eller enheden under afvikling.

Det foreslås i *§ 272, stk. 9,* at Finanstilsynets vurdering efter stk. 8 foretages på baggrund af værdiansættelsen i § 8 i lov om restrukturering og afvikling

af visse finansielle virksomheder. Værdiansættelsen foretages af Finansiel Stabilitet efter anmodning fra Finanstilsynet. Konstateres det, at en kapitalejer eller kreditor, herunder Garantiformuen, har lidt større tab, end den ville have gjort ved konkursbehandling af virksomheden eller enheden, betales forskellen af Afviklingsformuen.

De foreslåede bestemmelser er nye og skal implementere artikel 59, stk. 1, 3. afsnit, i BRRD for så vidt angår Finanstilsynets nedskrivnings- og konverteringsbeføjelser, jf. § 272, stk. 1. Der er tale om en direktivnær implementering.

Princippet om, at ingen kreditorer eller aktionærer må stilles økonomisk værre i afvikling, end hvis der var tale om en konkurssituation (det såkaldte no-creditor-worse-off-princip) er et afgørende princip i krisehåndtering. Bestemmelsen sikrer, at princippet overholdes ved Finanstilsynets nedskrivning eller konvertering i henhold til § 272, stk. 1, på samme måde som det allerede er tilfældet for isolerede nedskrivninger eller konverteringer, som foretages af Finansiel Stabilitet uden for afviklingssituationer efter § 18 a i lov om restrukturering og afvikling af visse finansielle virksomheder.

Til nr. 21 (§ 274, stk. 3, i lov om finansiel virksomhed)

Efter den gældende § 274, stk. 3, finder kravet om kontraktmæssig anerkendelse af bail-in, jf. § 274, stk. 1, ikke anvendelse, hvis forpligtelsen er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder, eller hvis forpligtelsen er et berettiget indskud, jf. § 2, nr. 7, i lov om restrukturering og afvikling af visse finansielle virksomheder.

Bestemmelsen har til hensigt at implementere artikel 55, stk. 1, 1. afsnit, i BRRD direktivnært, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 199-200. Bestemmelsen omfatter imidlertid alle berettigede indskud, mens artikel 55, stk. 1, 1. afsnit, litra b, i BRRD alene omfatter indskud som omhandlet i BRRD artikel 108, litra a.

Det foreslås derfor at nyaffatte *§ 273, stk. 3,* således, at stk. 1 ikke finder anvendelse, hvis 1) forpligtelsen er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder, eller 2) forpligtelsen er en del af et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, jf. § 2, nr. 19 i lov om restrukturering og afvikling af visse finansielle virksomheder, og overstiger beløbsgrænsen for dækkede indskud, jf. § 9 i lov om en indskyder- og investorgarantiordning, eller 3) forpligtelsen ville være et

berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, hvis ikke det var foretaget gennem filialer af institutter, der er etableret inden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område, når filialen er beliggende uden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område

Den foreslåede ændring vil indskrænke undtagelsen for så vidt angår berettigede indskud, således at den fremover alene vil gælde den del af berettigede indskud fra fysiske personer, mikrovirksomheder eller små eller mellemstore virksomheder, som defineret i § 2, nr. 19, i lov om restrukturering og afvikling af visse finansielle virksomheder, som overstiger beløbsgrænsen for dækkede indskud, jf. § 9 i lov om en indskyder- og investorgarantiordning.

Det foreslåede vil ligeledes medføre, at undtagelsen gælder forpligtelser, som ville være berettigede indskud fra samme kreds af fysiske personer og virksomheder, hvis de ikke var foretaget gennem filialer af institutter, der er etableret inden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område, når filialen er beliggende uden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område.

Den foreslåede ændring har til formål at bringe undtagelsen om anerkendelse af kontraktmæssig bail-in i § 274, stk. 1, i overensstemmelse med artikel 55, stk. 1, 1. afsnit, litra b, i BRRD.

Forpligtelser, der er undtaget fra bail-in, kan ikke nedskrives eller konverteres. På den baggrund gælder kravet i stk. 1 ikke kontrakter vedrørende disse forpligtelser.

Berettigede indskud er indestående beløb på en konto i et pengeinstitut m.v., som ikke er udelukket fra dækning efter § 13 i lov om en indskyder- og investorgarantiordning. Dækkede indskud, jf. §§ 9 og 10 i lov om en indskyder- og investorgarantiordning, udgør den del af det berettigede indskud, som er dækket af Garantiformuen. Definitionen af dækkede indskud følger af bemærkningerne til § 7, stk. 8, i lov om en indskyder- og investorgarantiordning, jf. Folketingstidende 2014-15, tillæg A, L 105 som fremsat, side 112. Den tidligere gældende henvisning til § 2, nr. 7, i lov om restrukturering af visse finansielle virksomheder er udeladt i den foreslåede bestemmelse, idet bestemmelsen henviser til den nævnte § 7, stk. 8, i lov om en indskyder- og investorgarantiordning, som ikke i sig selv definerer dækkede indskud. Med lovforslaget indsættes derfor en mere præcis

henvisning til dækkede indskud. Der er ikke tilsigtet nogen materiel ændring på dette punkt.

Det dækkede indskud kan være mindre end det berettigede indskud som følge af de fastsatte maksimumsgrænser for dækning. Dækkede indskud er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder.

Til nr. 22 (§ 275, stk. 1, i lov om finansiel virksomhed)

Efter § 275, stk. 1, skal en virksomhed underrette Finanstilsynet, hvis det ikke er muligt at opfylde § 274, stk. 1, om kontraktmæssig anerkendelse af bail-in, i forhold til en kontrakt vedrørende en forpligtelse omfattet af konkurslovens § 97. Underretningen skal angive kategorien af forpligtelsen og begrundelsen for, at det ikke er muligt at indføre kontraktbestemmelsen.

Bestemmelsen implementerer artikel 55, stk. 2, 1. afsnit, 1. pkt., og stk. 2, 4. afsnit, i BRRD, jf. Folketingstidende 2020-21, tillæg A, L 109 som fremsat, side 201. Ifølge artikel 55, stk. 2, 4. afsnit, i BRRD, finder bestemmelsen ikke anvendelse på passiver en række forpligtelser, hvis disse indeholder hybride kernekapitalinstrumenter, supplerende kapitalinstrumenter og gældsinstrumenter som omhandlet i artikel 2, stk. 1, nr. 48, nr. ii, hvis disse instrumenter er usikrede passiver.

§ 275, stk. 1, henviser til konkurslovens § 97, som omhandler simple krav, f.eks. almindelige fakturakrav for indkøb af varer og tjenesteydelser. Det er ifølge bemærkningerne til § 275, stk. 1, hensigten, at bestemmelsen alene skal finde anvendelse på sådanne forpligtelser. Hybride kernekapitalinstrumenter og supplerende kapitalinstrumenter er efterstillet simple krav, som er omfattet af konkurslovens § 97, hvorfor de er udelukket fra bestemmelsens anvendelsesområde. For så vidt angår gældsinstrumenter som omhandlet i artikel 2, stk. 1, nr. 48, nr. ii, defineres disse som obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld. Sådanne instrumenter vil, hvis de er omfattet af konkurslovens § 97, definitorisk være usikrede. Indehavere af fordringer med sikkerhed i pant vil således kunne søge fyldestgørelse i pantet ved debitors betalingsmisligholdelse. Dermed har indehaverne ikke i udgangspunktet et krav efter konkurslovens § 97. Den nuværende formulering af § 275, stk. 1, indebærer således, at usikrede gældsinstrumenter vil kunne undtages fra kravet om kontraktmæssig anerkendelse af bail-in.

Det foreslås derfor i *§ 275, stk. 1,* efter »konkurslovens § 97«: at indsætte », med undtagelse af usikrede obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld«.

Det foreslåede vil indskrænke anvendelsesområdet for § 275, stk. 1, til forpligtelser omfattet af konkurslovens § 97, som ikke er usikrede obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld.

Den foreslåede bestemmelse har til formål at bringe undtagelsen i § 275, stk. 1, i overensstemmelse med artikel 55, stk. 2, 4. afsnit i BRRD.

Til nr. 23 (Afsnit VIII a i lov om finansiel virksomhed)

Afsnit VIII indeholder regler om identifikation af operatører af væsentlige tjenester.

Det fremgår således af § 307 a, stk. 1, at Finanstilsynet mindst hvert andet år udpeger de penge- og realkreditinstitutter, der er operatører af væsentlige tjenester. Det fremgår af stk. 2, hvilke kriterier Finanstilsynet skal lægge vægt på i forbindelse med udpegningen efter stk. 1. Videre fremgår det af stk. 3, at Finanstilsynet på sin hjemmeside offentliggør, hvilke penge- og realkreditinstitutter, der er udpeget som operatører af væsentlige tjenester. Til sidst fremgår det af stk. 4, at Finanstilsynet kan fastsætte nærmere regler om udpegningen og kriterierne herfor. Det fremgår også af bestemmelsen, at Finanstilsynet udarbejder en liste over tjenester.

Bestemmelsen gennemfører NIS-direktivets artikel 5, stk. 1-3 og stk. 5, hvorefter medlemsstaterne identificerer operatører af væsentlige tjenester ud fra, at de tjenester der leveres er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesterne afhænger af net- og informationssystemer, og at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesterne.

Med en hændelse forstås enhver begivenhed, der har en negativ indvirkning på sikkerheden i en operatørs net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Der henvises i det hele til de specielle bemærkningerne til § 19, nr. 3, i Folketingstidende 2017-18, tillæg A, L 144 som fremsat, side 31.

Det foreslås derfor at ophæve *afsnit VIII.*

Det foreslåede ophæver en række bestemmelser, der implementerer NIS-direktivet. Dette foreslås, da NIS 2-direktivet ophæver NIS-direktivet, herunder reglerne i artikel 5 om medlemsstaternes identifikation af operatører af væsentlige tjenester og kriterierne herfor.

Til nr. 24 (Afsnit IX a-IX c i, i lov om finansiel virksomhed)

Til § 331

Det følger af § 333 a i lov om finansiel virksomhed, at Finanstilsynet fremmer den offentlige forbrugerinformation på det finansielle område.

Der foreslås at indsætte *§ 331,* hvorefter Finanstilsynet skal fremme den offentlige forbrugerinformation.

Det foreslåede er en lovteknisk rettelse, der har til formål at rykke den gældende § 333 a til § 331.

Finanstilsynet vil arbejde med at skabe lettilgængelig information og stille interaktive værktøjer til rådighed for forbrugerne på forskellige medieplatforme blandt andet i form af hjemmesiden www.raadtilpenge.dk og grupper på sociale medier. Det med sigte på at øge forbrugernes kendskab til og interesse for finansielle produkter og ydelser og derved styrke forbrugerne i deres beslutninger om valg af finansielle produkter. Det vil sikre større gennemslagskraft for indsatsen på det finansielle forbrugerområde.

Som led i en styrkelse og samling af opgavevaretagelse i regi af Finanstilsynet vil der blive oprettet et rådgivende kontaktudvalg, hvor medlemmer fra forbrugerorganisationer og sektoren deltager med henblik på en sparring og gensidig informationsudveksling. Finanstilsynet vil ligeledes inddrage viden og forslag fra universitetsverdenen, når nye initiativer skal planlægges. Det for at sikre størst mulig gennemslagskraft af forskellige forbrugerrettede informationsinitiativer.

Finanstilsynets arbejde med offentlig forbrugerinformation på det finansielle område kan blive finansieret gennem den årlige afgift, som de finansielle virksomheder under tilsyn betaler til Finanstilsynet efter reglerne i kapitel 22 i lov om finansiel virksomhed.

Til afsnit IX b

Til § 332

Under gældende dansk ret gives der ikke selvstændig tilladelse til en udsteder af aktivbaserede tokens. Udstedere af aktivbaserede tokens kan være omfattet af krav i den gældende finansielle lovgivning afhængig af den konkrete forretningsmodel. Visse udbydere er eksempelvis omfattet af krav om registrering efter hvidvasklovens § 48, stk. 1 og 2.

Nogle udstedere af aktivbaserede tokens skal dog ikke ansøge om tilladelse, men alene underrette Finanstilsynet om aktiviteterne og udarbejde en hvidbog.

Det foreslås at indsætte en ny bestemmelse i § 332, som supplerer artikel 16 i MiCA.

Det foreslås i *§ 332, stk. 1*, at en juridisk person eller virksomhed, der udbyder aktivbaserede tokens til offentligheden eller anmoder om optagelse af aktivbaserede tokens til handel i EU, skal være udsteder af disse aktivbaserede tokens og have tilladelse fra Finanstilsynet i overensstemmelse med artikel 21, jf. artikel 16, stk. 1, litra a, i MiCA.

Aktivbaserede tokens defineres i det foreslåede § 332 c, nr. 2, som affattet ved lovforslagets § 1, nr. 24. Den foreslåede bestemmelse i § 332 c, nr. 2, indsætter relevante definitioner fra MiCA.

Det foreslåede stk. 1, vil fastlægge, at Finanstilsynet er kompetent myndighed til at give tilladelse til en udsteder af aktivbaserede tokens efter artikel 16, stk. 1, litra a, i overensstemmelse med artikel 21 i MiCA.

Det er en forudsætning for, at en udsteder af aktivbaserede tokens kan opnå tilladelse fra Finanstilsynet, at den juridiske person eller virksomhed er etableret i Danmark. Finanstilsynet kan give tilladelse til en juridisk person eller virksomhed, der opfylder betingelserne i artikel 18 i MiCA. Det indebærer eksempelvis, at den juridiske person eller virksomhed skal indsende en hvidbog til Finanstilsynet efter artikel 19 i MiCA, jf. kravet i artikel 18 stk. 2, litra k.

En person eller virksomhed, der er meddelt tilladelse efter artikel 21 i MiCA, kan udbyde tjenesterne til offentligheden i hele EU eller anmode om optagelse til handel af sådanne aktivbaserede tokens, jf. artikel 16, stk. 3.

Hvis en virksomhed meddeles tilladelse, anses dens hvidbog om kryptoaktiver for godkendt, jf. artikel 21, stk. 1, i MiCA.

Bestemmelsen supplerer artikel 16, stk. 1, litra a, i MiCA.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024. MiCA fastsætter krav om, at en udsteder af aktivbaserede tokens skal opnå tilladelse til at udbyde aktivbaserede tokens til offentligheden eller anmode om optagelse af aktivbaserede tokens til handel i EU.

Nogle udstedere af aktivbaserede tokens skal dog ikke ansøge om tilladelse, men alene underrette Finanstilsynet om aktiviteterne og udarbejde en hvidbog.

Det foreslås i *§ 332, stk. 2*, at stk. 1 ikke finder anvendelse på et pengeinstitut, der opfylder kravene i artikel 17 i MiCA.

Bestemmelsen vil medføre, at pengeinstitutter, der opfylder kravene i artikel 17 i MiCA, kan udbyde aktivbaserede tokens til offentligheden eller anmode om optagelse af aktivbaserede tokens til handel i EU, jf. artikel 16, stk. 1, litra b.

Pengeinstitutter, der er meddelt tilladelse i henhold til lov om finansiel virksomhed, har ikke behov for yderligere tilladelse af Finanstilsynet i henhold til MiCA for at kunne udbyde eller anmode om optagelse til handel af aktivbaserede tokens.

Pengeinstituttet skal dog leve op til forpligtelserne i artikel 17 i MiCA. Det indebærer blandt andet, at pengeinstituttet skal underrette Finanstilsynet om en række oplysninger i overensstemmelse med artikel 17 i MiCA.

Det foreslåede stk. 2 vil fastlægge, at Finanstilsynet er kompetent myndighed til at vurdere en underretning efter artikel 17, i MiCA.

Pengeinstituttet må ikke udbyde den aktivbaserede token til offentligheden eller optage den til handel, så længe underretningen er ufuldstændig, jf. artikel 17, stk. 3, i MiCA.

Godkender Finanstilsynet pengeinstituttets hvidbog om kryptoaktiver i henhold til artikel 17, stk. 1, eller en ændret hvidbog om kryptoaktiver i henhold til artikel 25, gælder det i hele EU, jf. artikel 16, stk. 4, i MiCA.

Bestemmelsen supplerer artikel 16, stk. 1, litra b, i MiCA.

Der henvises i øvrigt til de lovforslagets § 1, nr. 47 og 48, der beskriver hvilke tjenester, et pengeinstitut og kreditinstitut må udbyde.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Det foreslås i *§ 332, stk. 3*, at stk. 1, ikke finder anvendelse på en udsteder af aktivbaserede tokens, som er undtaget efter artikel 16, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, såfremt udstederen giver meddelelse om en hvidbog om kryptoaktiver i overensstemmelse med artikel 19 i samme forordning, og efter anmodning giver meddelelse om enhver markedsføringskommunikation til Finanstilsynet.

Bestemmelsen vil medføre, at en udsteder af aktivbaserede tokens, som er undtaget efter artikel 16, stk. 2, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, kan udbyde aktivbaserede tokens til offentligheden i EU uden en tilladelse fra Finanstilsynet efter bestemmelsens stk. 1. Udstederen skal dog udarbejde en hvidbog om kryptoaktiver som omhandlet i artikel 19 og give meddelelse om denne hvidbog om kryptoaktiver og efter anmodning give meddelelse om enhver markedsføringskommunikation til Finanstilsynet, jf. artikel 16, stk. 2, i MiCA.

Det foreslåede stk. 3 vil fastlægge, at Finanstilsynet er kompetent myndighed til at modtage en meddelelse efter artikel 16, stk. 2, i MiCA.

Bestemmelsen supplerer artikel 16, stk. 2, i MiCA.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Til § 332 a

Efter gældende ret kan virksomheder med tilladelse som pengeinstitut, kreditinstitut eller e-pengeinstitut udstede og udbyde elektroniske penge. Dette reguleres af lov om betalinger. Disse aktører kan indenfor deres tilladelse også udstede og udbyde e-pengetokens, men det fremgår ikke eksplicit af gældende ret.

Det foreslås i *§ 332 a*, at en person, der udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU,

skal være udsteder af disse og være meddelt tilladelse fra Finanstilsynet som pengeinstitut eller e-pengeinstitut. Udbyderen skal også offentliggøre en hvidbog om kryptoaktiver, som Finanstilsynet er blevet underrettet om i overensstemmelse med artikel 51, jf. artikel 48, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Den foreslåede ændring vil præcisere, at virksomheder med tilladelse som pengeinstitut eller e-pengeinstitut fremadrettet også må udbyde e-pengetokens til offentligheden eller anmode om optagelse af e-pengetokens til handel i EU. Det forudsætter, at virksomheden lever op til de nye kravene i artikel 48 i MiCA. Det indebærer, at virksomheden har underrettet Finanstilsynet om en hvidbog om kryptoaktiver i overensstemmelse med artikel 51 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Med den foreslåede bestemmelse, bliver Finanstilsynet udpeget som kompetent myndighed til at modtage underretningen efter artikel 51 i MiCA.

Det foreslåede vil samtidig betyde, at pengeinstitutter og e-pengeinstitutter, der udsteder e-pengetokens, fremadrettet både vil være omfattet af kravene i lov om finansiel virksomhed, lov om betalinger samt MiCA, for så vidt angår deres aktiviteter vedrørende e-pengetokens. Det skyldes, at e-pengetokens udgør e-penge, som i dansk ret reguleres i lov om betalinger.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udstedere af e-pengetokens, der udbyder disse til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU, vil være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Den foreslåede § 332 a supplerer artikel 48, stk. 1, i MiCA.

Der henvises i øvrigt til lovforslagets § 1, nr. 47 og 48, som regulerer de aktiviteter, som et pengeinstitut og kreditinstitut må udøve.

Til § 332 b

Under gældende dansk ret gives der ikke selvstændig tilladelse som kryptoaktivtjenesteudbyder. En kryptoaktivtjenesteudbyder kan være omfattet af krav i den gældende finansielle lovgivning afhængig af den konkrete forretningsmodel. Visse udbydere er eksempelvis omfattet af krav om registrering efter hvidvasklovens § 48, stk. 1 og 2.

Det foreslås at indsætte en ny bestemmelse i § 332 b, som supplerer artikel 59 i MiCA.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udbydere af kryptoaktivtjenester skal have tilladelse af Finanstilsynet og visse andre finansielle enheder skal underrette Finanstilsynet om en hvidbog om kryptoaktiver og vil være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Det foreslås i *§ 332 b, stk. 1,* at en juridisk person eller anden virksomhed, der leverer kryptoaktivtjenester i EU, skal have tilladelse fra Finanstilsynet efter artikel 63, jf. artikel 59, stk. 1, litra a, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslåede stk. 1 vil fastlægge, at Finanstilsynet er den kompetente myndighed til at give tilladelse som kryptoaktivtjenesteudbyder.

Det foreslåede vil medføre, at en juridisk person eller anden virksomhed, der leverer kryptoaktivtjenester i EU, skal have tilladelse fra Finanstilsynet efter artikel 63, jf. artikel 59, stk. 1, litra a, i MiCA.

Finanstilsynet kan give tilladelse til en juridisk person eller virksomhed efter artikel 63 i MiCA, hvis betingelserne i artikel 62 i MiCA er opfyldt. Det er en forudsætning for, at en udbyder af kryptoaktivtjenester kan opnå tilladelse fra Finanstilsynet, at den juridiske person eller virksomhed er etableret i Danmark.

Enhver person, der er meddelt tilladelse efter artikel 63 i MiCA, kan udbyde tjenesterne til offentligheden i hele EU, jf. artikel 59, stk. 7. Udbydere af kryptoaktivtjenester, der leverer kryptoaktivtjenester på tværs af grænserne, er ikke forpligtede til at have en fysisk tilstedeværelse på et værtslands geografiske område.

Bestemmelsen supplerer artikel 59, stk. 1, litra a, i MiCA. MiCA fastsætter krav om, at en udbyder af kryptoaktivtjenester skal opnå tilladelse som kryptoaktivtjenesteudbyder.
Ifølge MiCA skal nogle udbydere af kryptoaktivtjenester dog ikke ansøge om tilladelse, men alene underrette Finanstilsynet om aktiviteterne og udarbejde en hvidbog, inden disse kan udbyde kryptoaktivtjenester i EU.

Det foreslås i *§ 332 b, stk. 2,* at stk. 1 ikke finder anvendelse på et pengeinstitut, en værdipapircentral, et fondsmæglerselskab, en

markedsoperatør, et e-pengeinstitut, et investeringsforvaltningsselskab eller en forvalter af en alternativ investeringsfond, der har underrettet Finanstilsynet i henhold til artikel 60, stk. 1-6, i MiCA.

Med det foreslåede stk. 2 bliver Finanstilsynet udpeget som kompetent myndighed til at vurdere en underretning efter artikel 60, stk. 1-6, jf. artikel 60, stk. 8, i MiCA.

Det foreslåede vil derudover medføre, at såfremt de i bestemmelsen nævnte virksomhedstyper leverer kryptoaktivtjenester, skal de ikke indsende en ansøgning om tilladelse som kryptoaktivtjenesteudbyder efter artikel 62 i MiCA. Virksomhederne skal derimod underrette Finanstilsynet i overensstemmelse med artikel 60, stk. 1-6, i MiCA.

En udbyder af kryptoaktivtjenester må ikke begynde at levere kryptoaktivtjenesterne, så længe underretningen er ufuldstændig, jf. artikel 60, stk. 8, i MiCA.

En virksomhed, der har tilladelse til at levere kryptoaktivtjenester i henhold til artikel 60, har mulighed for at levere kryptoaktivtjenester i hele EU. Derudover gælder, at udbydere af kryptoaktivtjenester, der leverer kryptoaktivtjenester på tværs af grænserne, ikke er forpligtede til at have en fysisk tilstedeværelse på et værtslands geografiske område, jf. artikel 59, stk. 7, i MiCA.

Retten til at levere kryptoaktivtjenester for disse virksomheder ophæves ved inddragelsen af den tilladelse, der gav den pågældende virksomhed mulighed for at levere kryptoaktivtjenester uden at skulle indhente en tilladelse i henhold til artikel 59 i MiCA, jf. artikel 60, stk. 11, i MiCA.

Bestemmelsen supplerer artikel 59, stk. 1, litra b, i MiCA.

Til § 332 c

Det foreslås i § 332 c at tilføje relevante definitioner fra MiCA til lov om finansiel virksomhed.

Det foreslås i *§ 332 c, nr. 1,* at ved kryptoaktiv forstås en digital gengivelse af en værdi eller af en rettighed, som kan overføres og lagres elektronisk ved hjælp af distributed ledger-teknologi eller lignende teknologi.

Definitionen svarer til definitionen i artikel 3, stk. 1, nr. 5, i MiCA.

Det foreslås i *§ 332 c, nr. 2,* at ved en aktivbaseret token forstås en form for kryptoaktiv, der ikke er en elektronisk pengetoken, og som hævdes at bevare en stabil værdi ved at henvise til en anden værdi eller rettighed eller en kombination heraf, herunder en eller flere officielle valutaer.

Definitionen svarer til definitionen i artikel 3, stk. 1, nr. 6, i MiCA.

Det foreslås i *§ 332 c, nr. 3,* at ved elektronik pengetoken eller e-pengetoken forstås en form for kryptoaktiv, som hævdes at bevare en stabil værdi ved at henvise til værdien af en officiel valuta.

Definitionen svarer til definitionen i artikel 3, stk. 1, nr. 7, i MiCA.

Det foreslås i *§ 332 c, nr. 4,* at ved udsteder af kryptoaktiver forstås en fysisk eller juridisk person eller en anden virksomhed, der udsteder kryptoaktiver.

Definitionen er tilpasset til dansk ret på baggrund af definitionen i artikel 3, stk. 1, nr. 10, i MiCA. Det skyldes, at "udsteder" allerede bruges i andre sammenhænge i lov om finansiel virksomhed. Derfor er artikel 3, stk. 1, nr. 10, i MiCA, implementeret som "udsteder af kryptoaktiver" i lov om finansiel virksomhed.

Det foreslås i *§ 332 c, nr. 5,* at ved udbyder af kryptoaktiver forstås en fysisk eller juridisk person eller en anden virksomhed, eller udstederen, som udbyder kryptoaktiver til offentligheden.

Definitionen er tilpasset til dansk ret på baggrund definitionen i artikel 3, stk. 1, nr. 13, i MiCA. Det skyldes, at "udbyder" allerede bruges i andre sammenhænge i lov om finansiel virksomhed. Derfor er artikel 3, stk. 1, nr. 13, i MiCA, implementeret som "udbyder af kryptoaktiver" i lov om finansiel virksomhed.

Det foreslås i *nr. 6,* at ved udbyder af kryptoaktivtjenester forstås en juridisk person eller en anden virksomhed, hvis erhverv eller forretning består i at levere en eller flere kryptoaktivtjenester til kunder på et erhvervsmæssigt grundlag, og som har tilladelse til at levere kryptoaktivtjenester i overensstemmelse med artikel 59 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Definitionen svarer til definitionen i artikel 3, stk. 1, nr. 15, i MiCA.

Det foreslås i *§ 332 c, nr. 7,* at ved kryptoaktivtjeneste forstås en af de i bestemmelsens litra a-j opremsede tjenester og aktiviteter vedrørende ethvert kryptoaktiv.

Det forslås i § 332 c, nr. 7, litra *a,* at levering af deponering og administration af kryptoaktiver på kunders vegne er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra b,* at drift af en handelsplatform for kryptoaktiver er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra c,* at veksling mellem kryptoaktiver og midler er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra d,* at veksling mellem kryptoaktiver og andre kryptoaktiver er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra e,* at udførelse af ordrer vedrørende kryptoaktiver på vegne af kunder er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra f,* at placering af kryptoaktiver er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra g,* at modtagelse og formidling af ordrer vedrørende kryptoaktiver på vegne af kunder er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra h,* at rådgivning om kryptoaktiver er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra i,* at porteføljepleje i forbindelse med kryptoaktiver er en kryptoaktivtjeneste.

Det forslås i § 332 c, nr. 7, *litra j,* at levering af tjenester vedrørende overførsel af kryptoaktiver på vegne af kunder er en kryptoaktivtjeneste.

Definitionerne svarer til definitionerne i artikel 3, stk. 1, nr. 16, i MiCA.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Til § 332 d

Efter gældende ret er der ikke regler om en tilladelsesordning for udstedere af aktivbaserede tokens. Som en konsekvens heraf har Finanstilsynet heller ikke mulighed for at tilbagekalde en tilladelse til at udstede aktivbaserede tokens.

Det foreslås i *§ 332 d*, at Finanstilsynet kan inddrage en tilladelse til en udsteder af aktivbaserede tokens efter artikel 24 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Den foreslåede bestemmelse vil give Finanstilsynet beføjelse til at kunne inddrage en tidligere givet tilladelse til en udsteder af aktivbaserede tokens efter artikel 24 i MiCA. Finanstilsynet kan blandt andet inddrage tilladelsen, hvis udstederen af aktivbaserede tokens ikke længere opfylder de betingelser, hvorpå tilladelsen blev meddelt.

Bestemmelsen er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en udsteder af aktivbaserede tokens skal have tilladelse af Finanstilsynet til at udbyde aktivbaserede tokens til offentligheden eller anmode om optagelse til handel i EU og være underlagt Finanstilsynets tilsyn i henhold til MiCA. Dette indebærer, at Finanstilsynet også har beføjelse til at inddrage en tidligere givet tilladelse til en udsteder af aktivbaserede tokens.

Bestemmelsen supplerer artikel 24 i MiCA.

Til § 332 e

Efter gældende ret er der ikke regler om en tilladelsesordning for udbydere af kryptoaktivtjenester. Som en konsekvens heraf har Finanstilsynet heller ikke mulighed for at tilbagekalde en tilladelse til at udbyde kryptoaktivtjenester.

Det foreslås i *§ 332 e*, at Finanstilsynet kan inddrage en tilladelse til en udbyder af kryptoaktivtjenester efter artikel 64 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Den foreslåede bestemmelse vil give Finanstilsynet beføjelse til at kunne inddrage en tidligere givet tilladelse til en udbyder af kryptoaktivtjenester efter artikel 64 i MiCA. Finanstilsynet kan blandt andet inddrage tilladelsen, hvis en udbyder af kryptoaktivtjenester har opnået sin tilladelse på uretmæssig vis såsom i form af falske erklæringer i sin ansøgning om tilladelse, eller ikke længere opfylder de betingelser, hvorpå tilladelsen blev meddelt.

Bestemmelsen er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en udbyder af kryptoaktivtjenester skal have tilladelse af Finanstilsynet og være underlagt

Finanstilsynets tilsyn i henhold til MiCA. Dette indebærer, at Finanstilsynet også har beføjelse til at inddrage en tidligere givet tilladelse som udbyder af kryptoaktivtjenester.

Bestemmelsen supplerer artikel 64 i MiCA.

Til § 332 f

Efter gældende ret er der ikke regler om en tilladelsesordning for udstedere af aktivbaserede tokens. Som følge heraf er udstedere af aktivbaserede tokens ikke efter gældende ret forpligtede til at foretage indberetninger til Finanstilsynet.

Det foreslås at indsætte en ny bestemmelse i § 332 f.

Det foreslås i *§ 333 f, stk. 1*, at en udsteder af aktivbaserede tokens omfattet af § 361, stk. 1, nr. 11, senest den 1. juli hvert år skal indberette summen af udstederens gennemsnitlige udestående til Finanstilsynet.

Den foreslåede bestemmelse vil fastlægge, at Finanstilsynet hvert år skal modtage data fra udstedere af aktivbaserede tokens til brug for opgørelsen af afgiften, som skal betales til Finanstilsynet, jf. den foreslåede § 361, stk. 1, nr. 11, i lov om finansiel virksomhed.

Finanstilsynet har generel hjemmel til at kræve alle oplysninger af en virksomhed, som Finanstilsynet finder nødvendige med henblik på at føre tilsyn med MiCA, jf. den foreslåede ændring til § 344 i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 25. Hjemlen kan udnyttes til at indsamle data til brug for tilrettelæggelsen af tilsynet med udstedere af aktivbaserede tokens.

Det foreslås i *§ 333 f, stk. 2*, at gennemsnittet af de udestående aktivbaserede tokens beregnes som den samlede markedsværdi af de udestående aktivbaserede tokens, opgjort på baggrund af det daglige udestående ved udgangen af hver dag i de foregående 6 måneder. Opgørelsen foretages den første dag i hver måned. Hvis virksomheden ikke har gennemført 6 måneders drift på datoen for beregningen, anvendes de eventuelt gennemførte måneder med drift og virksomhedens estimater for de gennemsnitlige udestående aktivbaserede tokens for det kommende år som grundlag for beregningen.

Den foreslåede bestemmelse vil fastsætte, at virksomheden til brug for beregningen skal anvende eventuelt gennemførte måneder med drift samt virksomhedens estimater for de gennemsnitlige udestående aktivbaserede

tokens for det kommende år, hvis virksomheden ikke har gennemført seks måneders drift på datoen for beregningen. Har virksomheden eksempelvis haft fem måneders drift anvendes disse måneder i beregningen sammen med virksomhedens estimat for de gennemsnitlige udestående aktivbaserede tokens for det kommende år divideret med 12.

Bestemmelsen er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en udsteder af aktivbaserede tokens skal have tilladelse af Finanstilsynet til at udbyde aktivbaserede tokens til offentligheden eller anmode om optagelse til handel i EU og være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Til § 332 g

Efter gældende ret er der ikke regler om en tilladelsesordning for udbydere af kryptoaktivtjenester. Som følge heraf er udbydere af kryptoaktivtjenester ikke efter gældende ret forpligtede til at foretage indberetninger til Finanstilsynet.

Det foreslås i *§ 332 g*, at en udbyder af kryptoaktivtjenester omfattet af § 361, stk. 1, nr. 12, senest den 1. juli hvert år skal indberette virksomhedens omkostninger til løn, provision og tantieme til Finanstilsynet.

Den foreslåede bestemmelse vil fastlægge, at Finanstilsynet hvert år skal modtage data fra udbydere af kryptoaktivtjenester til brug for opgørelsen af afgiften, som skal betales til Finanstilsynet, jf. den foreslåede § 361, stk. 1, nr. 12.

Finanstilsynet har generel hjemmel til at kræve alle oplysninger af en virksomhed, som Finanstilsynet finder nødvendige, med henblik på at føre tilsyn med MiCA, jf. den foreslåede ændring til § 344, i lov om finansiel virksomhed. Hjemlen kan udnyttes til at indsamle data til brug for tilrettelæggelsen af tilsynet med udbydere af kryptoaktivtjenester.

Ved omkostninger til løn, provision og tantieme menes lønninger og vederlagt til bestyrelse og direktion samt lønninger til personale i øvrigt.

Bestemmelsen er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en udbyder af kryptoaktivtjenester skal have tilladelse af Finanstilsynet til at udbyde kryptoaktivtjenester og være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Til § 332 h

Finanstilsynets har som led i sit tilsyn med overholdelse af en række retsakter beføjelse til at få adgang til lokaler og lokaliteter tilhørende virksomheder under tilsyn. Dette følger af bl.a. lov om finansielvirksomhed § 343 e, § 347, stk. 3, 4 og 5, samt § 233, stk. 1-4, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.

Det foreslås i *§ 332 h*, at Finanstilsynet til brug for tilsyn med overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver kan udøve de beføjelser, der følger af forordningens artikel 94, herunder til enhver tid mod behørig legitimation uden retskendelse få adgang til lokaler og lokaliteter tilhørende udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, og personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, udstedere af aktivbaserede tokens, udstedere af e-pengetokens og udbydere af kryptoaktivtjenester og med henblik på indhentelse af oplysninger, herunder ved inspektioner.

Den foreslåede bestemmelse vil således fastlægge, at Finanstilsynet er den kompetente myndighed til at påse overholdelsen af MiCA.

Til brug for tilsynet med overholdelsen af MiCA vil Finanstilsynet kunne udøve de beføjelser, der følger af forordningens artikel 94, herunder til enhver tid mod behørig legitimation uden retskendelse få adgang til lokaler og lokaliteter tilhørende udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, og personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, udstedere af aktivbaserede tokens, udstedere af e-pengetokens og udbydere af kryptoaktivtjenester, og med henblik på indhentelse af oplysninger, herunder ved inspektioner.

Den foreslåede bestemmelse vil udgøre en særegen undtagelse til kravet om retskendelse efter grundlovens § 72, 2. pkt., for foretagelse af husundersøgelse for så vidt angår beføjelsen i artikel 94, stk. 1, litra w.

I medfør af i artikel 94, stk. 1, litra w, skal den kompetente myndighed kunne få adgang til at gennemføre kontrolbesøg og undersøgelser på andre steder end i fysiske personers private boliger og med henblik herpå skaffe sig adgang til lokaler for at få adgang til dokumenter og andre oplysninger i enhver form, når der er rimelig mistanke om, at dokumenter og andre oplysninger vedrørende genstanden for kontrollen eller undersøgelsen kan være relevant som bevis for en overtrædelse af denne forordning. Denne beføjelse vil som det klare udgangspunkt skulle udøves af Finanstilsynet.

Vedrører mistanken imidlertid en overtrædelse af en af de artikler, der efter den foreslåede ændring i § 373, stk. 1 og 2, i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 43 og 44, § 152, stk. 1 og 2, i lov om betalinger, jf. lovforslagets § 2, nr. 24 og 25, § 251 b, stk. 1-3, i lov om kapitalmarkeder, jf. lovforslagets § 3, nr. 21, § 266, stk. 1, nr. 5 og § 266, stk. 2, nr. 4 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, jf. lovforslagets § 4, nr. 13 og 14, samt § 190, stk. 1 og 2, i lov om forvaltere af alternative investeringsfonde, m.v., jf. lovforslagets § 5, nr. 8 og 9, der vil være forbundet med strafansvar, vil en sådan beføjelse have karakter af ransagning og dermed et straffeprocessuelt tvangsindgreb, der efter reglerne i § 9, stk. 1, i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter, jf. lovbekendtgørelse nr. 1121 af 12. november 2019, vil skulle gennemføres efter reglerne i lov om rettens pleje og dermed i praksis af National enhed for Særlig Kriminalitet eller den stedlige politikreds.

Finanstilsynet har behov for at kunne udøve sin tilsynsvirksomhed også i de særlige tilfælde, hvor en virksomhed måtte nægte at give Finanstilsynets de nødvendige oplysninger til brug for tilsynsvirksomheden, eller hvor en virksomhed modsætter sig et inspektionsbesøg.

Finanstilsynet har mulighed for at foretage inspektion uden forudgående varsling. Denne hjemmel skal alene anvendes af Finanstilsynet efter et almindeligt proportionalitetsprincip i tilfælde, hvor Finanstilsynet vurderer, at formålet med inspektionen ville blive forspildt, hvis inspektionen blev varslet. Udgangspunktet er således fortsat, at inspektioner hos fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester, skal varsles på forhånd.

Hjemlen kan tænkes anvendt, f.eks. hvor en tilsynsbelagt virksomhed undtagelsesvist nægter Finanstilsynet adgang til virksomheden i forbindelse med en ordinær inspektion. Der kan også være tale om en krisesituation, der kræver, at Finanstilsynet skrider til omgående handling, og hvor en umiddelbar adgang til udbyderen er en forudsætning for at håndtere situationen.

Den foreslåede bestemmelse supplerer således artikel 94 i forordningen, idet den fastsætter, hvem der som udgangspunkt vil være den kompetente myndighed i Danmark til at udøve de beføjelser, som artikel 94 giver adgang til.

Bestemmelsen er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter Finanstilsynet som den

kompetente myndighed vil påse overholdelsen af MiCA, og fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester vil være underlagt Finanstilsynets tilsyn i henhold til MiCA. Med "visse andre virksomheder" menes f.eks. enkeltmandsvirksomheder, som i visse tilfælde ikke betragtes som juridiske personer i dansk ret.

Til afsnit IX c

Finanstilsynet fører i dag tilsyn med it-sikkerheden hos fælles datacentraler og it-operatører af detailbetalingssystemer.

Fælles datacentraler er reguleret i afsnit X c i lov om finansiel virksomhed.

Det kræver ikke tilladelse fra Finanstilsynet at drive en fælles datacentral, ligesom det f.eks. er tilfældet med et penge- eller realkreditinstitut. Derimod bliver en virksomhed automatisk omfattet af reglerne om fælles datacentraler, hvis f.eks. virksomhedens væsentligste aktiviteter består i it-drifts- eller udviklingsopgaver for flere finansielle virksomheder, og virksomheden samtidig overvejende er ejet af flere finansielle virksomheder, jf. § 343 q i lov om finansiel virksomhed.

Reglerne for fælles datacentraler afspejler de regler, der også gælder finansielle virksomheders kontrol- og sikringsforanstaltninger på it-området, ligesom tilsynsrammen for tilsynet med datacentraler også afspejler det it-tilsyn, som Finanstilsynet fører med de finansielle virksomheder.

Det følger således af § 343 r, stk. 1, i lov om finansiel virksomhed, at § 71, stk. 1, nr. 8, i lov om finansiel virksomhed, om betryggende kontrol- og sikringsforanstaltninger på it-området finder tilsvarende anvendelse for fælles datacentraler.

Reglerne om betryggende kontrol- og sikringsforanstaltninger på it-området, der er udstedt i medfør af § 71, stk. 3, i lov om finansiel virksomhed finder også tilsvarende anvendelse for fælles datacentraler, jf. § 343 r, stk. 2, i lov om finansiel virksomhed. Disse regler findes i bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.v., herunder særligt bekendtgørelsens bilag 5, der bl.a. fastsætter nærmere krav til den it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik, som en datacentral skal have.

Endelig følger det af § 343 r, stk. 5, i lov om finansiel virksomhed, at kapitel 21 og 23 i lov om finansiel virksomhed og regler udstedt i medfør af disse kapitler finder tilsvarende anvendelse for fælles datacentraler med de fornødne tilpasninger. Det indebærer bl.a., at tilsynsrammen for tilsynet med finansielle virksomheder også gælder for fælles datacentraler, herunder bl.a. reglerne om Finanstilsynets tavshedspligt, offentliggørelse, partsbestemmelser og klageadgang.

Finanstilsynet fører også tilsyn med it-operatører af detailbetalingssystemer, dvs. virksomheder, der er meddelt tilladelse til it-drift af et detailbetalingssystem efter § 180 a i lov om kapitalmarkeder. It-operatører af detailbetalingssystemer er reguleret i kapitel 32 a i lov om kapitalmarkeder.

Reglerne om it-operatører af detailbetalingssystemers kontrol- og sikringsforanstaltninger på it-området afspejler ligesom for datacentraler det it-tilsyn, som Finanstilsynet fører med de finansielle virksomheder.

Det følger af § 180 g, stk. 2, nr. 2, i lov om kapitalmarkeder, at it-operatører af detailbetalingssystemer skal have betryggende kontrol- og sikringsforanstaltninger på it-området. I forlængelse heraf følger det af § 180 g, stk. 3, at Finanstilsynet kan fastsætte nærmere regler om de foranstaltninger, som en it-operatør af et detailbetalingssystem skal træffe for at have betryggende kontrol- og sikringsforanstaltninger på it-området. Bemyndigelsen er ligesom for datacentraler, udnyttet i bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.v., herunder særligt bekendtgørelsens bilag 5, der bl.a. fastsætter nærmere krav til den it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik, som it-operatører af detailbetalingssystemer skal have.

Med vedtagelsen af NIS 2-direktivet og DORA-forordningen styrkes it- og cybersikkerheden i den finansielle sektor ved at gennemføre en væsentlig udvidelse, harmonisering og modernisering af de juridiske rammer på tværs af medlemslandene. Fælles datacentraler og it-operatører af detailbetalingssystemer omfattes af NIS 2-direktivets generelle regler, der bl.a. finder anvendelse på digital infrastruktur og forvaltning af it-tjenester, jf. direktivets bilag 1, pkt. 8 og 9. Derfor skal reglerne i NIS 2-direktivet implementeres for fælles datacentraler og it-operatører af detailbetalingssystemer. Fælles datacentraler og it-operatører omfattes dog ikke direkte af DORA-forordningen.

For at sikre et ensartet og stærkt cybersikkerhedsniveau i hele den finansielle sektor, og at Finanstilsynet kan føre tilsyn med it- og cybersikkerheden i alle relevante virksomheder på det finansielle område, foreslås det med § 333 i

lov om finansiel virksomhed, at Finanstilsynet kan udpege de virksomheder, der udbyder digital infrastruktur og forvaltning af it-tjenester indenfor den finansielle sektor, herunder fælles datacentraler og it-operatører af detailbetalingssystemer, som operatører af finansielle digitale infrastrukturer.

Der henvises i det hele til de almindelige bemærkninger i lovforslagets 2.2.

Til § 333

Det foreslås i *§ 333, stk. 1*, at Finanstilsynet kan udpege virksomheder, der udbyder digital infrastruktur eller forvalter it-tjenester, som omhandlet i bilag I, pkt. 8 og 9, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022, og hvis væsentligste aktiviteter består i at drive, administrere eller udvikle tjenester, der er nødvendige for kritiske og vigtige forretningsfunktioner i virksomheder, der er omfattet af Europa-Parlamentets og Rådets forordning (EU) 2022/2254 af 14 december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, som operatører af finansielle digitale infrastruktur.

Den foreslåede bestemmelse vil indebære, at de virksomheder, der udpeges, vil blive underlagt Finanstilsynets tilsyn på it- og cybersikkerhedsområdet. For f.eks. fælles datacentraler, der udpeges, vil bestemmelsen således betyde, at disse fortsat vil være omfattet af Finanstilsynets tilsyn.

Bestemmelsen indeholder også en afgrænsning af hvilke virksomheder, der potentielt kan udpeges som operatører af finansielle digitale infrastrukturer. For at kunne udpeges som operatør af en finansiel digital infrastruktur skal den pågældende virksomhed tilhøre en af delsektorerne under pkt. 8 (digital infrastruktur), eller pkt. 9 (forvaltning af it-tjenester), i bilag I, til NIS 2-direktivet. Herudover skal virksomheden væsentligste aktiviteter bestå i at drive, administrere eller udvikle tjenester, der er nødvendige for kritiske og vigtige forretningsfunktioner i de virksomheder, der omfattes af DORA-forordningen.

Blandt de virksomheder, der opfylder disse kriterier, vil Finanstilsynet kunne udpege de virksomheder, som er væsentlige i forhold til den finansielle sektor, ud fra kriterier som er angivet i stk. 2.

Kravene er kumulative og kan ikke fraviges.

Det foreslås i *§ 333, stk. 2*, at Finanstilsynet ved udpegningen af operatører af finansielle digitale infrastrukturer skal lægge vægt på de kriterier, der følger af nr. 1-4.

Det foreslås i *§ 333, stk. 2, nr. 1,* at Finanstilsynet skal lægge vægt på omfanget og antallet af finansielle virksomheder som operatøren varetager kritiske og vigtige funktioner for.

Bestemmelsen vil indebære, at Finanstilsynet både skal lægge vægt på antallet af de tilsluttede virksomheder indenfor den finansielle sektor, men også på forretningsomfanget med den eller de tilsluttede virksomheder. Det kan f.eks. være omfanget af kritiske og vigtige funktioner, som operatøren varetager, og herunder også omfanget af kunder eller engagementer, der berøres af operatørens ydelser.

Det foreslås i *§ 333, stk. 2, nr. 2,* at Finanstilsynet skal lægge vægt på karakteren af de kritiske og vigtige funktioner, som er afhængige af operatørens leverancer.

Bestemmelsen vil indebære, at Finanstilsynet skal lægge vægt på, hvor væsentlige de kritiske og vigtige funktioner er for de tilsluttede virksomheders levering af de finansielle kerneydelser, og om der er tale om leverancer, som ikke eller kun vanskeligt kan substitueres.

Det foreslås i *§ 333, stk. 2, nr. 3,* at Finanstilsynet skal lægge vægt på betydningen af operatørens leverancer for den finansielle stabilitet.

Bestemmelsen vil indebære, at Finanstilsynet skal lægge vægt på operatørens betydning og rolle i forhold til den samlede finansielle sektor, herunder den risiko operatøren potentielt kan eksponere den finansielle sektor for.

Det foreslås i *§ 333, stk. 2, nr. 4,* at Finanstilsynet skal lægge vægt på operatørens tilknytning til de virksomheder i den finansielle sektor som modtager operatørens ydelser, herunder koncernforbindelser og ejerskab.

Bestemmelsen vil indebære, at Finanstilsynet skal lægge vægt på bl.a. de indikationer om tilknytning mellem operatøren og dens finansielle kundevirksomheder, f.eks. gennem ejerskab, koncernforbindelser og relationer gennem medlemskab af foreninger eller sammenslutninger.

Kriterierne i stk. 2, er ikke kumulative og ikke alle kriterier skal være opfyldt for at en virksomhed kan udpeges som en operatør af en finansiel digital infrastruktur.

Vurderingen af de enkelte operatørers opfyldelse af kriterierne skal foretages ud fra en risikovurdering, som tager højde for den enkelte

virksomheds forhold og relationer og for den overordnede betydning af disse for det finansielle system og den finansielle stabilitet.

Det foreslås i *§ 333, stk. 3,* at it-operatører af detailbetalingssystemer og virksomheder, der udfører væsentlig drift eller udvikling af den fælles betalingsinfrastruktur kan udpeges som operatører af finansielle digitale infrastrukturer efter stk. 1.

Bestemmelsen vil indebære, at virksomheder der varetager driften af væsentlig betalingsinfrastruktur vil kunne udpeges som operatører af finansielle digitale infrastrukturer, når de opfylder betingelserne i § 333, stk. 1 og 2.

Det foreslås i *§ 333, stk. 4,* at Finanstilsynet skal offentliggøre på sin hjemmeside, hvilke virksomheder der er udpeget som operatører af finansielle digitale infrastrukturer.

Offentliggørelse vil medføre, at det overfor offentligheden og den øvrige finansielle sektor bliver tydeligt, hvilke virksomheder, der er omfattet af Finanstilsynets tilsyn på it- og cybersikkerhedsområdet, og at disse virksomheder er omfattet af de regler, som erhvervsministeren med den foreslåede § 333 b i lov om finansiel virksomhed bemyndiges til at udstede.

Det foreslås i *§ 333, stk. 5,* at Finanstilsynet kan fastsætte nærmere regler om den udpegning af operatører af finansielle digitale infrastrukturer og de kriterier, som Finanstilsynet kan lægge vægt på efter stk. 1 og 2.

Det foreslåede medfører bl.a., at Finanstilsynet kan fastsætte regler om kvantificering og vægtning af kriterierne i stk. 1 og 2.

Til § 333 a

Forslaget til § 333 a angiver de centrale foranstaltninger, som en operatør af digital finansiel infrastruktur skal foretage i forhold til styring af it- og cyberrisici som følge af artikel 21, stk. 1-3, i NIS 2-direktivet. Foranstaltningerne skal indgå i en overordnet forvaltnings- og kontrolramme. Den foreslåede bestemmelse implementerer art. 21, stk. 1-3, i NIS 2-direktivet. Bestemmelsen er tilpasset de supplerende krav i §§ 333 d, og 333 h, som er harmoniseret med kravene i artikel 6 i DORA-forordningen.

Det foreslås i *§ 333 a, stk. 1,* at en operatør af finansiel digitale infrastruktur skal have en forvaltnings- og kontrolramme, der sikrer en effektiv og forsigtig styring af it- og cyberrisici.

Den foreslåede bestemmelse indebærer, at en operatør af finansiel digital infrastruktur skal have en forvaltnings- og kontrolramme til styring af it- og cyberrisici, der skal forebygge it- og cybersikkerhedshændelser og minimere en hændelses indvirkning på de tjenester, som operatøren leverer. Kraven til de foranstaltninger, som en operatør af finansiel digital infrastruktur skal træffe som led i en forvaltnings- og kontrolramme, fremgår nærmere af stk. 2 og 3.

Bestemmelsen implementerer artikel 21, stk. 1, 1. afsnit, i NIS 2-direktivet.

Overtrædelse af § 333 a, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er en operatør af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have fastsat en ramme for styring af it- og cyberrisici.

Det foreslås i *§ 333 a, stk. 2,* at en operatør af finansiel digital infrastruktur som led i rammen for styring af it- og cyberrisici skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risici for sikkerheden i net- og informationssystemer.

Med passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger forstås, at foranstaltningerne skal være tilstrækkelige i forhold til de risici, som operatøren af finansiel digital infrastruktur er udsat for, og betydningen af de forretningsfunktioner, som foranstaltningerne tilsigter at beskytte. Operatøren skal bl.a. tage hensyn til sandsynligheden for en hændelse og konsekvenserne heraf set i forhold til de tjenester, som operatøren leverer.

De omhandlende foranstaltninger skal baseres på den risikovurdering, som virksomheden skal udarbejde i overensstemmelse med den foreslåede § 333 d, stk. 2, i lov om finansiel virksomhed. De nærmere krav til, hvad foranstaltninger skal omfatte, følger af det foreslåede § 333 a, stk. 3, i lov om finansiel virksomhed.

Bestemmelsen implementerer artikel 21, stk. 1, i NIS 2-direktivet.

Overtrædelse af § 333 a, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er en operatør

af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have iværksat tekniske, operationelle og organisatoriske foranstaltninger for at styre risici for sikkerheden i net- og informationssystemer. Den strafbare handling kan også bestå i at have indført foranstaltninger, som ikke er tilstrækkelige til beskyttelse af de forretningsfunktioner som foranstaltningerne skal beskytte.

Den foreslåede bestemmelse i *stk. 3,* opregner de foranstaltninger, som en operatør af finansiel digital infrastruktur som minimum skal træffe i henhold til NIS 2-direktivet.

En del af forpligtelserne omkring de konkrete foranstaltninger er yderligere præciseret i de foreslåede bestemmelser i §§ 333 b – 333 l. Opregningen af foranstaltninger skal desuden ses i sammenhæng med forpligtelserne i kapitel II, i DORA-forordningen.

Bestemmelsen implementerer artikel 21, stk. 2, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 1,* at de i stk. 2 omhandlede foranstaltninger skal omfatte politikker for risikoanalyse og informationssystemssikkerhed.

Med den foreslåede bestemmelse skal en operatør af finansiel digital infrastruktur udarbejde politikker, der fastsætter nærmere retningslinjer for den risikoanalyse, som operatøren skal foretage med passende mellemrum i henhold til det foreslåede § 333 d, stk. 2. I forbindelse hermed skal operatøren identificere og vurdere alle væsentlige it- og cyberrisici, som operatøren og dennes ydelser er eksponeret for. Analysen skal gøre det muligt for operatøren at fastsætte eller revurdere rammen for it- og risikostyring og træffe passende og forholdsmæssige foranstaltninger i forbindelse hermed.

Desuden vil operatøren af finansiel digital infrastruktur skulle fastsætte en politik for sikkerheden i informationssystemer til beskyttelse af sådanne systemer mod bl.a. systemfejl, menneskelige fejl og udefrakommende hændelser. Forpligtelsen er yderligere præciseret i det foreslåede § 333 e, stk. 5, hvoraf fremgår, at operatøren skal udforme og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er egnede til at sikre modstandsdygtighed, stabilitet og tilgængelighed for it-systemer, der understøtter kritiske eller vigtige funktioner og til at opretholde et højt niveau af tilgængelighed, autenticitet, integritet og fortrolighed af data.

Bestemmelsen implementerer artikel 21, stk. 2, litra a, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 2*, at de i stk. 2 omhandlede foranstaltninger skal omfatte håndtering af hændelser.

Den foreslåede bestemmelse skal ses i forhold til kravet om styring og indberetning af it- og cyberhændelser i medfør af det foreslåede § 333 f i lov om finansiel virksomhed. Det fremgår således af det foreslåede § 333 f, stk. 1, at en operatør af finansiel digital infrastruktur skal fastlægge og gennemføre en proces for overvågning, styring og indberetning af it- og cyberhændelser. Der henvises i det hele til den foreslåede bestemmelse i § 333 f og de specielle bemærkninger hertil.

Bestemmelsen implementerer artikel 21, stk. 2, litra b, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 3*, at de i stk. 2 omhandlede foranstaltninger skal omfatte driftskontinuitet, herunder backup-styring og reetablering efter større hændelser og krisestyring.

Den foreslåede bestemmelse skal ses i sammenhæng med de foreslåede bestemmelser til § 333 e, stk. 7 og 8, i lov om finansiel virksomhed, vedrørende politik og foranstaltninger for it-driftsstabilitet og krisestyring, § 333 e, stk. 9, i lov om finansiel virksomhed, vedrørende sikkerhedskopiering, gendannelse og genopretning, samt § 333 e, stk. 12, i lov om finansiel virksomhed, vedrørende krisekommunikation.

Bestemmelsen implementerer artikel 21, stk. 2, litra c, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 4*, at de i stk. 2 omhandlede foranstaltninger skal omfatte forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem operatøren af finansiel digital infrastruktur og dens direkte leverandører eller tjenesteudbydere.

De nærmere regler om en operatør af finansiel digital infrastrukturs brug af it-tjenester fra tredjeparter er nærmere reguleret i de foreslåede bestemmelser til §§ 333 h-j, i lov om finansiel virksomhed. Bestemmelserne i de foreslåede § 333 h, stk. 9-13, i lov om finansiel virksomhed indeholder regler om exitstrategier, hvoraf det f.eks. fremgår af § 333 h, stk. 10, at en operatør skal sikre, at den kan opsige kontraktlige ordninger, uden at dens forretningsaktiviteter afbrydes, efterlevelsen af de lovgivningsmæssige krav begrænses, og kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade. Forslaget til § 333 h, stk. 1, 3 og 4, i lov om finansiel virksomhed indeholder nærmere bestemmelser om en operatør af finansiel digital infrastrukturs styring af de it- og cyberrisici, der er relateret til brugen af it-tjenester fra tredjeparter.

Den foreslåede bestemmelse skal endvidere ses i sammenhæng med det foreslåede § 333 a, stk. 4, i lov om finansiel virksomhed, der supplerer kravene til risikostyring i forbindelse med it-tredjepartsleverandører.

Der henvises nærmere til forslagene til §§ 333 h-j og de specielle bemærkninger hertil.

Bestemmelsen implementerer artikel 21, stk. 2, litra d, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 5*, at de i stk. 2 omhandlede foranstaltninger skal omfatte sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

Det fremgår af det foreslåede § 333 e, stk. 4, i lov om finansiel virksomhed, at en operatør af finansiel digital infrastruktur skal overvåge og kontrollere it-systemernes og it-værktøjernes funktion og sikkerhed og minimere virkningerne af it- og cyberrisici ved at indføre passende sikkerhedsværktøjer, -politikker og -procedurer. På samme vis indebærer den foreslåede stk. 3, nr. 5, at en operatør skal have foranstaltninger, for overvågning og kontrol af sikkerheden, når operatøren erhverver net- og informationssystemer, udvikler på systemerne og foretager vedligeholdelse heraf.

Erhvervelse af net- og informationssystemer, der endnu ikke er fuldt integreret i operatørens øvrige systemer, herunder systemer til overvågning og kontrol af it-systemernes funktion og sikkerhed og funktioner, der skal minimere virkningerne af it- og cyberrisici, vil som oftest være mere sårbare i forhold til operatørens øvrige systemer. Det samme gælder i forbindelse med udvikling og vedligeholdelse af systemerne, der for en tid kan bevirke, at det pågældende system frakobles de øvrige systemer. Derfor er det vigtigt, at operatøren udarbejder foranstaltninger til håndteringen af sårbarheder i forbindelse hermed og offentliggørelsen heraf, så operatørens kunder er bevidste om, at der f.eks. kan forekomme perioder med udfald eller perioder, hvor et givent system midlertidigt er nede.

Forslaget vil indebære, at operatøren af finansiel digital infrastruktur forpligtes til at håndtere og offentliggøre sårbarheder efter principper for koordineret og ansvarlig offentliggørelse. Dette omfatter brug af kanaler for koordineret offentliggørelse, hvilket vil indebære involvering af relevante leverandører, og at sårbarhederne som udgangspunkt skal være udbedret før de offentliggøres. Der findes systemer for rapportering og offentliggørelse af sårbarheder, som kan anvendes af alle, og visse leverandører har egne praksisser for dette. De tværsektorielle samarbejder, som kan oprettes i

henhold til DORA-forordningen, og som operatører af finansielle digitale infrastrukturer og andre leverandører kan deltage i, vil kunne danne rammer for udveksling af information om sårbarheder og anden relevant trusselsinformation.

Bestemmelsen implementerer artikel 21, stk. 2, litra e, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 6*, at de i stk. 2 omhandlede foranstaltninger skal omfatte politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici.

Den foreslåede bestemmelse vil indebære, at en operatør af finansiel digital infrastruktur skal have politikker og procedurer, der sikrer, at infrastrukturen vurderer effektiviteten af de tekniske, operationelle og organisatoriske foranstaltninger til styring af bl.a. cybersikkerhedsrisici, som operatøren har truffet i medfør af forslaget til § 333 a, stk. 2, i lov om finansiel virksomhed.

Bestemmelsen implementerer artikel 21, stk. 2, litra f, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 7*, at de i stk. 2 omhandlede foranstaltninger skal omfatte grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

Bestemmelsen indebærer, at en operatør af finansiel digital infrastruktur skal indføre cyberhygiejnepraksisser såsom sikkerhedsopdateringer, sikker konfiguration af enheder hos brugere, netværkssegmentering, identitets- og adgangsstyring og brugerbevidsthed. Desuden skal en operatør arrangere kurser for deres personale og højne bevidstheden om cybertrusler og sikker adfærd for at imødegå f.eks. phishing og social engineering-teknikker.

Bestemmelsen implementerer artikel 21, stk. 2, litra g, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 8*, at de i stk. 2 omhandlede foranstaltninger skal omfatte politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering.

Den foreslåede bestemmelse vil indebære, at en operatør af finansiel digital infrastruktur skal anvende kryptering, hvor det er relevant og muligt. Normalt sondres mellem lagret data, data under overførsel og data i brug. Data under overførsel og lagrede data bør krypteres, hvis en risikovurdering tilsiger det, hvilket næsten altid vil være tilfældet med data under overførsel og i mange tilfælde også for lagrede data, mens data i brug i de fleste tilfælde ikke vil kunne krypteres.

Bestemmelsen implementerer artikel 21, stk. 2, litra h, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 9,* at de i stk. 2 omhandlede foranstaltninger skal omfatte personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver.

Personalesikkerhed omfatter foranstaltninger, der træffes for at sikre at systemer mv. kun er tilgængelige for personer, der har behov for det og som er godkendt til det, herunder fysisk og logisk adgangskontrol, både for almindelige brugere og brugere med udvidede rettigheder, herunder brugere med administratorrettigheder. Politikker og procedurer kan endvidere specificere, hvordan brugerkonti oprettes og nedlægges ved personaleændringer og regler om baggrundstjek af personer, der påtænkes ansat.

Fysisk adgangskontrol har til formål at forhindre at uautoriseret personel får adgang til operatøren af finansiel digital infrastrukturs it-systemer, hvilket kan skabe risiko for kompromittering af it- og cybersikkerheden. På samme vis, skal operatøren indføre foranstaltninger til forvaltning af it-aktiver, herunder data, software og hardware. Sidstnævnte kan f.eks. være foranstaltninger, der mindsker risikoen for tyveri af it-aktiver mv., såsom bærbare computere.

Bestemmelsen implementerer artikel 21, stk. 2, litra i, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 3, nr. 10,* at de i stk. 2 omhandlede foranstaltninger skal omfatte brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos operatøren, hvor det er relevant.

Bestemmelsen implementerer artikel 21, stk. 1, litra j, i NIS 2-direktivet.

Det foreslås i *§ 333 a, stk. 4, 1. pkt.*, at en operatør af finansiel digital infrastruktur, når den overvejer foranstaltninger omhandlet i stk. 3, nr. 4, skal tage hensyn til de sårbarheder, der er specifikke for hver direkte leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder sikkerheden i deres udviklingsprocedurer.

Bestemmelsen supplerer § 333 a, stk. 3, nr. 4, og bestemmelserne om styring af tredjepartsrisici i §§ 333 h, 333 i og 333 j, og implementerer artikel 21, stk. 3, 1. pkt.

Det foreslås endvidere, i *§ 333 a, stk. 4, 2. pkt.,* at en operatør af finansiel digital infrastruktur ved vurderingen efter stk. 3, nr. 4, også skal tage hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der foretages i overensstemmelse med artikel 22, stk. 1, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022, hvor det er relevant og hvor resultaterne af sådanne vurderinger foreligger.

NIS 2-direktivets artikel 22, stk. 1, giver mulighed for at foranstalte koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan. Vurderingerne foretages af samarbejdsgruppen, som oprettes i medfør af NIS 2-direktivets artikel 14, i samarbejde med Kommissionen og ENISA.

Samarbejdsgruppen kan, i samarbejde med Kommissionen og ENISA, foretage koordinerede sikkerhedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder under hensyntagen til både tekniske og ikke-tekniske risikofaktorer.

Hensyntagen til de ovennævnte risikovurderinger vil kun være relevante i situationer, hvor den konkrete, påtænkte leverandør har været genstand for en sådan vurdering eller har relation til andre leverandører eller forsyningskæder, som har været genstand for en koordineret sikkerhedsrisikovurdering.

Bestemmelsen supplerer bestemmelserne om styring af tredjepartsrisici i §§ 333 h, 333 i og 333 j, og implementerer artikel 21, stk. 3, 2. pkt. i NIS 2-direktivet.

Til § 333 b

Den foreslåede § 333 b i lov om finansiel virksomhed indeholder krav til operatører af finansiel digital infrastrukturs styringsmæssige rammer for it- og cyberrisici, herunder krav til de forpligtelser der gælder for bestyrelsen eller ledelsesorganet i operatøren af finansiel digital infrastruktur. Bestemmelsen implementerer dele af NIS 2-direktivet, men indeholder samtidig skærpede krav om it- og cyberrisikostyring for at sikre harmonisering med kravene til it- og cyberrisikostyring i DORA-forordningens kapitel II.

Det foreslås i *§ 333 b, stk. 1,* at bestyrelsen i en operatør af finansiel digital infrastruktur skal fastlægge, godkende, føre tilsyn med og har ansvaret for gennemførelsen af operatørens rammer, foranstaltninger og ordninger for it-

og cyberrisikostyring. Bestyrelsen skal godkende en strategi for digital operationel modstandsdygtighed, hvormed rammerne for it- og cyberrisikostyring gennemføres.

Den foreslåede bestemmelse vil indebære, at bestyrelsen i operatøren af finansiel digital infrastruktur skal fastlægge og godkende rammer, foranstaltninger og ordninger for it- og cyberrisikostyring, der skal forebygge og minimere de it- og cyberrisici, som operatøren udsættes for. For at bestyrelsen skal kunne godkende en ramme, foranstaltninger og ordninger for it- og cyberrisici, skal bestyrelsen også være bekendt med operatørens væsentligste it- og cyberrisici. Bestyrelsen kan f.eks. opnå viden herom ved regelmæssig rapportering fra operatørens it- og cyberrisikostyringsfunktioner.

Bestyrelsen skal endvidere godkende en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan operatørens rammer for it- og cyberrisikostyring gennemføres.

Desuden skal bestyrelsen føre tilsyn med operatørens rammer, foranstaltninger og ordninger for it- og cyberrisikostyring. Bestemmelsen vil indebære, at bestyrelsen skal gennemføre en ordning, hvormed bestyrelsen regelmæssigt modtager rapportering fra den uafhængige kontrolfunktion, der skal føre internt tilsyn med operatørens styring af sine it- og cyberrisici, jf. forslaget til § 333 b, stk. 2, i lov om finansiel virksomhed.

Drives en operatør af finansiel digital infrastruktur som en juridisk person med en bestyrelse, vil det være bestyrelsen, der er ansvarlig for at fastlægge, godkende, føre tilsyn med og gennemføre operatørens rammer, foranstaltninger og ordninger for it- og cyberrisikostyring. Er der tale om en juridisk person uden en bestyrelse, er det det øverste ledelsesorgan, der er ansvarlig herfor. Drives operatøren af finansiel digital infrastruktur som en enkeltmandsvirksomhed, er det indehaveren, der er ansvarlig herfor.

§ 333 b, stk. 1, implementerer artikel 20, stk. 1, i NIS 2-direktivet. Bestemmelsen er dog ikke tekstnært implementeret, da den også er søgt harmoniseret med kravene i DORA-forordningens artikel 5, stk. 2., hvorfor den bl.a. også indeholder skærpede krav om, at bestyrelsen skal godkende en strategi for digital operationel modstandsdygtighed.

Overtrædelse af § 333 b, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er det centrale ledelsesorgan i operatøren af finansiel digital infrastruktur, hvilket enten kan

være bestyrelsen, direktionen, hvis der er tale om en juridisk person uden en bestyrelse, eller indehaveren, hvis der er tale om en enkeltmandsvirksomhed. Den strafbare handling består f.eks. i, at bestyrelsen eller ledelsesorganet ikke har fastlagt og godkendt operatørens rammer, foranstaltninger og ordninger for it- og cyberrisikostyring eller ikke fører tilsyn hermed.

Det foreslås i *§ 333 b, stk. 2*, at en operatør af finansiel digital infrastrukturs tilsyn med styring af sine it- og cyberrisici skal placeres i uafhængige kontrolfunktioner. Operatøren skal sikre adskillelse og uafhængighed mellem it- og cyberrisikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

De foreslåede bestemmelse vil indebære, at den interne revision, der skal forestå tilsynet med it- og cyberrisici, skal være uafhængigt af den daglige ledelse og andre driftsfunktioner i virksomheden. Det er tilsigtet med bestemmelsen er at undgå interessekonflikter mellem f.eks. den daglige ledelse og den interne revision, der kan påvirke den interne revisions vurderinger og beslutninger. Det kan bl.a. være i forhold til at revidere operatørens ramme for styring af it- og cyberrisici, som den interne revision er forpligtet til, jf. forslaget til § 333 b, stk. 4, i lov om finansiel virksomhed. Af samme årsag er det også vigtigt, at operatøren af finansiel digital infrastruktur sikrer adskillelse og uafhængighed mellem it- og cyberrisikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer, eller en intern model som sikrer et tilsvarende beskyttelsesniveau, jf. DORA-forordningens artikel 6, stk. 4. Modellen med tre forsvarslinjer harmonerer med de krav til funktionsadskillelse, der stilles til virksomheder på det finansielle område.

For at en intern model for risikostyring og kontrol kan anerkendes efter bestemmelsen, skal modellen mindst sikre et niveau af beskyttelse og uafhængighed, som svarer til en model med 3 uafhængige forsvarslinjer.

Overtrædelse af § 333 b, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i at der ikke findes tre forsvarslinjer med en klar adskillelse af risikostyring, kontrolfunktion og den interne revisionsfunktion. Den strafbare handling kan også bestå i ikke at have en intern model, der sikrer samme niveau af beskyttelse som modellen med tre forsvarslinjer.

Det foreslås i *§ 333 b, stk. 3,* at rammen for styring af it- og cyberrisici skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it- eller cyberhændelser, og i overensstemmelse med tilsynsmæssige instrukser eller som følge af observationer efter test eller revisioner. Rammen skal forbedres løbende på grundlag af opnåede erfaringer og at en operatør af finansiel digital infrastruktur skal kunne dokumentere sin gennemgang af rammen for it- og cyberrisikostyring i en samlet rapport.

Bestemmelsen vil indebære, at operatøren af finansiel digital infrastruktur løbende skal revidere og forbedre sin ramme for styring af it- og cyberrisici på baggrund af de erfaringer, som operatøren gør sig. Bestemmelsen vil også indebære, at operatøren mindst én gang om året skal gennemgå rammen, og at dette dokumenteres i en samlet rapport.

Det foreslås i *§ 333 b, stk. 4, 1. pkt.,* at en operatør af finansiel digital infrastrukturs interne revision regelmæssigt skal revidere rammen for styring af it- og cyberrisici.

Den foreslåede bestemmelse indebærer, at den interne revision bl.a. på baggrund af sit kendskab til operatørens væsentligste it- og cyberrisici og sit tilsyn med styringen heraf, jf. det foreslåede § 333 b, stk. 2, 1. pkt., regelmæssigt skal revidere rammen for styring af it- og cyberrisici.

Det foreslås i *§ 333 b, stk. 4, 2. pkt.,* at den interne revision skal have tilstrækkelige viden, faglig kompetence og ekspertise til udførelsen af denne opgave.

Den foreslåede bestemmelse indebærer, at den interne revision skal have tilstrækkelig viden, faglig kompetence og ekspertise til at kunne revidere operatørens ramme for styring af it- og cyberrisici. Det betyder, at interne revision både uddannelsesmæssigt og erfaringsmæssigt skal have tilstrækkelig ekspertise til at kunne udføre opgaven. Det vil også betyde, at den interne revision løbende bør holde sig opdateret på cybertrusler og nye tiltag for at mindske it- og cyberrisici for også på den måde at kunne vurdere, om der evt. skal ske ændringer af operatørens ramme for styring af it- og cyberrisici.

Overtrædelse af § 333 b, stk. 4, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at foretage regelmæssig intern revision af rammerne for styring af it- og cyberrisici.

Den strafbare handling kan også bestå i ikke at have sikret den interne revisions kompetenceniveau.

Det foreslås i *§ 333 b, stk. 5,* at en operatør af finansiel digital infrastruktur skal oprette en funktion med henblik på overvågning af ordninger, der er indgået med tredjepartsudbydere om it-ydelser, eller udpege et direktionsmedlem som ansvarlig for tilsyn og dokumentation i forbindelse med eksponering for it- og cyberrisici fra tredjepartsudbydere.

Den foreslåede bestemmelse vedrører oprettelsen af en funktion til overvågning af ordninger om outsourcing af it-funktioner. Den foreslåede bestemmelse har bl.a. til formål at sikre, at en operatør af finansiel digital infrastruktur ved overvågning af disse ordninger får et overblik over de risici, der kan opstå fra tredjepartsudbydere af it-ydelser. Dette både i forhold til at kunne vurdere, om tredjepartsudbyderen skal foretage sig yderligere for at mindske en given risiko, men også for selv at kunne træffe de nødvendige foranstaltninger til at kunne styre disse risici, jf. forslaget til § 333 h, stk. 1, og hermed sikre operatørens modstandsdygtighed.

Funktionen kan også forankres ved udpegning af et medlem af operatørens direktion, som er ansvarlig for tilsyn og dokumentation i forbindelse med tredjepartsrisici på det digitale operationelle område.

Overtrædelse af § 333 b, stk. 5, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at overvåge ordninger med tredjepartsudbydere om it-ydelser, eller i ikke at føre tilsyn med og sikre dokumentation for de it- og cyberrisici som ordningen indebærer.

Det foreslås i *§ 333 b, stk. 6,* at en operatør af finansiel digital infrastruktur skal oprette en funktion til krisestyring, som skal håndtere større it- og cyberhændelser, der medfører aktivering af beredskabsplaner, forretningskontinuitetsplaner eller genopretningsplaner, og være ansvarlig for kommunikationen i forbindelse hermed.

Den foreslåede bestemmelse vil indebære, at operatøren af finansiel digital infrastruktur skal oprette en funktion til krisestyring i tilfælde af større it- og cyberhændelser, hvor det er nødvendigt enten at aktivere operatørens beredskabsplaner, forretningskontinuitetsplaner eller genopretningsplaner. I den forbindelse vil funktionen til krisestyring være ansvarlig for håndteringen af den pågældende it- eller cyberhændelse. Funktionen vil også skulle sikre en konsekvent håndtering af hændelsen, jf. forslaget til §

333 f, stk. 2, alt efter om det er en beredskabsplan, forretningskontinuitetsplan eller genopretningsplan, der bliver aktiveret.

Desuden vil den foreslåede bestemmelse indebære, at funktionen til krisestyring skal være ansvarlig for krisekommunikation i forbindelse med en it- eller cyberhændelse. Det gælder både intern kommunikation til personalet i de forskellige funktioner hos operatøren, men også eksternt i forhold til kunder og modparter og offentligheden, alt efter hvad der er relevant.

Med bestemmelsen søges det at harmonisere kravene til operatører af finansielle digitale infrastrukturer med det tilsvarende krav, der følger af artikel 11, stk. 7, i DORA-forordningen.

Overtrædelse af § 333 b, stk. 6, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i, at operatøren ikke opretter en funktion til krisestyring.

Det foreslås i *§ 333 b, stk. 7,* at bestyrelsesmedlemmerne af en operatør af finansiel digital infrastruktur aktivt skal vedligeholde den viden og de færdigheder, der er nødvendige for at forstå og vurdere it- og cyberrisici og disses indvirkning på driften af operatøren, herunder ved regelmæssigt at følge undervisning, som er passende i forhold til de it- og cyberrisici, som operatøren og dens kunder er eksponeret for.

Bestemmelsen vil indebære, at medlemmerne af en operatør af finansiel digital infrastrukturs bestyrelse aktivt skal sørge for at tilegne sig viden og færdigheder, der er nødvendige for at forstå og vurdere it- og cyberrisici, og den indvirkning de har på driften af operatøren. Dette skal bl.a. ske ved at følge undervisning om it- og cyberrisici i henhold til et niveau svarende til de it- og cyberrisici, som operatøren og dens kunder er eksponeret for. Derudover kan det f.eks. være nødvendigt at opnå viden om et aktuelt trusselsbillede, der kan have indflydelse på operatørens it- og cyberrisici, eller viden om de risici som tredjeparter af it-ydelser er eksponeret for, som også kan have betydning for operatørens it- og cyberrisici.

Den foreslåede bestemmelse implementerer NIS 2-direktivets artikel 20, stk. 2, og indebærer en harmonisering af reglerne for uddannelse og kompetenceudvikling af medlemmer af bestyrelser og ledelsesorganer for operatører af finansielle digitale infrastrukturer med de tilsvarende regler for virksomheder omfattet af reglerne i artikel 5, stk. 4, i DORA-forordningen.

Det foreslås i *§ 333 b, stk. 8,* at stk. 1 og 7, finder tilsvarende anvendelse for det øverste ledelsesorgan når en operatør af finansiel digital infrastruktur drives som en juridisk person uden en bestyrelse.

Forslaget medfører, at forpligtelsen til at fastlægge, godkende og føre tilsyn med rammer, foranstaltninger og ordninger for it- og cyberrisikostyring, påhviler det øverste ledelsesorgan i de tilfælde, hvor en operatør af finansiel digital infrastruktur drives som en juridisk person uden en bestyrelse. Tilsvarende gælder forpligtelsen til at godkende strategien for digital operationel modstandsdygtighed. Med det øverste ledelsesorgan forstås den eller de personer, der har ansvaret for operatørens overordnede ledelse. Hvor operatøren eksempelvis drives som en juridisk person, der alene har en direktion, men ingen bestyrelse, vil det være direktionen, der har ansvaret for operatørens overordnede ledelse. Det vil dermed være direktionen, der er operatørens øverste ledelsesorgan, i overensstemmelse med definitionen heraf i § 5 i selskabsloven.

Forslaget medfører endvidere, at forpligtelsen til aktivt at vedligeholde den viden og de færdigheder, der er nødvendige for at forstå og vurdere it- og cyberrisici og disses indvirkning på driften af operatøren af finansiel digital infrastruktur, påhviler det øverste ledelsesorgan i de tilfælde, hvor en operatør drives som en juridisk person uden en bestyrelse.

Det foreslås i *§ 333 b, stk. 9,* at stk. 1 og 7, finder tilsvarende anvendelse for indehavere når en operatør af finansiel digital infrastruktur drives som en enkeltmandsvirksomhed eller et interessentskab.

Forslaget medfører, at forpligtelsen til at fastlægge, godkende og føre tilsyn med rammer, foranstaltninger og ordninger for it- og cyberrisikostyring, påhviler indehaveren eller indehaverne i de tilfælde, hvor en operatør af finansiel digital infrastruktur drives som en enkeltmandsvirksomhed eller et interessentskab. Tilsvarende gælder forpligtelsen til at godkende strategien for digital operationel modstandsdygtighed.

Forslaget medfører endvidere, at forpligtelsen til aktivt at vedligeholde den viden og de færdigheder, der er nødvendige for at forstå og vurdere it- og cyberrisici og disses indvirkning på driften af operatøren af finansiel digital infrastruktur, påhviler indehaveren i de tilfælde, hvor operatøren drives som en enkeltmandsvirksomhed eller et interessentskab.

Til § 333 c

Virksomheder på det finansielle område, der er omfattet af DORA-forordningen, kan i henhold til artikel 6, stk. 10, i forordningen outsource

opgaver, der er forbundet med efterprøvning af deres overholdelse af forordningens krav til it- og cyberrisikostyring til eksterne virksomheder med det forbehold, at virksomhederne stadig er fuldt ud ansvarlige for efterprøvningen og overholdelsen af forordningens krav.

Det foreslås derfor i *§ 333 c*, at en operatør af en finansiel digital infrastruktur skal dokumentere anvendelsen af sin ramme for styring af it- og cyberrisici i forhold leverancer, der er nødvendige for kritiske og vigtige funktioner hos kunder, som er omfattet af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede bestemmelse har til formål at fremme samarbejdet mellem operatører af finansielle digitale infrastrukturer og virksomheder på det finansielle område, der er omfattet DORA-forordningen, jf. artikel 2 i forordningen.

Den foreslåede bestemmelse vil bevirke, at en operatør af finansiel digital infrastruktur skal dokumentere sin anvendelse af sin ramme for styring af it- og cyberrisici i forhold til leverancer, der er nødvendige for kritiske og vigtige funktioner hos virksomheder omfattet af DORA-forordningen. Denne dokumentation skal medvirke til at gøre det tydeligt for kundevirksomheder, om operatøren af finansiel digital infrastruktur lever op til de krav for it- og cyberrisikostyring, som gælder for virksomheder omfattet af DORA-forordningen. En operatørs dokumentation for sin anvendelse af rammen for styring af it- og cyberrisici, vil derfor gøre det nemmere for kundevirksomheder omfattet af DORA-forordningen løbende at føre tilsyn med, om operatøren lever op til de krav til styring af it- og cybersikkerhed, som kunden har stillet mhp. at efterleve DORA-forordningen.

Til § 333 d

Det foreslås i § 333 d at fastsætte nærmere regler om operatører af finansielle digitale infrastrukturers styring af it- og cyberrisici med udgangspunkt i de regler, der følger af artikel 6 i DORA-forordningen, og som gælder for virksomhederne på det finansielle område, der er omfattet af forordningen.

Det foreslås i *§ 333 d, stk. 1*, at den ramme for it- og cyberrisikostyring, som en operatør af finansiel digital infrastruktur skal have, jf. § 333 a, skal omfatte en overordnet strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen skal gennemføres.

Den foreslåede bestemmelse vil medføre, at en operatør af finansiel digital infrastruktur skal have en strategi for digital operationel modstandsdygtighed, ligesom virksomheder på det finansielle område er forpligtede til i henhold til artikel 6, stk. 8, i DORA-forordningen. Strategien skal konkretisere risikostyringsrammerne ved at fastsætte mål og metoder mv. i forbindelse med anvendelsen af rammen for it- og cyberrisikostyring, der skal forebygge it- og cybersikkerhedshændelser og minimere en hændelses indvirkning på de tjenester, som operatøren leverer.

Overtrædelse af § 333 d, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have en strategi for digital operationel modstandsdygtighed, der konkretiserer risikostyringsrammen ved at fastsætte mål og metoder for anvendelsen af rammen for it- og cyberrisikostyring.

Det foreslås i *§ 333 d, stk. 2,* at en operatør af finansiel digital infrastruktur med passende mellemrum skal foretage identifikation og vurderinger af alle væsentlige it- og cyberrisici, som operatøren og dennes ydelser er eksponeret for.

Den foreslåede bestemmelse vil medføre, at en operatør af finansiel digital infrastruktur skal foretage identifikation og vurdering af alle væsentlige it- og cyberrisici, som kan påvirke operatøren og de ydelser som operatøren leverer. Kravet om identifikation og vurdering af de væsentlige risici skal ses i sammenhæng med kravet om at fastsætte en ramme for it- og cyberrisikostyring, jf. den foreslåede § 333a, stk. 1, og kravet i det foreslåede stk. 1 om at fastsætte en strategi for digital operationel modstandsdygtighed. For at kunne opfylde disse krav er det en forudsætning, at operatøren kender karakteren og omfanget af de væsentlige it- og cyberrisici, som den er eksponeret for.

Da risikobilledet løbende ændrer sig, er det nødvendigt, at operatøren af finansiel digital infrastruktur foretager en identifikation og vurdering af risici med passende mellemrum for på baggrund heraf at kunne tilpasse rammen og den overordnede strategi for digital operationel modstandsdygtighed. Det vil derfor konkret afhænge af operatørens størrelse, kundegrundlag og betydningen af de tjenester, som operatøren leverer for det finansielle system, hvilke intervaller for risikoidentifikation og vurdering, der anses for passende.

Overtrædelse af § 333 d, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af §

372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have identificeret væsentlige it- og cyberrisici som både operatøren, men også de ydelser som infrastrukturen leverer, er eksponeret for.

Det foreslås i *§ 333 d, stk. 3,* at rammen for it- og cyberrisikostyring som minimum skal omfatte strategier, politikker, procedurer, og foranstaltninger, som er nødvendige for at beskytte al fysisk og digital infrastruktur og data i overensstemmelse med de identificerede risici, herunder software, hardware, servere, netværk og relaterede fysiske komponenter og infrastrukturer, såsom lokaler, datacentre og sensitive udpegede områder mod risici, som f.eks. skade og uautoriseret adgang eller brug.

Den foreslåede bestemmelse stiller minimumskrav til indholdet af risikostyringsrammen hos en operatør af finansiel digital infrastruktur og genstandsområdet for dennes foranstaltninger til risikostyring, herunder den fysiske og digitale infrastruktur. Hvor udformningen af strategien vil skulle anvendes til at konkretisere risikostyringsrammerne ved bl.a. at fastsætte mål og metoder herfor, vil politikker og procedurer skulle anvendes til at fastsætte nærmere regler på et mere konkret niveau f.eks. grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse.

Beskyttelsen af digital infrastruktur vil typisk bestå i at beskytte mod cyberangreb og uautoriseret digital adgang til systemerne. Beskyttelsen af fysisk infrastruktur, såsom hardware og servere består f.eks. i at beskytte systemerne mod skader som følge af f.eks. brand eller oversvømmelse samt mod uautoriseret fysisk adgang.

Overtrædelse af § 333 d, stk. 3, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at overholde minimumskravene til indholdet af risikostyringsrammen.

Det foreslås i *§ 333 d, stk. 4, 1. pkt.,* at en operatør af finansiel digital infrastruktur skal modvirke de potentielle virkninger af it- og cyberrisici ved at indføre passende strategier, politikker, procedurer og foranstaltninger.

Den foreslåede bestemmelse angiver de væsentligste styringsmæssige redskaber, som en operatør af finansiel digital infrastruktur skal gøre brug af til udmøntning af sin styring af de identificerede it- og cyberrisici. Hvor udformningen af strategien skal anvendes til at konkretisere risikostyringsrammerne ved bl.a. at fastsætte mål og metoder herfor, skal

politikker og procedurer anvendes til at fastsætte nærmere regler ned på et mere konkret niveau f.eks. grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse. Foranstaltningerne til at modvirke it- eller cyberrisici kan omfatte foranstaltninger af enhver art, herunder anvendelse af værktøjer, protokoller, metoder og systemer.

Det foreslås i *§ 333 d, stk. 4, 2. pkt.,* at operatøren efter anmodning skal forelægge fuldstændige og ajourførte oplysninger om sine it- og cyberrisici og om sin ramme for it- og cyberrisikostyring for Finanstilsynet.

Den foreslåede bestemmelse medfører, at en operatør af finansiel digital infrastruktur har pligt til at dokumentere sine risici og styringen af disse for Finanstilsynet efter anmodning fra Finanstilsynet. En sådan anmodning kan blive relevant i forbindelse med, at Finanstilsynet udfører tilsyn med operatøren.

Overtrædelse af § 333 d, stk. 4, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digitale infrastruktur. Den strafbare handling består f.eks. i ikke at indføre strategier, politikker, procedurer, protokoller og værktøjer, der skal modvirke de potentielle virkninger af it- og cyberrisici. Den kan også bestå i ikke at forelægge fuldstændige og ajourførte oplysninger om it- og cyberrisici og om rammen for it- og cyberrisikostyring for Finanstilsynet, hvis Finanstilsynet har anmodet herom.

Til § 333 e

Det foreslås i § 333 e at fastsætte regler om en operatør af finansiel digital infrastrukturs identifikation af forretningsfunktioner mv. og de for forretningsfunktionerne nødvendige infrastrukturer, i overensstemmelse med de tilsvarende forpligtelser for virksomheder omfattet af DORA-forordningens artikel 8. Det foreslås desuden i § 333 e at fastsætte regler om foranstaltninger til beskyttelse af disse infrastrukturer og forebyggelse af sikkerhedshændelser, svarende til forpligtelserne efter DORA-forordningens artikel 9.

Det foreslås i *§ 333 e, stk. 1,* at en operatør af finansiel digital infrastrukturs it-systemer, it-protokoller og it-værktøjer skal være pålidelige og med tilstrækkelig kapacitet til rettidigt at håndtere de nødvendige transaktioner m.v. i situationer med spidsbelastning, herunder uventet høje spidsbelastninger.

Den foreslåede bestemmelse fastsætter en forpligtelse til, at kapaciteten i operatøren af den digitale infrastrukturs it-systemer skal kunne håndtere spidsbelastninger, der står i rimeligt forhold til operatørens størrelse og risiko. It-systemerne skal være pålidelige nok til at sikre, at de i tilstrækkelig grad kan håndtere yderligere behandlingsrelaterede behov som følge af stressede markedsforhold eller andre vanskelige situationer.

Overtrædelse af § 333 e, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have it-systemer, it-protokoller og it-værktøjer, der er pålidelige og kan håndtere situationer med uventet høj belastning.

Det foreslås i *§ 333 e, stk. 2,* at en finansiel digital infrastruktur løbende skal identificere alle kritiske forretningsfunktioner og it-aktiver, herunder it-aktiver, der understøtter kritiske og vigtige forretningsfunktioner for operatørens kunder.

Bestemmelsen vil medføre, at operatører af finansielle digitale infrastrukturer løbende skal identificere alle kritiske forretningsfunktioner og it-aktiver. Det gælder bl.a. de it-aktiver, der understøtter kritiske og vigtige forretningsfunktioner hos operatørens kunder. Kravet om løbende identifikation af disse forretningsfunktioner og it-aktiver vil være med til at sikre, at operatøren kontinuerligt kan forebygge, opdage, reagere på og reetablere sig efter hændelser og til at afbøde deres indvirkning ved et cyberangreb.

Overtrædelse af § 333 e, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have identificeret kritiske forretningsfunktioner og it-aktiver, herunder dem der understøtter kritiske og vigtige funktioner for deres kunder.

Det foreslås i *§ 333 e, stk. 3,* at en operatør af finansiel digital infrastruktur skal identificere alle kritiske eller vigtige forretningsprocesser og tjenester, der er afhængige af eksterne leverandører, og dokumentere egne og kunders afhængigheder af ydelser fra underleverandører.

Den foreslåede bestemmelse skal være med til at sikre både operatøren af finansiel infrastruktur og dens kunder mod tredjepartsrisici. For at forebygge, opdage og kunne reagere på og reetablere sig efter hændelser, samt afbøde deres indvirkning ved et cyberangreb, skal operatøren

identificere alle kritiske eller vigtige forretningsprocesser og tjenester, der er afhængige af eksterne leverandører, og dokumentere egne og kunders afhængigheder af ydelser fra underleverandører.

Overtrædelse af § 333 e, stk. 3, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have identificeret kritiske forretningsfunktioner og it-aktiver, som er afhængige af eksterne leverandører, og ikke at dokumentere egne og kundernes afhængighed af ydelserne fra operatørens eksterne leverandører.

Det foreslås i *§ 333 e, stk. 4,* at en operatør af finansiel digital infrastruktur skal overvåge og kontrollere it-systemernes og it-værktøjernes funktion og sikkerhed og minimere virkningerne af it- og cyberrisici ved at indføre passende sikkerhedsværktøjer, -politikker og -procedurer. Operatøren skal løbende identificere potentielle sårbarheder og single points of failure.

Den foreslåede bestemmelse vil medføre, at en operatør af finansiel digital infrastruktur løbende skal overvåge sine it-systemer mv. i forhold til disse funktioner og sårbarheder samt single points of failure. Bestemmelsen medfører desuden, at en operatør løbende skal minimere de risici som dens it-systemer mv. er eksponeret for.

Bestemmelsens krav om overvågning vil skulle medvirke til at identificere sårbarheder i den finansielle infrastrukturs it-systemer. Overvågningen skal således gøre det muligt hurtigt at konstatere og detektere risikokilder, som fører til sårbarheder i it-systemet, der medfører behov for en øget beskyttelse og forebyggelse af cyberangreb.

Overtrædelse af § 333 e, stk. 4, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke løbende at overvåge sine it-systemer. Den strafbare handling kan også bestå i ikke at minimere den risici som deres it-systemer er udsat for.

Det foreslås i *§ 333 e, stk. 5,* at en operatør af finansiel digital infrastruktur skal udforme og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der er egnede til at sikre modstandsdygtighed, stabilitet og tilgængelighed for it-systemer, der understøtter kritiske eller vigtige funktioner og til at opretholde et højt niveau af tilgængelighed, autenticitet, integritet og fortrolighed af data.

Vurderingen af hvornår it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer er egnede, skal baseres på en risikovurdering og ske under hensyntagen til proportionalitetsprincippet. Der er tale om et overordnet krav til operatørens styring, som skal vurderes ud fra de tilsynsmæssige krav til de virksomheder, hvis kritiske eller vigtige forretningsfunktioner er afhængige af operatørens ydelser. Operatørens sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer skal følge en risikobaseret tilgang for en forsvarlig forvaltningskultur. EU-Kommissionen ventes i øvrigt at vedtage en gennemførelsesforordning med reguleringsmæssige tekniske standarder for dette område. Finanstilsynet foreslås med lovforslagets bestemmelse til § 333 p i lov om finansiel virksomhed tillagt en beføjelse til at fastsætte nærmere regler for finansielle digitale infrastrukturer, herunder på dette område.

Overtrædelse af § 333 e, stk. 5, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have vedtaget tilstrækkelige it-sikkerhedspolitikker, -procedurer, protokoller og -værktøjer til at sikre modstandsdygtigheden, stabiliteten og tilgængeligheden af forretningskritiske funktioner.

Det foreslås i *§ 333 e, stk. 6,* at en operatør af finansiel digital infrastruktur skal indføre mekanismer til overvågning og sporing af anormale aktiviteter, trusler og hændelser i relevant infrastruktur og fastsætte tærskler for igangsættelse af indsats- og beredskabsforanstaltninger.
Det er tiltænkt, at mekanismerne skal have til formål at sikre en effektiv og hurtigt reagerende koordinering ved håndteringen af it-relaterede hændelser, navnlig cyberangreb.

Den foreslåede bestemmelse supplerer DORA-forordningens artikel 10 om detektion.

Overtrædelse af § 333 e, stk. 6, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke løbende at have overvåget og sporet anormale aktiviteter, trusler og hændelser. Den kan f.eks. også bestå i ikke at have tærskler for igangsættelse af indsats- og beredskabsforanstaltninger.

Det foreslås i *§ 333 e, stk. 7,* at en operatør af finansiel digital infrastruktur skal indføre en politik for it-driftsstabilitet.

Den foreslåede bestemmelse vil indebære, at en finansiel digital infrastruktur skal have en politik for it-driftsstabilitet som led i sin ramme for it- og cyberrisikostyring. Politikken skal medvirke til at sikre, at infrastrukturen har effektive planer for driftsstabilitet og genopretning, så den hurtigt kan finde en løsning på it-relaterede hændelser, herunder cyberangreb, ved at begrænse skaden og prioritere genoptagelsen af infrastrukturens aktiviteter.

Den foreslåede bestemmelse supplerer den foreslåede bestemmelse i § 333 a, stk. 3, nr.3, der implementerer NIS 2-direktivets artikel 21, stk. 2, litra c. De tilsluttede finansielle enheder er omfattet af et tilsvarende krav i DORA-forordningens artikel 11, hvorfor den foreslåede bestemmelse også vil understøtte disse enheders opfyldelse af DORA-forordningen.

Overtrædelse af § 333 e, stk. 7, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have en politik for it-driftsstabilitet.

Det foreslås i *§ 333 e, stk. 8, nr. 1-5*, at en operatør af finansielle digitale infrastruktur skal gennemføre politikken for it-driftsstabilitet, jf. stk. 7, ved hjælp af dokumenterede beredskabsplaner, ordninger, procedurer mv., med henblik på 1) at sikre, at den finansielle digitale infrastrukturs og dennes kunders kritiske eller vigtige funktioner er stabile, 2) hurtigt, passende og effektivt at sætte ind over for og løse alle it-relaterede hændelser på en måde, der begrænser skaden og prioriterer genoptagelsen af aktiviteter og genopretningstiltag, 3) omgående at aktivere planer, der omfatter inddæmningsforanstaltninger, der er passende i forhold til hændelserne og som forhindrer yderligere skade, 4) at anslå foreløbige virkninger, skader og tab, og 5) at indføre kommunikations- og krisestyringstiltag, der sikrer, at ajourførte oplysninger videresendes til al relevant internt personale og eksterne interessenter og indberettes til Finanstilsynet.

Den foreslåede bestemmelse fastsætter krav om, at en operatør af finansiel digital infrastrukturs skal gennemføre sin politik for it-driftsstabilitet, jf. det foreslåede stk. 7, ved hjælp af dokumenterede beredskabsplaner, ordninger, procedurer mv. Bestemmelsen konkretiserer derved udmøntningen af politikken for it-driftsstabilitet og indeholder dokumentationskrav hertil.

Bestemmelsen fastsætter endvidere i nr. 1-5, at gennemførelsen af politikken specifikt skal ske med henblik på, at sikre stabiliteten i de kritiske funktioner, en effektiv løsning af it-hændelser, at foranstalte begrænsninger af evt. hændelsers konsekvenser, at anslå virkninger og tab mv. samt

kommunikations- og krisestyringstiltag i forhold til at informere alle relevante interessenter og Finanstilsynet. Operatøren skal derfor ved udarbejdelsen af sine beredskabsplaner, ordninger, procedurer mv. tage udgangspunkt i de hensyn, der er oplistet i nr. 1-5.

Overtrædelse af § 333 e, stk. 8, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet for overtrædelse er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at gennemføre politikken for it-driftsstabilitet ved brug af dokumenterede beredskabsplaner, ordninger, procedurer mv., der bl.a. sikrer, at både kritiske eller vigtige funktioner hos operatøren og hos operatørens kunder, er stabile. Den strafbare handling kan f.eks. også bestå i ikke at have ordninger mv., der sikrer, at operatøren hurtigt og på tilstrækkelig vis kan reagere på it-relaterede hændelser. Den kan f.eks. også bestå i ikke at have indført procedurer eller ordninger for kommunikations- og krisestyringstiltag, der sikrer, at al nødvendig information rettidigt videresendes til alle interne og eksterne interessenter, herunder til Finanstilsynet. Hvad, der er nødvendig information, og hvem der er relevante interessenter, vil afhænge af den pågældende krises karakter. Relevante interessenter kan være enhver, der er berørt af den hændelse, der har udløst krisen, herunder kunder, medarbejdere, modparter, leverandører, investorer, myndigheder, eller andre der bliver berørt eller har risiko for, direkte eller indirekte at blive berørt af hændelsen.

Det foreslås i *§ 333 e, stk. 9, 1. pkt.*, at en operatør af finansiel digital infrastruktur skal have politikker og procedurer for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene.

Den foreslåede bestemmelse stiller krav om, at en operatør af finansiel digital infrastruktur skal have politikker og procedurer for sikkerhedskopiering. Politikkerne og procedurerne vil skulle præcisere omfanget af de data, der er genstand for sikkerhedskopiering. Politikkerne og procedurerne vil også skulle fastlægge minimumshyppigheden af sikkerhedskopieringen, som skal være baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Der bør i den forbindelse foretages hyppigere sikkerhedskopiering, jo mere kritisk betydning dataene har eller af jo mere fortrolige disse er.

Bestemmelsen supplerer den foreslåede bestemmelse til § 333 a, stk. 3, nr. 3, der implementerer NIS 2-direktivets artikel 21, stk. 2, litra c. Bestemmelsen skal i øvrigt ses i sammenhæng med DORA-forordningens

artikel 12, som specificerer en række minimumskrav til politikkerne for sikkerhedskopiering, gendannelse og genopretning for de virksomheder, der er kunder for operatører af finansiel digital infrastruktur, og som er omfattet af forordningen.

Det foreslås i *§ 333 e, stk. 9, 2. pkt.*, at operatøren endvidere skal have procedurer og metoder for gendannelse og genopretning efter væsentlige hændelser.

Overtrædelse af § 333 e, stk. 9, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have politikker og procedurer for sikkerhedskopiering. Den strafbare handling kan også bestå i, at en politik eller procedure for sikkerhedskopiering, der ikke nævner noget om omfanget af de data, der er genstand for sikkerhedskopiering eller minimumshyppigheden for sikkerhedskopiering, eller i ikke at have procedurer for gendannelse af data efter væsentlige hændelser.

Det foreslås i *§ 333 e, stk. 10*, at en operatør af finansiel digital infrastruktur regelmæssigt skal teste sine foranstaltninger til beredskab, indsats, genopretning, sikkerhedskopiering og gendannelse.

Den foreslåede bestemmelse stiller krav til regelmæssig test af foranstaltningerne til beredskab, indsats, genopretning, sikkerhedskopiering og gendannelse. Det er hensigten, at de regelmæssige test skal være med til at sikre effektiviteten foranstaltningerne. Testene bør derfor omfatte en bred vifte af værktøjer og tiltag, der spænder lige fra vurderingen af grundlæggende krav, herunder f.eks. sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerhed, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest eller end-to-end-test til mere avancerede test ved hjælp af TLPT.

Bestemmelsen supplerer den foreslåede bestemmelse i § 333 a, stk. 3, nr. 6, der implementerer NIS 2-direktivets artikel 21, stk. 2, litra f. Den foreslåede bestemmelse skal endvidere ses i sammenhæng med DORA-forordningens artikel 11, stk. 4, og 6, som gælder for virksomheder, der er kunder for operatører af finansiel digital infrastruktur, og som er omfattet af DORA-forordningen

Overtrædelse af § 333 e, stk. 10, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i, at en operatør ikke regelmæssigt tester sine foranstaltninger til beredskab, indsats, genopretning, sikkerhedskopiering og gendannelse.

Det foreslås i *§ 333 e, stk. 11*, at en operatør af finansiel digital infrastruktur skal udvikle politikker for en systematisk læring på baggrund af den viden, som operatøren opnår ved opfølgning på sin ramme for risikostyring, trusselsovervågning, testresultater og it- og cyberhændelser. Den opnåede viden skal danne grundlag for en årlig rapportering til ledelsesorganet med anbefalinger til forbedringer i relevant omfang.

Den foreslåede bestemmelse vil medføre, at en operatør af finansiel digital infrastruktur forpligtes til at udvikle politikker for en systematisk læring, der bruger den viden og erfaring, som operatøren opnår, til løbende forbedring af sine rammer. Med bestemmelsen vil operatøren endvidere blive forpligtet til at give operatørens ledelsesorgan en årlig rapportering med eventuelle anbefalinger på baggrund af den læring, som operatøren har gjort sig.

Ledelsesorganet skal forstås som operatørens bestyrelse, hvis operatøren har en bestyrelse. Drives en operatøren som en juridisk person uden en bestyrelse skal der ved ledelsesorganet forstås direktionen. Drives operatøren som enkeltmandsvirksomhed eller interessentskab forstås ved ledelsesorganet operatørens indehavere.

Overtrædelse af § 333 e, stk. 11, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at indføre en politik for læring på baggrund af den viden, som den finansielle digitale infrastruktur opnår ved sin opfølgning på sin ramme for risikostyring, trusselsovervågning, testresultater og it- og cyberhændelser. Den strafbare handling kan også bestå i ikke at foretage en årlig rapportering til operatørens ledelsesorgan på baggrund af den opnåede viden.

Det foreslås i § *333 e, stk. 12*, at en operatør af finansiel digital infrastruktur skal have beredskab for krisekommunikation og ansvarlig offentliggørelse af oplysninger om større cyberhændelser eller væsentlige sårbarheder til berørte parter, herunder kunder, modparter og offentligheden.

Den foreslåede bestemmelse vil indebære en forpligtelse for operatøren af finansiel digital infrastruktur til at indføre planer for krisekommunikation

og ansvarlig offentliggørelse af information om større it- og cyberhændelser og væsentlige cybertrusler til alle berørte parter.

Bestemmelsen skal ses i sammenhæng med DORA-forordningens artikel 14.

Til § 333 f

Det foreslås i § 333 f i lov om finansiel virksomhed fastsætterkrav til finansielle digitale infrastrukturers håndtering og rapportering af væsentlige hændelser.

Det foreslås i *§ 333 f, stk. 1,* at en operatør af finansiel digital infrastruktur skal fastlægge og følge en proces for overvågning, styring og indberetning af it- og cyberhændelser.

Den foreslåede bestemmelse vil indebære, at en operatør af finansiel digital infrastruktur skal fastlægge og følge nødvendige foranstaltninger til at sikre en korrekt overvågning, styring og indberetning af it- og cyberhændelser. Dette har til formål at sikre til hurtig kommunikation og koordination både intern og eksternt i tilfælde it- og cyberhændelser.

Med bestemmelsen søges det at harmonisere kravene for operatører af finansielle digitale infrastrukturer med det krav, der følger af artikel 17, stk. 1, i DORA-forordningen. Bestemmelsen supplerer desuden kravet i den foreslåede bestemmelse til § 333 a, stk. 3, nr. 2, i lov om finansiel virksomhed, der implementerer NIS 2-direktivets artikel 21, stk. 2, litra b, og supplerer kravene, der følger af artikel 23 i NIS 2-direktivet.

Overtrædelse af § 333 f, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at fastlægge eller følge en proces for hændelsesstyring og -indberetning.

Det foreslås i *§ 333 f, stk. 2, 1. pkt.,* at en operatør af finansiel digital infrastruktur skal registrere alle it- og cyberhændelser og væsentlige cybertrusler.

Det foreslås i *§ 333 f, stk. 2, 2. pkt.,* at operatøren skal fastlægge passende procedurer, der sikrer en konsekvent og integreret overvågning, håndtering og opfølgning af it- og cyberhændelser og at de grundlæggende årsager identificeres, dokumenteres og håndteres.

Den foreslåede bestemmelse vil indebære, at operatøren af finansiel digital infrastruktur vil skulle dokumentere og analysere deres it- og cyberhændelser, bl.a. med henblik på at identificere deres grundlæggende årsager.

Såfremt operatøren varetager operationelle opgaver på betalingsområdet for kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere eller e-pengeinstitutter, så vil operatøren i relevant omfang skulle registrere operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser.

Overtrædelse af § 333 f, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed.

Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i at operatøren ikke i relevant omfang registrerer operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser, jf. DORA-forordningens artikel 23.

Det foreslås i *§ 333 f, stk. 3, 1. pkt.*, at en operatør af finansiel digital infrastruktur skal indberette væsentlige it- og cyberhændelser til Finanstilsynet og CSIRT'en oprettet i medfør af artikel 10, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022.

Center for Cybersikkerhed er udpeget som CSIRT i Danmark.

Indberetningspligten vil omfatte såvel hændelser, der kategoriseres som større i henhold til DORA-forordningen og hændelser, der kategoriseres som væsentlige i henhold til NIS 2-direktivet. I DORA-forordningens artikel 3, stk. 1, nr. 10, defineres en it- eller cyberhændelse som større, hvis den har en stor negativ indvirkning på net- og informationssystemer, som understøtter kritiske eller vigtige funktioner i den finansielle enhed. I NIS 2-direktivets artikel 23, stk. 3 defineres en hændelse som væsentlig, hvis den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller hvis den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydeligt materiel eller immateriel skade.

Såfremt operatøren af finansiel digitale infrastruktur varetager operationelle opgaver på betalingsområdet for kreditinstitutter, betalingsinstitutter, kontooplysningstjenesteudbydere eller e-pengeinstitutter, vil infrastrukturen i relevant omfang skulle indberette større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser.

Det foreslås i *§ 333 f, stk. 3, 2. pkt.*, at indberetningen skal indeholde alle oplysninger, der er nødvendige for at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Overtrædelse af § 333 f, stk. 3, foreslås strafbelagt i § 373 f, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling kan bestå i, at operatøren ikke indberetter større operationelle eller sikkerhedsmæssige betalingsrelaterede hændelser

Det foreslås i *§ 333 f, stk. 4, nr. 1* og *2*, at en hændelse, jf. stk. 3, anses for væsentlig, hvis 1) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den finansielle digitale infrastruktur, eller 2) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydeligt materiel eller immateriel skade.

Det foreslåede § 333 f, stk. 4, uddyber indholdet af det foreslåede § 333 f, stk. 3, ved at tydeliggøre, hvad der anses som en væsentlig hændelse. Bestemmelsen medfører bl.a., at hændelser, der har indflydelse på operatørens levering af tjenester eller på kritiske eller vigtige funktioner hos de tilsluttede finansielle virksomheder vil skulle indberettes til Finanstilsynet.

Det foreslås i *§ 333 f, stk. 5,* at ved indberetning, jf. stk. 3, skal en operatør af digital finansiel infrastruktur foretage de handlinger, der følger af bestemmelsens nr. 1-5.

Den foreslåede bestemmelse implementerer NIS 2-direktivets artikel 23, stk. 4.

Det foreslås i *§ 333 f, stk. 5, nr. 1,* at ved indberetning, jf. stk. 3, skal operatøren uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at have fået kendskab til den væsentlige hændelse fremsende en tidlig, som skal angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning.

Det foreslås i *§ 333 f, stk. 5, nr. 2,* at ved indberetning, jf. stk. 3, skal operatøren uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse fremsende en hændelsesunderretning, som skal ajourføre de oplysninger, der er omhandlet

under litra a, og en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger.

Det foreslås i *§ 333 f, stk. 5, nr. 3,* at ved indberetning, jf. stk. 3, skal operatøren efter anmodning fra Finanstilsynet eller fra CSIRT'en fremsende en foreløbig rapport om relevante statusopdateringer.

Det foreslås i *§ 333 f, stk. 5, nr. 4, litra 1-d*, at ved indberetning, jf. stk. 3, skal operatøren fremsende en endelig rapport senest en måned efter forelæggelsen af den i nr. 2 omhandlede hændelsesunderretning, der skal omfatte a) en detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning, b) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen, c) anvendte og igangværende afbødende foranstaltninger, og d) oplysninger om eventuelle grænseoverskridende virkninger af hændelsen.

Det foreslås i *§ 333 f, stk. 5, nr. 5,* at ved indberetning, jf. stk. 3, skal operatøren forelægge en statusrapport for Finanstilsynet og CSIRT'en senest en måned efter forelæggelsen af den i litra nr. 2 omhandlede hændelsesunderretning, hvis hændelsen fortsat pågår på dette tidspunkt, og en endelig rapport senest en måned efter operatørens håndtering af hændelsen.

Overtrædelse af § 333 f, stk. 5, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at overholde kravene til hvad hændelsesrapporterne skal indeholde, og hvornår de skal sendes til Finanstilsynet.

Det foreslås i *§ 333 f, stk. 6,* at en operatør af finansiel digital infrastruktur, hvor det er relevant, uden unødigt ophold skal underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt.

Det foreslås i *§ 333 f, stk. 7,* at en operatør af finansiel digital infrastruktur uden unødigt ophold skal underrette modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller modforholdsregler, som disse modtagere kan træffe som reaktion på den pågældende trussel. Operatøren skal også informere de pågældende modtagere om den konkrete væsentlige cybertrussel, hvor dette er relevant.

Forpligtelserne i stk. 6, og stk. 7, vil indebære, at operatøren af finansiel digital infrastrukturforpligtes til at underrette modtagere af deres tjenester om væsentlige hændelser og cybertrusler.

Den foreslåede bestemmelse implementerer NIS 2-direktivets artikel 23, stk. 2.

Overtrædelse af § 333 f, stk. 7, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed.

Ansvarssubjektet for overtrædelse er operatøren af finansielle digitale infrastruktur. Den strafbare handling består i, at en ikke underretter kunder mv. om modforholdsregler i forhold til væsentlige cybertrusler og hvis relevant, om selve truslen.

Det foreslås i *§ 333 f, stk. 8,* at en operatør af finansiel digital infrastruktur kan underrette Finanstilsynet om væsentlige cybertrusler, når den anser truslen for at være relevant for det finansielle system, tjenestebrugere eller kunder.

Med den foreslåede bestemmelse tydeliggøres muligheden for, at operatører af finansiel digital infrastruktur kan videregive oplysninger om væsentlige cybertrusler til Finanstilsynet.

Det er tiltænkt, at bestemmelsen skal tydeligere, at operatører af finansiel digital infrastruktur har samme mulighed for at videregive oplysninger til Finanstilsynet, som også gælder for virksomheder omfattet af DORA-forordningen, jf. artikel 19, stk. 2, i DORA-forordningen.

Til § 333 g

Det foreslås med § 333 g i lov om finansiel virksomhed at fastsætte generelle regler om test af it- og cybersikkerhed for operatører af finansielle digitale infrastrukturer. Reglerne angår overordnet to slags testprogrammer. Den ene type er de almindelige, interne og systematiske test i overensstemmelse med et program herfor. Den anden type er trusselsbaserede penetrationstest (TLPT), som gennemføres af uafhængige parter med særlig ekspertise i cybertrusler, som tester infrastrukturens produktionsmiljø under anvendelse af metoder, der kan sammenlignes med de metoder som ondsindede aktører erfaringsmæssigt anvender. Den foreslåede bestemmelse i § 333 g i lov om finansiel virksomhed supplerer den foreslåede bestemmelse til § 333 a, stk. 3, nr. 6, der implementerer NIS 2-direktivet artikel 21, stk. 2, litra f. Med bestemmelsen søges det endvidere at harmonisere reglerne for operatører af

finansielle digitale infrastrukturer med relevante regler som gælder for virksomheder omfattet af DORA-forordningen kapitel IV

Det foreslås i *§ 333 g, stk. 1,* at en operatør af finansiel digital infrastruktur løbende skal teste effektiviteten af sine foranstaltninger til sikring mod it- og cyberhændelser, der har eller kan have skadelige virkninger på virksomhedens drift.

Bestemmelsen omfatter de test, der normalt er påkrævede i forbindelse med drift af it-infrastrukturer, som f.eks. løbende sårbarhedsscanninger, test i forbindelse med ændringer og løbende test af virkningen af gennemførte sikringsforanstaltninger, herunder test af foranstaltninger til back-up, restore, nødstrøm og skift af datacenter mv.

Overtrædelse af § 333 g, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i at operatøren ikke løbende tester sine foranstaltninger mod it- og cyberhændelser.

Det foreslås i *§ 333 g, stk. 2,* at en operatør af finansiel digital infrastruktur skal have et program for test af digital operationel modstandsdygtighed, som er integreret med operatørens s ramme for it- og cyberrisikostyring og passende i forhold til de identificerede risici.

Programmet skal sikre en systematisk tilgang til test af operatørens it-værktøjer og -systemer, f.eks. regelmæssige sårbarhedsscanninger, gap-analyser, interne penetrationstest, applikationstest, softwarescanninger og evt. scenariebaserede test.

Programmet skal tillige medvirke til at sikre en proaktiv tilgang til at sikre de it-tjenester, som operatøren benytter og udbyder.

Overtrædelse af § 333 g, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have et testprogram, som er en integreret del af rammerne for risikostyring. Den strafbare handling kan også bestå i, at testprogrammet ikke er i overensstemmelse med de identificerede risici.

Det foreslås i *§ 333 g, stk. 3,* at en operatør af finansiel digital infrastruktur kan pålægges at gennemgå trusselsbaserede penetrationstest i

overensstemmelse med de regler, der gælder for virksomheder omfattet af kapitel IV i forordning 2022/2554 om digital operationel modstandsdygtighed i den finansielle sektor og retsakter udstedt i medfør af forordningen. Vurderingen af, i hvilket omfang en operatør af finansiel digital infrastruktur skal gennemføre disse penetrationstests, ud fra 1) virkningsrelaterede faktorer, navnlig i hvilket omfang de tjenester, der leveres, og de aktiviteter, der udføres af den finansielle digitale infrastruktur, indvirker på den finansielle sektor, 2) eventuelle betænkeligheder vedrørende finansiel stabilitet, herunder den finansielle digitale infrastrukturs systemiske karakter, og 3) den finansielle digitale infrastrukturs specifikke it-risikoprofil, grad af it-modenhed eller de teknologiske kendetegn, der er involveret.

Den foreslåede bestemmelse vil indebære, at operatører af finansielle digitale infrastrukturer kan pålægges at gennemgå trusselsbaserede penetrationstest (TLPT) i overensstemmelse med de regler, som følger af DORA-forordningens kapitel IV og retsakter udsted i medfør heraf. Reglerne i DORA-forordningen om TLPT følger af forordningens artikel 26 og 27, og er baseret på rammeværket TIBER-EU, som er implementeret i Danmark af Danmarks Nationalbank med rammeværket TIBER-DK, som er rettet mod virksomheder under Danmarks Nationalbanks overvågning og deres større it-leverandører. I modsætning til TIBER-DK, omfatter DORA-forordningens TLPT-regler dog som udgangspunkt hele den finansielle sektor.

Efter art. 26, stk. 9, i DORA forordningen, kan medlemslande vælge at udpege en fælles offentlig myndighed i den finansielle sektor, til at varetage TLPT relaterede spørgsmål i den finansielle sektor på nationalt plan. Derfor er der også med den i lovforslaget foreslåede bestemmelse til § 344 e i lov om finansiel virksomhed foreslået at bemyndige erhvervsministeren til at udpege en sådan TLPT-myndighed. Det omfatter også varetagelse af TLPT-relaterede anliggender i forhold til operatører af finansielle digitale infrastrukturer.

Det er forventningen, at bemyndigelsen vil blive udnyttet til at fastsætte regler, der udpeger Danmarks Nationalbank som ansvarlig myndighed i henhold til DORA-forordningens artikel 26, stk. 9. Såfremt Danmarks Nationalbank udpeges som ansvarlig myndighed vil de være ansvarlig for TLPT-relaterede anliggender for alle virksomheder, der skal gennemføre TLPT, hvilket også omfatter at udpege de virksomheder, der skal pålægges at gennemføre TLPT, herunder operatører af finansiel digital infrastruktur i overensstemmelse med § 333 g, stk. 3. Der henvises i øvrigt til lovforslagets § 1, nr. 27, og bemærkningerne hertil.

Til § 333 h

Det foreslås i §§ 333 h-j i lov om finansiel virksomhed at fastsætte regler om operatører af finansielle digitale infrastrukturers styring af risici i forbindelse med brug af leverandører og andre tredjeparter.

Bestemmelserne vil erstatte de hidtidige regler om outsourcing på it-området, som har været gældende for bl.a. fælles datacentraler og it-operatører af detailbetalingssystemer. §§ 333 h – 333 j supplerer den foreslåede bestemmelse i 333 a, stk. 3, nr. 4, der implementerer artikel 21, stk. 2, litra d, i NIS 2-direktivet. Reglerne afspejler derudover en række af de krav, der også gælder for virksomheder omfattet af DORA-forordningens kapitel V, afdeling I, og reglerne skal derfor også ses i lyset heraf.

Det foreslås i *§ 333 h, stk. 1,* at en operatør af finansiel digital infrastruktur skal styre sine it- og cyberrisici, der er relateret til brug af it-tjenester fra tredjeparter som en integreret del af sin ramme for it- og cyberrisikostyring.

Med den foreslåede bestemmelse fastsættes den overordnede forpligtelse til styring af tredjepartsrisici og dennes sammenhæng med operatøren af finansiel digital infrastrukturs ramme for it- og cyberrisikostyring.

Overtrædelse af § 333 h, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i, at operatøren ikke at styrer sine tredjepartsrisici eller, at styrer disse risici uden nogen sammenhæng med rammen for operatørens it- og cyberrisikostyring.

Det foreslås i *§ 333 h, stk. 2,* at en operatør af finansiel digital infrastruktur, der har overladt driften af en forretningsfunktion til en leverandør, til enhver tid har det fulde ansvar for at overholde og opfylde alle forpligtelser i henhold til denne lov.

Med den foreslåede bestemmelse fastsættes en generel ansvarsregel for operatører af finansielle digitale infrastrukturer, der er i overensstemmelse med allerede gældende regler og principper for styring af risiko fra leverandører mv., herunder de gældende regler om outsourcing for både datacentraler og it-operatører af detailbetalingssystemer.

Det foreslås i *§ 333 h, stk. 3,* at en operatør af finansiel digital infrastruktur regelmæssigt skal gennemgå de risici, der er forbundet med brugen af it-tredjepartsudbydere.

Den foreslåede bestemmelse vil indebære, at operatører af finansielle digitale infrastrukturer har pligt til at vedligeholde og udvikle styringen af tredjepartsrisici på linje med den generelle it- og cyberrisikostyring.

Der henvises i øvrigt til den foreslåede § 333 i, der fastsætter nærmere krav til risikovurderingen ved indgåelse af kontrakter med it-tredjepartsudbydere.

Overtrædelse af § 333 h, stk. 3, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke regelmæssigt at identificere eller ajourføre risici forbundet med brugen af it-tredjepartsudbydere.

Det foreslås i *§ 333 h, stk. 4,* at en operatør af finansiel digital infrastruktur skal vedtage og regelmæssigt gennemgå en strategi for sine it-tredjepartsrisici. Strategien for it-tredjepartsrisici skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere.

Den foreslåede bestemmelse vil medføre en forpligtelse operatøren af finansiel digital infrastrukturer til at have en strategi for it-tredjepartsrisiko og regelmæssigt revidere denne strategi med henblik på løbende at kunne udvikle videre på denne strategi. Bestemmelsen vil også indebære et krav om, at strategien bl.a. omfatter en politik for tjenester, der understøtter kritiske og vigtige funktioner, og som leveres af tredjepartsudbydere.

Overtrædelse af § 333 h, stk. 4, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have en strategi for it-tredjepartsrisici eller regelmæssigt gennemgå denne. Den strafbare handling kan også bestå i at strategien for it-tredjepartsrisici ikke omfatter en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere.

Det foreslås i *§ 333 h, stk. 5, 1. pkt.,* at en operatør af finansiel digital infrastruktur skal opretholde og ajourføre et register over oplysninger om alle ordninger for brugen af it-tjenester, der leveres af tredjepartsudbydere.

Det foreslås i *§ 333 h, stk. 5, 2. pkt.,* at operatøren skal underrette Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-

tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Vurderingen af hvornår en funktion anses for at være kritiske eller vigtig vil skulle foretages under hensyn til DORA-forordningens artikel 3, nr. 22, hvori definitionen på en kritisk eller vigtig funktion er fastlagt.

Heraf fremgår det, at en funktion er kritisk eller vigtig, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret.

Overtrædelse af § 333 h, stk. 5, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at føre et register over operatørens ordninger for brugen af tredjepartsudbydere. Den strafbare handling kan også bestå i, ikke at underrette Finanstilsynet om planlagte kontraktlige ordninger vedr. it-tjenester, som understøtter kritiske eller vigtige funktioner.

Det foreslås i *§ 333 h, stk. 6, nr. 1-5,* at inden en operatør af finansiel digital infrastruktur indgår en kontraktlig ordning for brugen af it-tjenester, skal operatøren 1) vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, 2) vurdere om de tilsynsmæssige betingelser for udlicitering er opfyldt, 3) identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, 4) foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under udvælgelses- og vurderingsprocessen sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet og 5) identificere og vurdere interessekonflikter, som den kontraktlige ordning kan give anledning til.

Overtrædelse af § 333 h, stk. 6, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at leve op til forpligtelserne for indgåelse af kontrakter med leverandører af it-tjenester fastsat i § 333, h, stk. 6, nr. 1-5.

Det foreslås i *§ 333 h, stk. 7, 1. pkt.,* at når en operatør af finansiel digital infrastruktur indgår it-kontrakter, der relaterer sig til kritiske og vigtige funktioner, skal infrastrukturen sikre, at den har passende adgangs-, inspektions- og revisionsrettigheder over for tredjepartsudbyderen af it-tjenester.

Vurderingen af hvornår en funktion anses for at være kritiske eller vigtig vil skulle foretages under hensyn til DORA-forordningens artikel 3, nr. 22, hvori definitionen på en kritisk eller vigtig funktion er fastlagt.

Heraf fremgår det, at en funktion er kritisk eller vigtig, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret.

Det foreslås i *§ 333 h, stk. 7,* 2. *pkt.,* at operatøren, på grundlag af en risikobaseret tilgang, skal fastsætte hyppigheden af revisioner og inspektioner samt de områder, der skal underkastes revision.

Overtrædelse af § 333 h, stk. 7, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have sikret passende adgangs-, inspektions- og revisionsrettigheder overfor sine tredjepartsudbydere af it-tjenester ved indgåelse af en kontrakt. Den strafbare handling kan også bestå i ikke at skal fastsætte hyppigheden af revisioner og inspektioner samt de områder, der skal underkastes revision.

Det foreslås i *§ 333 h, stk. 8, nr. 1-4,* at en operatør af finansiel digital infrastruktur skal sikre, at de kontraktlige ordninger for brugen af it-tjenester som minimum kan opsiges i enhver af følgende situationer: 1) Tredjepartsudbyderen begår en væsentlig overtrædelse af gældende lovgivning eller kontraktvilkår. 2) Den finansielle digitale infrastruktur identificerer forhold under overvågningen af it-tredjepartsrisici, som kan ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester. 3) Den finansielle digitale infrastruktur dokumenterer svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring. 4) Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle digitale

infrastruktur som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Med den foreslåede bestemmelse fastsættes en række minimumskrav til opsigelsesrettigheder i de kontrakter finansielle digitale infrastrukturer indgår med deres it-leverandører.

Overtrædelse af § 333 h, stk. 8, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at fastsætte opsigelsesrettigheder, der som minimum opfylder kravene i nr. 1-4, når operatøren indgår kontraktlige ordninger for brugen af it-tjenester med it-leverandører. Dette kan f.eks. være såfremt it-leverandøren ikke overholder gældende love eller såfremt den kontraktlige ordning er til hinder for Finanstilsynets tilsyn med infrastrukturen.

Det foreslås i *§ 333 h, stk. 9, nr. 1-5*, at en operatør af finansiel digital infrastruktur skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner. Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, herunder 1) mulige svigt fra tredjepartsudbyderens side, 2) en forringelse af kvaliteten af de leverede it-tjenester, 3) eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester, 4) eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester, eller 5) opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i stk. 8 anførte situationer.

Vurderingen af hvornår en funktion anses for at være kritiske eller vigtig vil skulle foretages under hensyn til DORA-forordningens artikel 3, nr. 22, hvori definitionen på en kritisk eller vigtig funktion er fastlagt.

Heraf fremgår det, at en funktion er kritisk eller vigtig, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret.

Overtrædelse af § 333 h, stk. 9, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke

at have en exitstrategi for leverede it-tjenester, der understøtter kritiske eller vigtige funktioner, eller ikke at have en exitstrategi, der tager højde for de risici, som kan opstå hos tredjepartsudbydere af it-tjenester, og som er oplistet i nr. 1-5.

Det foreslås i *§ 333 h, stk. 10, nr. 1-3*, at en operatør af finansiel digital infrastruktur skal sikre, at den kan opsige kontraktlige ordninger, uden 1) at dens forretningsaktiviteter afbrydes, 2) at efterlevelsen af de lovgivningsmæssige krav begrænses, og 3) at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade.

Det foreslåede skal ses i sammenhæng med det foreslåede stk. 8 og 9.

Overtrædelse af § 333 h, stk. 10, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansielle digitale infrastruktur. Den strafbare handling består i ikke at sikre, at operatøren kan opsige en kontrakt uden at afbryde forretningsaktivitet, uden efterlevelsen af lovgivningsmæssige krav begrænses og uden tab af kvalitet eller kontinuitet i de leverede tjenester til kunderne.

Det foreslås i *§ 333 h, stk. 11*, at exitstrategierne skal være dokumenterede, proportionale, testet i tilstrækkeligt omfang og gennemgået regelmæssigt.

Overtrædelse af § 333 h, stk. 11, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at havedokumenterede, proportionale, testede og ajourførte exitplaner.

Det foreslås i *§ 333 h, stk. 12*, at en operatør af finansiel digital infrastruktur skal identificere alternative løsninger og udarbejde overgangsplaner, så den kan fratage tredjepartsudbyderen af it-tjenester de relevante it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller indarbejde dem internt.

Den foreslåede bestemmelse skal ses i sammenhæng med det foreslåede stk. 10, og være med til at sikre, at en operatør kan afbryde samarbejdet en tredjepartsudbyder uden at dette skader operatøren eller de ydelser, som operatøren leverer. Bestemmelsen medfører konkret krav om at operatøren skal identificere alternativer til leverandører og udarbejde overgangsplaner, så de kan overføre tjenester fra en leverandør til en anden leverandør, eller hjemtage den pågældende tjeneste.

Overtrædelse af § 333 h, stk. 12, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består f.eks. i ikke at have identificeret alternativer til leverandører. Den strafbare handling kan også bestå i ikke at have udformet overgangsplaner, så tjenester kan overføres mellem en ny og gammel leverandør, eller så tjenester kan hjemtages.

Det foreslås i *§ 333 h, stk. 13*, at en operatør af finansiel digital infrastruktur skal indføre passende beredskabsforanstaltninger for at opretholde driftsstabiliteten i tilfælde af, at de i stk. 9, nr. 1-5, omhandlede omstændigheder indtræder.

Overtrædelse af § 333 h, stk. 13, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have passende beredskabsplaner for opretholdelse af driften.

Til § 333 i

Det foreslås i § 333 i, at uddybe forpligtelsen i § 333 h, stk. 6, nr. 3, om due diligence mv, med særskilte krav til vurdering af potentiel koncentrationsrisiko i forhold til den enkelte operatør af finansiel digital infrastruktur. Med bestemmelsen søges det at harmonisere reglerne for operatører af finansielle digitale infrastrukturer med de regler som gælder for virksomheder omfattet af DORA-forordningens artikel 29 om foreløbige vurderinger af it-koncentrationsrisici på enhedsniveau.

Det foreslås i *§ 333 i, nr. 1*, at når en operatør af finansiel digital infrastruktur foretager identifikation og vurdering af de risici, der er omhandlet i § 333 h, stk. 6, nr. 3, skal den finansielle digitale infrastruktur tage hensyn til, hvorvidt den påtænkte indgåelse af en kontraktlig ordning, der understøtter kritiske eller vigtige funktioner for de tilsluttede virksomheder, vil føre til henlæggelse af funktioner til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte.

Den foreslåede bestemmelse vil indebære, at operatøren forud for indgåelsen af en kontraktlig ordning, der understøtter kritiske eller vigtige funktioner for de virksomheder, der er tilsluttet operatøren, herunder f.eks. pengeinstitutter, skal vurdere og tage hensyn til, om udliciteringen eller

henlæggelsen af de pågældende funktioner til tredjepartsudbyderen fremadrettet vil blive vanskelig at erstatte.

Vurderingen skal være med til at sikre, at operatøren identificerer og bliver bevidste om, hvorvidt der skabes en afhængighed af tredjepartsudbyderen, der kan skade de virksomheder på det finansielle område, som operatøren leverer sine ydelser til. Vurderingen kan bl.a. tage udgangspunkt i, om det uden større vanskeligheder vil muligt for operatøren at tilbagetage og drifte den henlagte funktion, eller om det uden større vanskeligheder vil være muligt at finde en anden tredjepartsudbyder, som kan overtage og drifte den henlagte funktion.

Vil en henlæggelse af funktioner til en tredjepartsudbyder indebære at henlæggelsen bliver vanskelig at erstatte, så skal operatøren afveje fordele og omkostninger ved alternative løsninger under hensyntagen til, om sådanne løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i operatørens strategi for digital modstandsdygtighed.

Det foreslås i *§ 333 i, nr. 2,* at når en operatør af finansiel digital infrastruktur foretager identifikation og vurdering af de risici, der er omhandlet i § 333 h, stk. 6, nr. 3, skal den finansielle digitale infrastruktur tage hensyn til, hvorvidt den påtænkte indgåelse af en kontraktlig ordning, der understøtter kritiske eller vigtige funktioner for de tilsluttede virksomheder, vil føre til indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne.

Den foreslåede bestemmelse vil indebære, at operatøren forud for indgåelsen af en kontraktlig ordning, der understøtter kritiske eller vigtige funktioner for de virksomheder, der er tilsluttet operatøren, herunder f.eks. pengeinstitutter, skal vurdere og tage hensyn til om udliciteringen eller henlæggelsen af de pågældende funktioner til tredjepartsudbyderen fremadrettet vil medføre en koncentrationsrisiko.

Vurderingen skal være med til at sikre, at operatøren identificerer og bliver bevidste om, hvorvidt der skabes en koncentrationsrisiko hos tredjepartsudbyderen, der kan skade de virksomheder på det finansielle område, som operatøren leverer sine ydelser til. Vurderingen bør derfor tage udgangspunkt i, om indgåelsen af den kontraktlige ordning vil indebære, at flere funktioner, der understøtter kritiske eller vigtige funktioner for de virksomheder, der er tilsluttet operatøren, samles hos den samme tredjepartsudbyder, og om dette indebærer en risiko for de tilsluttede virksomheder.

Vil henlæggelse af funktioner til en tredjepartsudbyder indebære en koncentrationsrisiko, så skal operatøren afveje fordele og omkostninger ved alternative løsninger, såsom brug af forskellige tredjepartsudbydere, under hensyntagen til, om sådanne løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i operatørens strategi for digital modstandsdygtighed.

Overtrædelse af § 333 i, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i, at en operatør ikke forud for indgåelsen af en kontraktlig ordning med en tredjepartsudbyder af it-tjenester vurderer og tager hensyn til, om de funktioner, der henlægges til tredjepartsudbyderen, er let at erstatte, når funktionerne er kritiske eller vigtige for de virksomheder, som er tilsluttet operatøren. Den strafbare handling kan også bestå i, at en operatør ikke forud for indgåelsen af en kontraktlig ordning med en tredjepartsudbyder af it-tjenester vurderer og tager hensyn til, om der skabes en koncentrationsrisiko ved at henlægge funktionerne til tredjepartsudbyderen, når funktionerne er kritiske eller vigtige for de virksomheder, som er tilsluttet operatøren.

Til § 333 j

Det foreslås i § 333 j i lov om finansiel virksomhed, at fastsætte regler om indholdet af kontrakter, som indgås mellem finansielle digitale infrastrukturer og tredjepartsudbydere af it-tjenester. Med bestemmelsen søges det, at harmonisere reglerne for operatører af finansielle digitale infrastrukturer med de regler som gælder for virksomheder omfattet af DORA-forordningens artikel 30 om krav til kontrakter med it-leverandører.

Det foreslås i *§ 333 j, stk. 1*, at rettigheder og forpligtelser for en operatør af finansiel digital infrastruktur og for tredjepartsudbyderen af it-tjenester skal fordeles klart og fastlægges skriftligt. Den samlede kontrakt skal omfatte serviceniveauaftaler og dokumenteres i et samlet dokument, som parterne skal have adgang til i et varigt og tilgængeligt format.

Det foreslåede krav om at parterne skal have adgang til dokumentet i et varigt og tilgængeligt format vil f.eks. være opfyldt med et papirdokument eller med et digitalt dokument af en art, som ikke kræver særlig systemunderstøttelse for at kunne læses.

Overtrædelse af § 333 j, stk. 1, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af §

372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at have en skriftlig kontrakt i varig og tilgængelig form.

Det foreslås i *§ 333 j, stk. 2,* at de kontraktlige ordninger for brugen af it-tjenester mindst skal omfatte de elementer, der fremgår af bestemmelsens stk. 2, nr. 1-8.

Med bestemmelsen foreslås det at specificere de minimumskrav, som stilles til alle kontrakter for brugen af it-tjenester, uanset om de vedrører kritiske eller vigtige funktioner eller ikke.

Det foreslås i *§ 333 j, stk. 2, nr. 1,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen skal levere, med angivelse af om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf, er tilladt, og hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise.

Det foreslås i *§ 333 j, stk. 2, nr. 2,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte en angivelse af de steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og krav om, at tredjepartsudbyderen på forhånd skal underrette operatøren, hvis den har planer om at ændre disse steder.

Det bemærkes, at angivelsen af steder, herunder regioner og lande, hvor tjenesterne skal leveres og data skal behandles samt lagres, skal forstås ud fra anvendelsen af begrebet databehandling i EU-retten, herunder på området for databeskyttelse.

Det foreslås i *§ 333 j, stk. 2, nr. 3,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger.

Det foreslås i *§ 333 j, stk. 2, nr. 4,* at de kontraktretlige ordninger for brugen af it-tjenester skal mindst omfatte bestemmelser om sikring af adgang, genopretning og tilbagelevering af data i et tilgængeligt format i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen varetager, eller i tilfælde af opsigelse af kontrakten.

Det bemærkes, at tilbageleveringen af data i et let tilgængeligt format skal ses i sammenhæng med både databeskyttelse og dataportabilitet, hvilket indebærer at et let tilgængeligt format i denne sammenhæng både kan forstås som læsbart for personer og i et format, der kan overføres til andre typer systemer, hvori de pågældende data skal kunne behandles.

Det foreslås i *§ 333 j, stk. 2, nr. 5,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf.

Det foreslås i *§ 333 j, stk. 2, nr. 6,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte en forpligtelse for tredjepartsudbyderen til at yde bistand til operatøren uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en it-hændelse, der vedrører den it-tjeneste, som leveres tiloperatøren.

Det foreslås i *§ 333 j, stk. 2, nr. 7,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte en forpligtelse for tredjepartsudbyderen til at samarbejde fuldt ud med Finanstilsynet og afviklingsmyndigheder, herunder personer, som myndighederne har udpeget.

Det foreslås i *§ 333 j, stk. 2, nr. 8,* at de kontraktretlige ordninger for brugen af it-tjenester mindst skal omfatte opsigelsesrettigheder og dertil knyttede minimumsfrister for opsigelse af de kontraktlige ordninger.

Overtrædelse af § 333 j, stk. 2, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i ikke at overholde minimumskravene fastsat i § 333 j, stk. 2.

Det foreslås i *§ 333 j, stk. 3,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte en række yderligere elementer, der følger af § 333 j, stk. 3, nr. 1-6.

Med den foreslåede bestemmelse fastsættes yderligere minimumskrav, som stilles til kontrakter for brugen af it-tjenester, der vedrører kritiske eller vigtige funktioner ud over de krav, som følger af stk. 2. Kontrakter for brugen af it-tjenester, der vedrører kritiske eller vigtige funktioner, skal således indeholde alle elementer, som er opregnet i stk. 2, nr. 1-10, og alle elementer, som er opregnet i stk. 3, nr. 1-6.

De yderligere elementer tager generelt sigte på at imødekomme det forøgede behov, som den finansielle digitale infrastruktur har i forhold til at styre de særlige eller forøgede risici, der følger af, at driften af it-tjenester, der understøtter kritiske eller vigtige funktioner, varetages af en anden virksomhed, som kan være etableret i en anden jurisdiktion, herunder fra jurisdiktioner i tredjelande.

Vurderingen af hvornår en funktion anses for at være kritiske eller vigtig vil skulle foretages under hensyn til DORA-forordningens artikel 3, nr. 22, hvori definitionen på en kritisk eller vigtig funktion er fastlagt.

Heraf fremgår det, at en funktion er kritisk eller vigtig, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret.

Det foreslås i *§ 333 j, stk. 3, nr. 1,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, så operatøren kan foretage en effektiv overvågning af it-tjenester, og den uden unødigt ophold kan træffe passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes.

Det foreslås i *§ 333 j, stk. 3, nr. 2,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle digitale infrastruktur, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer

Det foreslås i *§ 333 j, stk. 3, nr. 3,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte krav til tredjepartsudbyderen om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et

passende niveau af sikkerhed for, at den finansielle digitale infrastruktur kan levere sine tjenester.

Det foreslås i *§ 333 j, stk. 3, nr. 4,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte en forpligtelse for tredjepartsudbyderen til at deltage i og fuldt ud samarbejde om operatørens trusselsbaserede penetrationstest som omhandlet i § 333 g, stk. 3.

Det bemærkes, at tredjepartsudbydere som varetager it-drift af kritiske eller vigtige forretningsfunktioner, skal kunne pålægges at deltage i – og blive genstand for trusselsbaserede penetrationstest i forhold til deres drift af it-tjenester for operatører og operatørernes tilsluttede finansielle virksomheder.

Det foreslås i *§ 333 j, stk. 3, nr. 5,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte en ret til løbende at overvåge tredjepartsudbyderens opgavevaretagelse og risikostyring, herunder adgangs- og inspektions- og revisionsrettigheder for operatøren, Finanstilsynet eller udpegede tredjeparter og adgang til nødvendig information og dokumentation.
Det foreslås i *§ 333 j, stk. 3, nr. 6, litra a* og *b,* at de kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, ud over de elementer, der er oplistet i stk. 2, mindst skal omfatte exitstrategier, herunder indførelse af en obligatorisk passende overgangsperiode a) i løbet af hvilken tredjepartsudbyderen fortsat leverer de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i operatøren eller sikre en effektiv afvikling eller omstrukturering heraf, og b) som giver operatøren mulighed for at migrere til en anden tredjepartsudbyder, eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Overtrædelse af § 333 j, stk. 3, foreslås strafbelagt i § 373, stk. 2, 1. pkt., i lov om finansiel virksomhed med den i lovforslaget foreslåede ændring af § 372, stk. 2, i lov om finansiel virksomhed. Ansvarssubjektet er operatøren af finansiel digital infrastruktur. Den strafbare handling består i at indgå kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, uden at de kontraktlige ordninger omfatter exitstrategier, herunder med en overgangsperiode, der opfylder kravene i litra a og b.

Til § 333 k

Det foreslås i *§ 333 k, stk. 1,* at en operatør af finansiel digital infrastruktur kan udveksle oplysninger og efterretninger om cybertrusler i overensstemmelse med reglerne i kapitel VI, i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022, og indgå i ordninger oprettet i henhold forordningens artikel 45, stk. 2. En operatør af finansiel digital infrastruktur kan ligeledes udveksle relevante cybersikkerhedsoplysninger i overensstemmelse med reglerne i kapitel VI, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022, og indgå i ordninger oprettet i overensstemmelse hermed.

Den foreslåede bestemmelse angår muligheden for at en operatør af finansiel digital infrastruktur kan deltage i de frivillige ordninger for informationsudveksling, som er oprettet af finansielle virksomheder i henhold til DORA-forordningens artikel 45, stk. 2.

Ordningerne har til formål at muliggøre informationsudveksling i pålidelige miljøer, for at hjælpe den finansielle sektor til at forebygge og i fællesskab sætte ind over for cybertrusler ved hurtigt at begrænse spredningen af it- og cyberrisici.

Praktisk deltagelse af operatøren vil desuden forudsætte, at den relevante ordnings bestemmelser om inddragelse af it-tredjepartsudbydere indeholder denne mulighed.

Den foreslåede bestemmelse vil også medføre, at operatører af finansielle digitale infrastrukturer kan udveksle cybersikkerhedsoplysninger i overensstemmelse med NIS 2-direktivets artikel 29 og deltage i ordninger for informationsudveksling oprettet i henhold hertil.

Det foreslås i *§ 333 k, stk. 2,* at en finansiel digital infrastruktur skal underrette Finanstilsynet om sin deltagelse i de i stk. 1, omhandlede ordninger og i tilfælde af udtrædelse af sådanne ordninger.

Det foreslåede fastsætter en pligt for operatøren af finansiel digital infrastruktur til at underrette Finanstilsynet om sin deltagelse eller udtrædelse i en ordning i henhold til DORA-forordningens kapitel IV eller en ordning i henhold til NIS 2-direktivets artikel 29.

Til § 333 l

I henhold til NIS 2-direktivets artikel 27, stk. 1, opretter og fører ENISA et register over en række kategorier af enheder, som er væsentlige i henhold til direktivets artikel 3, jf. bilag I.

Med henblik på oprettelse og ajourføring af dette register skal alle virksomheder omfattet af NIS 2-direktivet afgive de nødvendige informationer til de kompetente myndigheder, indenfor nærmere bestemte frister, i henhold til NIS 2-direktivets artikel 27, stk. 2, og stk. 3.

Det foreslås i *§ 333 l, stk. 1, nr. 1-3,* at en operatør af finansiel digital infrastruktur skal oplyse Finanstilsynet følgende: 1) Operatørens navn. 2) Adressen på operatørens hovedforretningssted og dens andre retlige forretningssteder i Den Europæiske Union. 3) Den relevante sektor og delsektor og typen af enhed, som nævnt i bilag I, i direktiv (EU) 2022/2555 af 14. december 2022. 4) Ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre på operatøren. 5) De medlemsstater, hvor operatøren leverer tjenester.
Det foreslåede fastsætter de oplysningerne der skal afgives efter udpegning.

Det foreslås i *§ 333 l, stk. 2,* at ved ændring af oplysningerne i stk. 1 skal operatøren af finansiel digital infrastruktur straks og senest tre måneder efter datoen for ændringen underrette Finanstilsynet herom.

Til § 333 m

Det foreslås i *§ 333 m,* at kapitel 21 om tilsyn og kapitel 23 om delegation og klager, i lov om finansiel virksomhed og regler udstedt i medfør af disse kapitler skal finde tilsvarende anvendelse for operatører af finansielle digitale infrastrukturer med de nødvendige tilpasninger.

Den foreslåede bestemmelse vil indebære, at Finanstilsynets eksisterende tilsynsramme, der følger af kapitel 21 og 23 i lov om finansiel virksomhed, vil finde tilsvarende anvendelse for operatører af finansielle digitale infrastrukturer.

Kapitel 21 i lov om finansiel virksomhed indeholder regler om tilsyn, herunder bl.a. en række konkrete tilsynsbeføjelser, regler om tavshedspligt, offentliggørelse af afgørelser og partsstatus.

Det vil bl.a. betyde, at Finanstilsynet ved sin tilsynskompetence i medfør af § 344, stk. 1, i lov om finansiel virksomhed får beføjelser til at føre tilsyn med operatører af finansielle digitale infrastrukturer og deres overholdelse af reglerne i nærværende lovforslag. Bestemmelsen indebærer bl.a. også, at tilsynet med operatører af finansielle digitale infrastrukturer indgår i Finanstilsynets tilrettelæggelse af sin tilsynsvirksomhed i henhold til § 344, stk. 2 og 3, i lov om finansiel virksomhed, og at Finanstilsynets bestyrelse indgår i tilsynet med den kompetence, som bestyrelsen er tillagt i medfør af § 345 i lov om finansiel virksomhed.

Bestemmelsen indebærer også, at tilsynsbeføjelsen til at udstede påbud og påtaler for overtrædelse af lov om finansiel virksomhed og regler udstedt i medfør heraf, der følger af kompetencen i § 344, stk. 1, i lov om finansiel virksomhed også vil gælde i forhold til operatører af finansielle digitale infrastrukturer. Ligeledes vil Finanstilsynets beføjelser til at indhente oplysninger og foretage kontroller, som bl.a. følger af § 347 i lov om finansiel virksomhed finde tilsvarende anvendelse.

Med disse tilsynsbeføjelser implementeres således også de krav til den kompetente myndigheds tilsyns- og håndhævelsesbeføjelser, der følger af NIS 2-direktivets artikel 32, stk. 2, litra a og e-g, og stk. 4, litra b-f, h og i.

Bestemmelsen indebærer herudover også, at den tavshedspligt, som Finanstilsynet er pålagt i medfør af § 354 i lov om finansiel virksomhed tilsvarende finder anvendelse for fortrolige oplysninger vedrørende operatører af finansielle digitale infrastrukturer. Ligesom reglerne om offentliggørelse af Finanstilsynets afgørelser vil finde tilsvarende anvendelse på afgørelser truffet over for operatører af finansielle digitale infrastrukturer.

Kapitel 23 i lov om finansiel virksomhed indeholder bestemmelser om klageadgang og delegation.

Bestemmelsen vil derfor også indebære, at Erhvervsankenævnet bliver klageinstans for afgørelser truffet af Finanstilsynet overfor operatører af finansielle digitale infrastrukturer.

Til § 333 n

I NIS 2-direktivets artikel 32, stk. 2 og 4, fastsættes en række tilsyns- og håndhævelsesbeføjelser for overtrædelse af forpligtelser fastsat i medfør af direktivet. En del af de beføjelser, der er fastsat i den nævnte artikel foreslås gennemført ved forslaget om, at kapitel 21 i lov om finansiel virksomhed skal finde tilsvarende anvendelse for finansielle digitale infrastrukturer, jf. den foreslåede § 333 m i lov om finansiel virksomhed. Det omfatter nærmere beføjelserne i henhold til NIS 2-direktivets artikel 32, stk. 2, litra a og e-g, og stk. 4, litra b-f, h og i., er i overensstemmelse med de beføjelser, der følger af kapitel 21 i lov om finansiel virksomhed. Nogle af tilsyns- og håndhævelsesbeføjelserne i NIS 2-direktivets artikel 32, stk. 2 og 4, følger dog ikke af tilsynsbeføjelserne i kapitel 21 i lov om finansiel virksomhed, hvorfor det foreslås at fastsætte disse i en særskilt bestemmelse herom.

Det foreslås i *§ 333 n, stk. 1, nr. 1,* at Finanstilsynet kan pålægge en operatør af finansiel digital infrastruktur regelmæssige og målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed og at afholde udgifterne hertil.

Den foreslåede bestemmelse implementerer artikel 32, stk. 2, litra b, i NIS 2-direktivet. Den foreslåede ændring har som konsekvens, at operatører af finansielle digitale infrastrukturer fremover vil kunne pålægges uafhængige sikkerhedsaudits og at afholde udgifterne hertil. En sådan foranstaltning vil kunne benyttes i situationer, hvor det almindelige løbende tilsyn ikke skønnes at være tilstrækkeligt.

Det foreslås i *§ 333 n, stk. 1, nr. 2,* at Finanstilsynet kan pålægge en operatør af finansiel digital infrastruktur ad hoc-audits, herunder hvor det er berettiget på grund af en væsentlig hændelse eller en overtrædelse af loven.

Den foreslåede bestemmelse implementerer artikel 32, stk. 2, litra c, i NIS 2-direktivet.

Foranstaltningerne i litra c svarer til de beføjelser, der også hidtil har været i lovgivningen med den forskel, at der ikke har været praksis for eksterne ad-hoc audits på det digitale operationelle område. Der er allerede hjemmel til at foretage almindelige inspektioner og pålægge sagkyndige undersøgelser efter kapitel 21 i lov om finansiel virksomhed, men den foreslåede ændring har som konsekvens, at der skal ligge en væsentlig hændelse til grund for en afgørelse om pålæg af en ad hoc-audit. En sådan foranstaltning vil f.eks. kunne benyttes i situationer, hvor en væsentlig hændelse indikerer alvorlige mangler i operatørens styring af sine it- eller cyberrisici, og det almindelige løbende tilsyn ikke skønnes at være tilstrækkeligt. Sikkerhedsaudits, der gennemføres efter den foreslåede bestemmelse, skal være baseret på risikovurderinger, som er foretaget af Finanstilsynet, den finansielle digitale infrastruktur eller på anden tilgængelig risikoinformation, jf. NIS 2-direktivets artikel 32, stk. 2.

Det foreslås i *§ 333 n, stk. 1, nr. 3,* at Finanstilsynet kan pålægge en operatør af finansiel digital infrastrukturer sikkerhedsscanninger baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte finansielle digitale infrastruktur.

Beføjelsen implementerer NIS 2-direktivets artikel 32, stk. 2, litra d, og er ny.

Det foreslås i *§ 333 n, stk. 1, nr. 4,* at Finanstilsynet kan udstede advarsler om en operatør af finansiel digital infrastrukturs overtrædelse af loven.

Advarsler er en ny håndhævelsesbeføjelse, der ikke følger af de nuværende regler på det operationelle område. Advarsler kan udstedes ved overtrædelser uafhængig af en evt. forudgående inspektion.

Den foreslåede bestemmelse implementerer NIS 2-direktivets artikel 32, stk. 4, litra a.

Det foreslås i *§ 333 n, stk. 1, nr. 5,* at Finanstilsynet kan udpege en person med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med den pågældende operatør af finansiel digital infrastrukturs overholdelse af §§ 333 a og 333 f.

Det fremgår af den foreslåede bestemmelse, at den person, der udpeges til at føre tilsyn, alene vil skulle føre tilsyn med operatørens overholdelse af regler fastsat i medfør af §§ 333 a og 333 f. Afgrænsningen skyldes, at artikel 32, stk. 4, litra g, i NIS 2-direktivet tilsvarende afgrænser den udpegede persons tilsyn til at omfatte overholdelse af direktivets artikel 21 og 23, der ved dette lovforslag implementeres i de foreslåede §§ 333 a og 333 f i lov om finansiel virksomhed.

Forslaget implementerer NIS 2-direktivets artikel 32, stk. 4, litra g.

Til § 333 o

Det kræver ikke i dag særskilt tilladelse fra Finanstilsynet eller andre myndigheder, at drive virksomhed som fælles datacentral. Derfor er det heller ikke ved nærværende lovforslag foreslået, at de virksomheder, der udpeges som operatør af finansiel digital infrastruktur skal underlægges et særskilt tilladelseskrav hertil, men alene at disse virksomheder kan udpeges jf. den foreslåede § 333 i lov om finansiel virksomhed.

Ligeledes kræver det i dag heller ikke godkendelse fra Finanstilsynet at besidde stillinger i ledelsen hos fælles datacentraler, og sådanne ledelsesmedlemmer er heller ikke omfattet af f.eks. krav til egnet og hæderlighed. Derfor er der heller ikke ved nærværende lovforslag foreslået særskilte krav herom for ledelsesmedlemmer i de virksomheder, der udpeges som operatører af finansielle digitale infrastrukturer.

De gældende regler for fælles datacentraler indebærer således heller ikke mulighed for, at Finanstilsynet kan suspendere en tilladelse eller påbyde en fælles datacentral at afsætte et ledelsesmedlem.

Straffelovens § 79 indeholder regler om rettighedsfrakendelse ved dom for strafbare forhold, og bestemmelsen udgør den almindelige regel i dansk ret om rettighedsfrakendelse.

Efter straffelovens § 79, stk. 1, kan den, som udøver en af den i straffelovens § 78, stk. 2, omhandlede virksomheder ved dom for strafbart forhold frakendes retten til fortsat at udøve den pågældende virksomhed eller til at udøve den under visse former, såfremt det udviste forhold begrunder en nærliggende fare for misbrug af stillingen. Det samme gælder, når særlige omstændigheder taler derfor, om udøvelsen af anden virksomhed, jf. straffelovens § 79, stk. 2. Efter samme regel kan der ske frakendelse af retten til at deltage i ledelsen af en erhvervsvirksomhed her i landet eller i udlandet uden at hæfte personligt og ubegrænset for virksomhedens forpligtelser. Frakendelsen sker på tid fra 1 til 5 år regnet fra endelig dom, eller indtil videre.

Med NIS 2-direktivet følger imidlertid krav om, at den relevante tilsynsmyndighed har to særlige håndhævelsesbeføjelser, jf. direktivets artikel 32, stk. 5. Den ene beføjelse angår tilsynsmyndighedens mulighed for midlertidigt at suspendere en myndighedsudstedt certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, enheden leverer, eller aktiviteter, der udføres af enheden. Den anden angår tilsynsmyndighedens mulighed for midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller juridisk repræsentant i enheden at udøve ledelsesfunktioner i denne.

Det foreslås derfor i *§ 333 o, stk. 1, nr. 1* og *2*, at efterkommer en operatør af finansiel digital infrastruktur ikke Finanstilsynets påbud i medfør af denne lov, og efterkommer operatøren ikke påbuddet inden en fornyet frist, som Finanstilsynet efterfølgende sætter, kan Finanstilsynet træffe afgørelse om: 1) Midlertidigt at suspendere en myndighedsudstedt certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, operatøren leverer, eller aktiviteter, der udføres af operatøren. 2) Midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller juridisk repræsentant i operatøren at udøve ledelsesfunktioner i denne.

Bestemmelsen vil implementere artikel 32, stk. 5, 1. afsnit, i NIS 2-direktivet. Det følger af bestemmelsen i direktivets artikel 32, stk. 5, 1. afsnit, at medlemsstaterne skal sikre, at de kompetente myndigheder i en situation, hvor håndhævelsesforanstaltninger anvendt i medfør af direktivets

artikel 32, stk. 4, litra a-d og f, er virkningsløse, skal have beføjelse til at fastsætte en frist inden for hvilken den væsentlige enhed skal tage de nødvendige tiltag for at afhjælpe manglerne eller opfylde myndighedernes krav. Hvis de ønskede tiltag ikke tages inden for den fastsatte frist, skal de kompetente myndigheder have beføjelse til: a) midlertidigt at suspendere, eller anmode et certificerings- eller godkendelsesorgan eller en domstol om i overensstemmelse med national ret midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres, af en væsentlig enhed, og b) at anmode de relevante organer eller domstole om i overensstemmelse med national ret midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller som juridisk repræsentant i den pågældende væsentlige enhed at udøve ledelsesfunktioner i den pågældende enhed.

Det bemærkes, at de eksisterende muligheder for rettighedsfrakendelse i straffeloven ikke vurderes tilstrækkelige til at sikre korrekt og tilstrækkelig implementering af bestemmelsen i direktivet.

Erhvervsministeriet har ikke foretaget en meget tekstnær direktivimplementering, da bestemmelsen er søgt tilpasset den øvrige tilsynsramme, der foreslås for operatører af digitale finansielle infrastrukturer i lov om finansiel virksomhed. Den foreslåede bestemmelse skal dog forstås og anvendes i overensstemmelse med direktivets forudsætninger og eventuelle fortolkningsbidrag fra Kommissionen, ENISA eller andre af EU's institutioner.

Det bemærkes i den forbindelse, at det af den danske oversættelse af NIS 2-direktivets artikel 32, stk. 5, 1. afsnit, fremgår, at bestemmelsen kan anvendes, hvor de relevante håndhævelsesforanstaltninger er »virkningsløse«. Denne oversættelse vurderes imidlertid ikke at være forenelig med den engelske udgave af direktivet, hvori »ineffective« er anvendt. Det er således Erhvervsministeriets vurdering, at formuleringen »virkningsløse« vil udgøre en indholdsmæssig forskydning i forhold til den engelske sprogversion. Det er desuden Erhvervsministeriets vurdering, at et kriterium om, at foranstaltningerne er »virkningsløse«, vil indebære, at enhver virkning af de anvendte foranstaltninger – uanset om virkningen måtte være utilstrækkelig eller endda negativ – vil betyde, at bestemmelsen ikke vil kunne anvendes. Det vurderes, at dette reelt vil gøre bestemmelsen uanvendelig i praksis i strid med direktivets forudsætninger. Det er derfor Erhvervsministeriets opfattelse af formuleringen »virkningsløse«, skal forstås som »utilstrækkelige«.

Den foreslåede bestemmelse skal på baggrund heraf forstås således, at det vil være en forudsætning for anvendelse af bestemmelsen, at Finanstilsynets påbud eller øvrige tilsynsskridt har vist sig utilstrækkelige. Det er dermed også en forudsætning, at mindre indgribende midler har været forsøgt, og at dette har vist sig utilstrækkelige til at sikre, at operatøren foretager de nødvendige tiltag for at afhjælpe mangler, som den kompetente myndighed har konstateret, eller opfylder den kompetente myndigheds krav.

Bestemmelsen vil skulle anvendes i overensstemmelse med direktivets forudsætninger som udtrykt i præambelbetragtning nr. 133, hvorefter bestemmelsen kun bør anvendes som en sidste udvej, dvs. først efter at de øvrige, relevante håndhævelsesforanstaltninger er udtømt. Det fremgår videre af samme præambelbetragtning, at i betragtning af deres alvor og indvirkning på enhedernes aktiviteter og i sidste ende brugerne, bør sådanne midlertidige suspensioner eller forbud kun anvendes proportionalt med overtrædelsens alvor og under hensyntagen til omstændighederne i hvert enkelt tilfælde, herunder i lyset af, om overtrædelsen var forsætlig eller uagtsom, og ethvert tiltag, der er iværksat for at forebygge eller afbøde den materielle eller immaterielle skade.

Der vil efter den foreslåede bestemmelse skulle fastsættes en nærmere angivet frist, inden for Finanstilsynets påbud skal være efterlevet, og manglerne derved være afhjulpet eller kravene være opfyldt. Varigheden af fristen vil afhænge af en konkret vurdering, som foretages af Finanstilsynet.

Den foreslåede bestemmelse i stk. 1, *nr. 1*, indebærer, at såfremt operatøren ikke har afhjulpet manglerne eller efterkommet de krav som Finanstilsynet har påbudt inden for den fastsatte frist, kan Finanstilsynet træffe afgørelse om midlertidigt at suspendere en myndighedsudstedt certificering eller godkendelse vedrørende dele af eller alle de tjenester, operatøren leverer, eller aktiviteter, der udføres af operatøren.

En afgørelse efter nr. 1 vil være af midlertidig karakter. Der henvises i øvrigt til det foreslåede stk. 2, hvorefter afgørelsen kun kan opretholdes, så længe operatøren ikke har afhjulpet manglerne eller efterlever Finanstilsynets påbud.

Efter den foreslåede bestemmelse vil det alene være myndighedsudstedte godkendelser eller certificeringer, der kan suspenderes. Det vurderes således ikke at have været hensigten med bestemmelsen i direktivet, at godkendelser eller certificeringer, der er udstedt af private virksomheder, eksempelvis en ISO 27001-certificering, skal kunne suspenderes.

Den foreslåede bestemmelse giver ikke i sig selv hjemmel til at suspendere en myndighedsudstedt certificering. Det vil således forudsætte, at der er skabt hjemmel til at suspendere certificeringen i den relevante regulering.

Den foreslåede bestemmelse i stk. 1, *nr. 2,* indebærer, at såfremt operatøren ikke har afhjulpet manglerne eller efterkommet de krav, som Finanstilsynet har påbudt, inden for den fastsatte frist, kan Finanstilsynet træffe afgørelse om midlertidigt at forbyde enhver fysisk person med ledelsesansvar på direktionsniveau eller juridisk repræsentant i operatøren at udøve ledelsesfunktioner i den pågældende operatør.

En afgørelse efter nr. 2 vil være af midlertidig karakter. Der henvises i øvrigt til det foreslåede stk. 2, hvorefter afgørelsen kun kan opretholdes, så længe operatøren ikke har afhjulpet manglerne eller efterlever myndighedens krav.

Det følger af NIS 2-direktivets artikel 32, stk. 7, at den kompetente myndighed ved anvendelsen af håndhævelsesforanstaltninger såsom suspension eller forbud efter den foreslåede bestemmelse, skal tage hensyn til en række nærmere angivne forhold.

NIS 2-direktivet foreskriver nærmere, hvilke hensyn, der skal indgå i en afgørelse om at træffe håndhævelsesforanstaltninger. I direktivets artikel 32, stk. 7, er følgende hensyn oplistet: 1) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser: a) gentagne overtrædelser, b) manglende underretning om eller afhjælpning af væsentlige hændelser, c) manglende afhjælpning af mangler efter bindende instrukser fra den kompetente myndighed, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse, e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i direktivets artikel 21 og 23, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver materiel eller immateriel skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt gerningsmanden har begået overtrædelsen forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige, samarbejder med den kompetente myndighed.

Det foreslås i *§ 333 o, stk. 2,* at midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kun kan anvendes, indtil operatøren træffer de nødvendige foranstaltninger til at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne i medfør af stk. 1, blev anvendt.

Den foreslåede bestemmelse vil implementere NIS 2-direktivets artikel 32, stk. 5, 2. afsnit, 1. pkt., hvoraf det følger, at midlertidige suspensioner eller forbud, som er pålagt i henhold til dette stykke, kun anvendes, indtil den pågældende operatør træffer de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav, som gav anledning til, at disse håndhævelsesforanstaltninger blev anvendt.

Den foreslåede bestemmelse svarer således indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 5, 2. afsnit, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger og eventuelle fortolkningsbidrag fra Kommissionen, ENISA eller andre af EU's institutioner.

Bestemmelsen indebærer, at Finanstilsynet skal træffe afgørelse om at ophæve en suspension eller et forbud, når operatøren har afhjulpet de mangler eller opfyldt de krav, som gav anledning til, at foranstaltningen blev anvendt.

Det foreslås i *stk. 3,* at en afgørelse efter stk. 1 af operatøren af finansiel digital infrastruktur eller den fysiske person, afgørelsen vedrører, kan forlanges indbragt for domstolene.

Den foreslåede bestemmelse vil implementere NIS 2-direktivets artikel 32, stk. 5, 2. afsnit, 2. pkt., hvoraf det følger, at pålæggelse af midlertidige suspensioner eller forbud skal være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder retten til effektive retsmidler og til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

Det vil efter den foreslåede bestemmelse være muligt for operatøren eller den fysiske person, som afgørelsen om suspension eller forbud vedrører, at forlange afgørelsen indbragt for retten. Når en sådan sag indbringes for retten, vil bestemmelserne i retsplejeloven finde anvendelse, hvilket vil sikre de nødvendige retssikkerhedsgarantier.

Den foreslåede bestemmelse vil ikke afskære operatøren eller den fysiske person, som afgørelsen vedrører, fra at påklage afgørelsen som led i almindelig administrativ rekurs, herunder til Erhvervsankenævnet.

Til § 333 p

Både NIS 2-direktivet og DORA-forordningen indeholder delegationer til, at Kommissionen kan fastsætte nærmere bindende regler på en række områder. Da disse reglers indhold endnu ikke er kendt, er det nødvendigt at tilvejebringe hjemmel til at fastsætte nærmere regler om it- og cyberrisikostyring i finansielle digitale infrastrukturer, der vil give mulighed for at fastsætte nærmere regler herom.

Det foreslås derfor i *§ 333 p,* at Finanstilsynet kan fastsætte nærmere regler om it- og cyberrisikostyring og kontrol- og sikringsforanstaltninger i en operatør af finansiel digital infrastruktur, herunder om de forhold, der er oplistet i nr. 1-8.

Den foreslåede bestemmelse vil indebære, at Finanstilsynet ved bekendtgørelse kan fastsætte regler, der implementerer eventuelle krav i delegerede retsakter, som udspringer NIS 2-direktivet, eller afspejler krav der udspringer af delegerede retsakter til DORA-forordningen, og som skal gælde tilsvarende for operatører af finansielle digitale infrastrukturer. Bekendtgørelser, der fastsætter regler, som implementerer eventuelle krav, der udspringer af NIS 2-direktivet, vil skulle udarbejdes i tæt koordination med Forsvarsministeriet.

Det foreslås i *nr. 1*, at Finanstilsynet kan fastsætte nærmere regler om indholdet af rammerne for styring af it- og cyberrisici og om indholdet af strategier og politikker på området for digital operationel modstandsdygtighed.

Det foreslås i *nr. 2*, at Finanstilsynet kan fastsætte nærmere regler om ledelsesorganets opgaver i forbindelse med styringen af it- og cyberrisici.

Det foreslås i *nr. 3*, at Finanstilsynet kan fastsætte nærmere regler om operatører af finansielle digitale infrastrukturers rapportering af væsentlige hændelser og cybertrusler.

Det foreslås i *nr. 4*, at Finanstilsynet kan fastsætte nærmere regler om test, herunder eksterne test, af en operatør af finansielle digitale infrastrukturers cybersikkerhed.

Det foreslås i *nr. 5*, at Finanstilsynet kan fastsætte nærmere regler om krav til testere af en operatør af finansielle digitale infrastrukturers cybersikkerhed.

Det foreslås i *nr. 6*, at Finanstilsynet kan fastsætte nærmere regler om styring og rapportering af tredjepartsrisici.

Det foreslås i *nr. 7*, at Finanstilsynet kan fastsætte nærmere regler om obligatorisk brug af særlige sikkerhedscertificerede produkter eller tjenesteydelser.

Det foreslås i *nr. 8*, at Finanstilsynet kan fastsætte nærmere regler om den interne og eksterne systemrevision i operatører af finansielle digitale infrastrukturer.

Det er tiltænkt med den foreslåede bemyndigelse i nr. 8, at Finanstilsynet vil udstede en systemrevisionsbekendtgørelse for operatører af finansielle digitale infrastrukturer, som viderefører de gældende nationale regler om systemrevision, der også i dag gælder for fælles datacentraler og it-operatører af detailbetalingssystemer.

Den foreslåede vil derfor også være en videreførelse af den bemyndigelse, der i dag følger af § 199, stk. 12, i lov om finansiel virksomhed, og § 180 h i lov om kapitalmarkeder, og som er blevet udnyttet til at udstede bekendtgørelse nr. 1581 af 22. december 2022.

Til nr. 25 (Afsnit X c i lov om finansiel virksomhed)

Kapitel 20 c i lov om finansiel virksomhed finder anvendelse for fælles datacentraler.

Ved fælles datacentraler forstås virksomheder, hvis væsentligste aktiviteter omfatter it-drifts- eller udviklingsopgaver for flere finansielle virksomheder, finansielle holdingvirksomheder, forsikringsholdingvirksomheder eller sådanne virksomheders dattervirksomheder, og som overvejende er ejet af en eller flere finansielle virksomheder mv. eller foreninger, hvis medlemmer overvejende er finansielle virksomheder, jf. § 343 q, stk. 1, i lov om finansiel virksomhed.

Det følger af § § 343 q, stk. 2, i lov om finansiel virksomhed, at reglerne for fælles datacentraler endvidere omfatter datacentraler, der udfører både væsentlig it-drift og it-udvikling for den fælles betalingsinfrastruktur, medmindre de har tilladelse som it-operatør af et detailbetalingssystem, jf. § 180 a, stk. 1, i lov om kapitalmarkeder.

Af § 343 r, stk. 1, i lov om finansiel virksomhed fremgår det, at kravet om betryggende kontrol- og sikringsforanstaltninger på it-området i § 71, stk. 1, nr. 8, finder tilsvarende anvendelse på fælles datacentraler.

Det følger videre af § 343 r, stk. 2, i lov om finansiel virksomhed, at regler om betryggende kontrol- og sikringsforanstaltninger på it-området, der er udstedt i medfør af § 71, stk. 3, i lov om finansiel virksomhed finder tilsvarende anvendelse for fælles datacentraler. Bemyndigelsen i § 71, stk. 3, i lov om finansiel virksomhed er udnyttet til at udstede bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.v., herunder bekendtgørelsens bilag 5, der fastsætter nærmere regler om bl.a. datacentralernes styring af it- og cybersikkerhed.

Det følger herudover af § 343 r, stk. 3, i lov om finansiel virksomhed, at reglerne om outsourcing udstedt i medfør af § 72 a i lov om finansiel virksomhed finder tilsvarende anvendelse for fælles datacentraler, hvis de fælles datacentraler outsourcer it-opgaver, der udføres for virksomheder omfattet af lovens § 5, stk. 1. Bemyndigelsen er udnyttet til at udstede bekendtgørelse nr. 973 af 22. juni 2022 om outsourcing for kreditinstitutter m.v., der bl.a. også omfatter datacentraler.

Med lovforslaget foreslås det, at fælles datacentraler fremover skal omfattes af de foreslåede regler til afsnit IX c, i lov om finansiel virksomhed. Det indebærer, at de gældende regler for fælles datacentraler i afsnit X c, i lov om finansiel virksomhed skal ophæves.

Det foreslås derfor at ophæve *afsnit X c*, i lov om finansiel virksomhed.

Ophævelsen af afsnit X c, i lov om finansiel virksomhed vil indebære at de fælles datacentraler, som udpeges som finansielle digitale infrastrukturer i medfør af den foreslåede § 333 i lov om finansiel virksomhed, alene vil være reguleret af reglerne i det foreslåede afsnit IX c, i lov om finansiel virksomhed.

Ophævelsen vil også indebære, at fælles datacentraler ikke længere vil blive reguleret i bekendtgørelse nr. 1103 af 30. juni 2022 om ledelse og styring af pengeinstitutter m.v. eller bekendtgørelse nr. 973 af 22. juni 2022 om outsourcing for kreditinstitutter m.v.

Til nr. 26 (§ 344, stk. 1, 1. pkt., i lov om finansiel virksomhed)

Det gældende § 344, stk. 1, i lov om finansiel virksomhed, fastlægger blandt andet Finanstilsynets generelle beføjelse til at påse overholdelsen af nærmere angivne forordninger.

Det foreslås i *§ 344, stk. 1, 1. pkt.,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022

om digital operationel modstandsdygtighed i den finansielle sektor og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 om markeder for kryptoaktiver og regler udstedt i medfør heraf.

Den foreslåede bestemmelse medfører, at Finanstilsynet udpeges som kompetent myndighed i henhold til DORA-forordningen og MiCA. Det foreslåede medfører derved, at Finanstilsynet får hjemmel til give påbud og påtaler for manglende overholdelse af DORA-forordningen og MiCA.

Med den foreslåede ændring vil Finanstilsynet desuden kunne påse overholdelsen af de regler, som der udstedes med hjemmel i henholdsvis DORA-forordningen og MiCA.
Indsættelse af henvisning til MiCA, foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester, skal være underlagt Finanstilsynets tilsyn i henhold til MiCA.

DORA-forordningen finder bl.a. anvendelse på penge- og realkreditinstitutter, jf. artikel 2, stk. 1, litra a, investeringsforvaltningsselskaber, jf. artikel 2, stk. 1, litra l, og crowdfundingtjenesteudbydere, jf. artikel 2, stk. 1, litra s.

Efter artikel 46, litra a, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, med senere ændringer (CRD), sikre overholdelsen af DORA-forordningen for penge- og realkreditinstitutter. Efter artikel 46, litra j, skal den kompetente myndighed, der er udpeget efter Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer sikre overholdelsen af forordningen for investeringsforvaltningsselskaber. Efter artikel 46, litra p, skal den kompetente myndighed, der er udpeget efter Europa-Parlamentets og Rådets forordning (EU) 2020/1503 af 7. oktober 2020 om europæiske crowdfundingtjenesteudbydere for erhvervslivet sikre overholdelsen af forordningen for crowdfundingtjenesteudbydere. Finanstilsynet er udpeget som kompetent myndighed i Danmark i henhold til disse bestemmelser.

Indsættelse af henvisning til DORA-forordningen supplerer artikel 46, litra a, j og q, i DORA-forordningen.

Til nr. 27 (§ 344 e i lov om finansiel virksomhed)

Der findes ikke i dag regler om gennemførsel af TLPT i dansk ret.

Den Europæiske Centralbank har udviklet det fælleseuropæiske rammeværk TIBER-EU. TIBER står for Threat Intelligence-Based Ethical Red-teaming og indebærer, at virksomheder med væsentlig betydning for den finansielle stabilitet, herunder pengeinstitutter, betalingsinfrastruktur og datacentraler, i samarbejde med centralbanker iværksætter simulerede cyberangreb på deres systemer ved hjælp at etiske hackere for at identificere svagheder i systemerne og cyberforsvaret generelt. Danmarks Nationalbank og den finansielle sektor er gået sammen om at etablere TIBER-DK som den danske implementering af TIBER-EU. Formålet er at styrke cyberrobustheden hos hver enkelt testdeltager og i den finansielle sektor generelt for derved at fremme den finansielle stabilitet i Danmark. TIBER-DK blev indført i december 2018, og de første test startede i januar 2019. Deltagelse i TIBER-DK er i dag frivillig for de finansielle virksomheder, der udpeges. Alle finansielle virksomheder, som Danmarks Nationalbank har rettet henvendelse til, deltager i TIBER-DK og gennemfører regelmæssige test.

Udførsel af TIBER-DK er indeholdt i Danmarks Nationalbanks overordnede formål med at sikre stabilitet i den finansielle sektor, som udledt af lov om Danmarks Nationalbank § 1, idet testen bidrager til at styrke cyberforsvaret i forhold til samfundskritiske aktiviteter i de væsentligste virksomheder i den finansielle sektor.

Det foreslås med *§ 344 e*, i lov om finansiel virksomhed, at erhvervsministeren kan fastsætte regler, der udpeger en myndighed til at varetage TLPT-relaterede anliggender i henhold til artikel 26, stk. 9, i DORA. Det omfatter også varetagelse af TLPT-relaterede anliggender i forhold til operatører af finansielle digitale infrastrukturer, jf. § 333.

Bemyndigelsen vil kunne benyttes til at fastsætte regler, der udpeger en myndighed til at være ansvarlig myndighed i henhold til DORA-forordningens artikel 26, stk. 9.

Det vil herunder være den myndighed, erhvervsministeren udpeger, der udpeger de virksomheder, der skal gennemføre test, ud fra de kriterier, der er fastlagt i DORA-forordningens kapitel IV og retsakter udstedt i medfør heraf.

Det er hensigten, at den udpegede myndighed, vil skulle være ansvarlig for TLPT-relaterede anliggender for alle virksomheder, der skal gennemføre

TLPT, herunder også virksomheder der ikke er omfattet direkte af DORA-forordningen, hvilket kan inkludere virksomheder, der er er udpeget som operatører af finansielle digitale infrastrukturer i henhold til det foreslåede § 333, jf. lovforslagets § 1, nr. 24. Med TLPT-relaterede anliggender menes de opgaver, der er indeholdt i DORA-forordningens artikel 26 og 27, der vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT (trusselsbaserede penetrationstest).

En myndighed, der af erhvervsministeren udpeges ved bemyndigelsen, som ansvarlig myndighed i henhold til DORA-forordningens artikel 26, stk. 9, vil være forpligtet til at varetage opgaven i overensstemmelse med DORA-forordningen og retsakter udstedt i medfør heraf.

Det er forventningen, at bemyndigelsen vil udnyttes til at fastsætte regler, der udpeger Danmarks Nationalbank som ansvarlig myndighed i henhold til DORA-forordningens artikel 26, stk. 9.

Til nr. 28 (§ 348, stk. 2, i lov om finansiel virksomhed)

Lov om finansiel virksomhed § 348, stk. 2, indeholder regler om Finanstilsynets beføjelser til at give påbud om berigtigelse af forhold, der er i strid med §§ 43 og 57 i lov om finansiel virksomhed.

Det følger af § 335, nr. 81, i lov nr. 718 af 13. juni 2023 om forsikringsvirksomhed, at §§ 55-60 a i lov om finansiel virksomhed ophæves.

Ved en fejl er der ikke foretaget en konsekvensrettelse af henvisningen til § 57 i § 348, stk. 2, i lov om finansiel virksomhed.

Det foreslås i *§ 348, stk. 2,* at ændre »§§ 43 og 57« til »§ 43«.

Det foreslåede vil medføre, at henvisningen til den ophævede § 57 udgår af § 348, stk. 2.

Til nr. 29 (§ 351, stk. 8, i lov om finansiel virksomhed)

§ 351 indeholder regler om påbud om afsættelse af direktører og bestyrelsesmedlemmer i forsikringsselskaber. § 351, stk. 8, fastsætter regler om, at Finanstilsynet af egen drift eller efter ansøgning kan tilbagekalde et påbud meddelt efter stk. 2 og 3, og stk. 5, 3. pkt.

Med § 1, nr. 35, i lov nr. 409 af 25. april 2023 (Gennemførelse af Ansvarsudvalgets forslag om skærpet ansvarsvurdering for

ledelsesmedlemmer m.v. i finansielle virksomheder og ændring af reglerne om egnethed og hæderlighed) blev der indsat to nye punktummer i § 351, stk. 5. Ved en fejl blev der ikke foretaget en konsekvensændring af henvisningen til stk. 5, 3. pkt., i § 351, stk. 8, i lov om finansiel virksomhed.

Det foreslås i *§ 351, stk. 8,* at ændre »stk. 5, 3. pkt.« til »stk. 5, 5. pkt.«.

Ændringen er en konsekvensrettelse på baggrund af § 1, nr. 35, i lov nr. 409 af 25. april 2023.

Til nr. 30 (§ 354, stk. 6, i lov om finansiel virksomhed)

I medfør af § 354, stk. 1, i lov om finansiel virksomhed er Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger, som de bl.a. får kendskab til gennem tilsynsvirksomheden.

§ 354, stk. 6, i lov om finansiel virksomhed er en undtagelse til tavshedspligten i stk. 1. Bestemmelsen fastsætter til hvem og i hvilke tilfælde Finanstilsynet kan videregive fortrolige oplysninger, uanset § 354, stk. 1.

I medfør af § 354, stk. 6, har Finanstilsynet ikke mulighed for at videregive oplysninger til Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 354, stk. 6,* at indsætte *nr. 50,* hvorefter Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større it-relateret hændelse fra et penge- eller realkreditinstitut, et investeringsforvaltningsselskab eller en crowdfundingtjenesteudbyder, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4,

litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 31 (§ 354 e, stk. 3 og § 373 i lov om finansiel virksomhed)

Det følger af § 354 e, stk. 1, i lov om finansiel virksomhed, at Finanstilsynet offentliggør påtaler, påbud eller tvangsbøder i sager nævnt i stk. 2, som bl.a. fremhæver sager i henhold til § 125 d, stk. 3. § 373 angiver, at overtrædelse af relevant lovgivning, herunder § 125, stk. 3, straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

§ 125 d, stk. 3, nr. 1-3, blev ved lov nr. 2110 af 22. december 2020 rykket til § 125 d, stk. 5, nr. 1-3.

Det foreslås to steder i *§ 354 e, stk. 2, 1. pkt.,* og to steder i *§ 373, stk. 1* og *9,* at ændre »§ 125 b, stk. 1-4 og 6« til: »§ 125 b, stk. 3-5 og 8«.

Med det foreslåede tager henvisningen højde for de ændringer, der blev foretaget af § 125 b ved § 1, nr. 39, i lov nr. 2110 af 22. december 2020.

Til nr. 32 (§ 354 e, stk. 2, 2. pkt., i lov om finansiel virksomhed)

Det fremgår af § 354 e, stk. 1, at Finanstilsynet på sin hjemmeside offentliggør i de sager, der er nævnt i stk. 2, påtaler, påbud eller tvangsbøder meddelt i henhold til § 269, stk. 1, eller § 344, stk. 1, og navnet på virksomheden eller personen.

Stk. 2, 1. pkt., fastsætter, at der skal ske offentliggørelse ved overtrædelse af en række bestemmelser i lov om finansiel virksomhed og i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 om tilsynsmæssige krav til kreditinstitutter (CRR). Videre fremgår det af stk. 2, 2. pkt., at offentliggørelse ligeledes skal ske i sager om overtrædelse af Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter (MiFIR).

Det fremgår af stk. 4 i bestemmelsen, at indbringes påtalen, påbuddet eller tvangsbøden nævnt i stk. 1, jf. stk. 2, for Erhvervsankenævnet eller domstolene, skal dette fremgå af offentliggørelsen. Status og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Det foreslås i *§ 354 e, stk. 2, 2. pkt.,* at indsætte en henvisning til DORA-forordningen, hvormed offentliggørelse, jf. stk. 1, ligeledes skal ske i sager om overtrædelse af forordningen.

Det foreslås i § 1, nr. 9, i nærværende lovforslag, at Finanstilsynet bliver udpeget som kompetent myndighed efter DORA-forordningen til at føre tilsyn med overholdelsen af forordningen. Den foreslåede ændring vil medføre, at Finanstilsynet bl.a. vil kunne udstede påbud og påtaler for overtrædelser af DORA-forordningen.

Den foreslåede ændring gennemfører artikel 54, stk. 1, i DORA-forordningen, hvormed de kompetente myndigheder uden unødigt ophold på deres officielle websteder skal offentliggøre enhver afgørelse om pålæggelse af en administrativ sanktion, som ikke kan påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen. En administrativ sanktion kan bl.a. kan være et påbud eller en påtale. Det fremgår dog videre af artikel 54, stk. 5, i DORA-forordningen, at hvis den kompetente myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En

judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

Artikel 54, stk. 1 og 5, svarer derfor til kravet om offentliggørelse i § 354 e, stk. 1, sammenholdt med kravet i § 354 e, stk. 4.

For nærmere om § 354 e og offentliggørelse henvises der i det hele til de specielle bemærkningerne til § 354 e i Folketingstidende 2013-14, tillæg A, L 133 som fremsat, side 188-189.

Til nr. 33 (§ 354 h i lov om finansiel virksomhed)

Det følger af § 254 h, 1. pkt., at Finanstilsynet efter høring af den virksomhed, der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, orienterer offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere en igangværende hændelse. I 2. og 3. pkt. i bestemmelsen fremgår nærmere om, at en offentliggørelse ikke må indeholde fortrolige oplysninger.

Bestemmelsen gennemfører artikel 14, stk. 6, i NIS-direktivet om, at den kompetente myndighed kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge en hændelse eller håndtere en igangværende hændelse.

Med NIS 2-direktivet sker der en ophævelse af NIS-direktivet, herunder reglerne i artikel 14, stk. 6.

Det foreslås derfor at ophæve *§ 354 h.*

Til nr. 34 (§ 355, stk. 1, i lov om finansiel virksomhed)

§ 355, stk. 1, i lov om finansiel virksomhed, nævner de virksomheder, der kan anses som part i forhold til Finanstilsynet i sager, hvor Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af bl.a. lov om finansiel virksomhed og andre relevante forordninger på det finansielle område.

Det foreslås i *§ 355, stk. 1,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU)

2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf.

Det foreslåede medfører, at virksomheder, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af DORA-forordningen, MiCA eller regler udstedt i medfør af disse forordninger, også vil være at anse som parter i afgørelsessagen.

Til nr. 35 (§ 361, stk. 1, nr. 4, i lov om finansiel virksomhed)

§ 361 i lov om finansiel virksomhed foreskriver, at en række fysiske og juridiske personer skal betale et årligt grundbeløb i afgift til Finanstilsynet. Beløbene angivet i bestemmelsen er angivet i 2016-niveau, men reguleres årligt svarende til udviklingen i Finanstilsynets bevilling på finansloven, jf. § 361, stk. 11, i lov om finansiel virksomhed.

Det følger af § 361, stk. 1, nr. 4, 1. pkt., i lov om finansiel virksomhed, at en fælles datacentral årligt betaler et grundbeløb til Finanstilsynet på 119.000 kr. Videre fremgår det af 2. pkt., at har en fælles datacentral i et regnskabsår gennemsnitligt færre end 25 fuldtidsansatte, betaler den fælles datacentral dog 2.200 kr.

Ved fælles datacentraler forstås virksomheder, hvis væsentligste aktiviteter omfatter it-drifts- eller udviklingsopgaver for flere finansielle virksomheder, finansielle holdingvirksomheder, forsikringsholdingvirksomheder eller sådanne virksomheders dattervirksomheder, og som overvejende er ejet af en eller flere finansielle virksomheder, finansielle holdingvirksomheder, forsikringsholdingvirksomheder eller sådanne virksomheders dattervirksomheder i forening eller en eller flere foreninger, hvis medlemmer overvejende er finansielle virksomheder, finansielle holdingvirksomheder, forsikringsholdingvirksomheder eller sådanne virksomheders dattervirksomheder, jf. § 343 q, stk. 1.

Reglerne for fælles datacentraler i lov om finansiel virksomhed gælder også for datacentraler, der udfører både væsentlige it-drifts og it-udvikling for den fælles betalingsinfrastruktur, jf. § 343 q, stk. 2, 1. pkt. Derfor er disse virksomheder også omfattet af gebyrbestemmelsen i § 361, stk. 1, nr. 4.

På baggrund heraf foreslås det, at den nuværende *§ 361, stk. 1, nr. 4*, ophæves, og i stedet foreslås det i *stk. 1, nr. 4, 1. pkt.*, at en finansiel digital infrastruktur årligt betaler et grundbeløb til Finanstilsynet på 119.000 kr. Afgiften er fastsat med udgangspunkt i det forventede ressourceforbrug og

det forventede antal virksomheder, der vil blive udpeget som finansielle digitale infrastrukturer.

Det foreslås i *nr. 4, 2. pkt.*, at har en finansiel digital infrastruktur i et regnskabsår gennemsnitligt færre end 25 fuldtidsansatte, betaler den finansielle digitale infrastruktur dog 2.200 kr.

Den foreslåede bestemmelse er tilsvarende den nuværende nr. 4, 2. pkt., for så vidt angår fælles datacentraler. Da Finanstilsynet bl.a. regner med at udpege de virksomheder, der i dag er fælles datacentraler, findes det hensigtsmæssigt, at finansielle digitale infrastrukturer også kun skal betale 2.200 kr., hvis de gennemsnitligt har færre end 25 fuldtidsansatte i et regnskabsår.

Det foreslås i *nr. 4, 3. pkt.*, at 1. og 2. pkt., ikke finder anvendelse på en it-operatør af detailbetalingssystemer, der er udpege som finansiel digital infrastruktur.

Det foreslåede skal ses i sammenhæng med lovforslagets § 1, nr. 25, hvorved afsnit X c i lov om finansiel virksomhed foreslås ophævet, herunder §§ 343 q og r, der indeholder regler om fælles datacentraler.

Det foreslåede skal ligeledes ses i sammenhæng med lovforslagets § 1, nr. 24, hvorved det foreslås, at Finanstilsynet kan udpege en enhed, der udbyder digital infrastruktur eller forvalter it-tjenester, som omhandlet i bilag I i NIS 2-direktivet, og hvis væsentligste aktiviteter består i at drive, administrere eller udvikle tjenester, der er nødvendige for finansielle virksomheders kritiske og vigtige forretningsfunktioner, som en finansiel digital infrastruktur. Forslaget herom vil bl.a. bevirke, at de virksomheder, der i dag er fælles datacentraler eller datacentraler, der udfører både væsentlige it-drifts og it-udvikling for den fælles betalingsinfrastruktur, vil blive udpeget af Finanstilsynet som finansielle digitale infrastrukturer.

Da en it-operatør af detailbetalingssystemer i forvejen betaler et årligt grundbeløb til Finanstilsynet på 725.000 kr., jf. § 361, stk. 2, nr. 15, er Finanstilsynets udgifter til løbende tilsyn allerede dækket heraf.

Til nr. 36 (§ 361, stk. 1, nr. 11 og 12, i lov om finansiel virksomhed)

Den gældende § 361, stk. 1, i lov om finansiel virksomhed fastlægger størrelsen på den afgift, som virksomheder med tilladelse efter den finansielle regulering pålægges at betale til Finanstilsynet.

Udgifterne til Finanstilsynet dækkes af de finansielle virksomheder m.fl., som Finanstilsynet fører tilsyn med. Den årlige afgift for de forskellige typer virksomheder er fastsat i §§ 361-366 i lov om finansiel virksomhed.

Det foreslås i *§ 361, stk. 1, nr. 11,* at udstedere af aktivbaserede tokens, der er meddelt tilladelse af Finanstilsynet i henhold til artikel 21, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, årligt betaler et grundbeløb til Finanstilsynet i henhold til litra a-c.

Det foreslås i § 361, stk. 1, *litra a,* at udstedere af aktivbaserede tokens årligt betaler 35.000 kr. til Finanstilsynet, når summen af udstederens gennemsnitlige udestående aktivbaserede tokens i 2. halvår af det foregående kalenderår og 1. halvår af det indeværende kalenderår er mindre end 100 mio. kr.

Det foreslås i § 361, stk. 1, *litra b,* at udstedere af aktivbaserede tokens årligt betaler 100.000 kr. til Finanstilsynet, når summen af udstederens gennemsnitlige udestående aktivbaserede tokens i 2. halvår af det foregående kalenderår og 1. halvår af det indeværende kalenderår er mellem 100 mio. kr. og 1 mia. kr.

Det foreslås i § 361, stk. 1, *litra c,* at udstedere af aktivbaserede tokens årligt betaler 600.000 kr. til Finanstilsynet, når summen af udstederens gennemsnitlige udestående aktivbaserede tokens i 2. halvår af det foregående kalenderår og 1. halvår af det indeværende kalenderår er større end 1 mia. kr.

Den foreslåede bestemmelse vil medføre, at en udsteder af aktivbaserede tokens på lige fod med andre virksomheder omfattet af den finansielle regulering pålægges en afgift.

Det foreslås i *§ 361, stk. 1, nr. 12,* at en udbyder af kryptoaktivtjenester, der er meddelt tilladelse af Finanstilsynet i henhold til artikel 63 i MiCA, skal betale et årligt grundbeløb til Finanstilsynet på 12,5 promille af deres omkostninger til løn, provision og tantieme, dog minimum 20.000 kr.

Den foreslåede bestemmelse vil fastsætte, at en udbyder af kryptoaktivtjenester på lige fod med andre virksomheder omfattet af den finansielle regulering pålægges en afgift.

De foreslåede bestemmelser er nye og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter fysiske og juridiske personer og visse andre virksomheder, der er involveret i

udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester, skal være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Til nr. 37 (§ 361, stk. 6, nr. 1, i lov om finansiel virksomhed)

Det følger af § 361, stk. 6, nr. 1, i lov om finansiel virksomhed, at Virksomheder og personer omfattet af § 1, stk. 1, nr. 8 og 22-26, i hvidvaskloven betaler 4.400 kr. årligt til Finanstilsynet.

I *§ 361, stk. 6, nr. 1,* at »og 22-26« udgår.

Det foreslåede medfører, at der ikke vil blive krævet afgift af virksomheder, der er omfattet af § 1, stk. 1, nr. 22-26, i hvidvaskloven.

Det foreslåede skal ses i sammenhæng med lovforslagets § 1, nr. 36, om afgiftsforpligt for virksomheder, der er omfattet af MiCA.

Til nr. 38 (§ 361, stk. 7, nr. 4, i lov om finansiel virksomhed)

Det følger af § 361, stk. 7, i lov om finansiel virksomhed, at en række fysiske og juridiske personer omfattet af lov om forvaltere og alternative investeringsfonde m.v. skal betale et årligt grundbeløb til Finanstilsynet.

Grundbeløbet reguleres årligt i henhold til § 361, stk. 12, i lov om finansiel virksomhed.

Det fremgår af § 130 i lov om forvaltere af alternative investeringsfonde m.v., at forvaltere af alternative investeringsfonde med registreret hjemsted i et tredjeland, kan få tilladelse af Finanstilsynet til at markedsføre andele til professionelle investorer i Danmark i en alternativ investeringsfond, som forvalteren forvalter, når en række nærmere angivne betingelser er opfyldt.

Ved en fejl blev forvaltere af alternative investeringsfonde, der markedsfører andele i en alternativ investeringsfond fra et land inden for Den Europæiske Union eller et land, som Unionen har indgået aftale med på det finansielle område, ikke medtaget ved nyaffattelsen af § 361, stk. 7, i lov om finansiel virksomhed som blev gennemført ved lov nr. 480 af 12. maj 2023.

Det foreslås i *§ 361, stk. 7,* at indsætte et nyt *nr. 4,* hvorefter forvaltere af alternative investeringsfonde med registreret hjemsted i et tredjeland, som i henhold til § 130 i lov om forvaltere af alternative investeringsfonde m.v. har tilladelse til markedsføring i Danmark af andele i en alternativ

investeringsfond fra et andet land inden for Den Europæiske Union eller et land, som Unionen har indgået aftale med på det finansielle område, betaler et årligt grundbeløb til Finanstilsynet på 8.000 kr.

Den foreslåede bestemmelse vil medføre, at der fremover vil være hjemmel til at opkræve et årligt grundbeløb for forvaltere af alternative investeringsfonde fra et tredjeland, der i Danmark markedsfører andele i en alternativ investeringsfond fra et land inden for Den Europæiske Union eller et land, som Unionen har indgået aftale med på det finansielle område.

Til nr. 39 (§ 361, stk. 12, i lov om finansiel virksomhed)

Det følger af § 361, stk. 12, at grundbeløb, jf. stk. 1-11, er angivet i 2016-niveau og reguleres årligt svarende til udviklingen i Finanstilsynets bevilling på finansloven.

§§ 361 og 362 indeholder grundbeløb, maksimumafgift og minimumsbeløb.

Et eksempel på et grundbeløb er § 361, stk. 1, nr. 2, hvorved Arbejdsmarkedets Tillægspension (ATP) betaler 4.922.000 kr. årligt.

Et eksempel på et maksimumbeløb er § 361, stk. 2, nr. 2, 1. pkt., hvorved afgiften til et selskab, der driver en multilateral handelsfacilitet højst, kan udgøre 1.462.000 kr.

Et eksempel på en minimumsafgift er § 362, stk. 1, 2. pkt., hvorved Fondsmæglerselskaber altid pålægges en minimumsafgift på 15.000 kr. årligt.

Det foreslås i *§ 361, stk. 12,* at ændre »grundbeløb, jf. stk. 1-11,« til: »faste beløb i dette kapitel«.

Den foreslåede ændring præciserer, at maksimumbeløbene og minimumsafgifterne, er i 2016-niveau og årligt reguleres i forhold til udviklingen i Finanstilsynets bevilling i henhold til Finansloven.

Den foreslåede ændring forventes at medføre en minimal ændring i fordelingen af afgifterne i henhold til kapitel 22, hvorved virksomhederne, der betaler minimumsafgifter eller maksimumbeløb, vil skulle betale en marginalt højere afgifter.

Formålet med ændringen er at sikre afgifter angivet som faste beløb i kapitel 22, såkaldte minimums-, og grundbeløb samt minimusafgifter, mod inflation.

Der henvises i øvrigt til pkt. 2.6 i lovforslagets almindelige bemærkninger.

Til nr. 40 (§ 368, stk. 1, 4. pkt., i lov om finansiel virksomhed)

Det gældende § 368, stk. 1, i lov om finansiel virksomhed, fastsætter, hvordan beregning af afgifter fra en række virksomheder skal foretages.

I § 368, stk. 1, foreslås et nyt *4. pkt.*, som bestemmer, at for så vidt angår udstedere af aktivbaserede tokens, foregår beregningen på grundlag af den senest indsendte indberetning efter § 332 f, og for så vidt angår udbydere af kryptoaktivtjenester, foregår beregningen på grundlag af den senest indsendte indberetning efter § 332 g.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter fysiske og juridiske personer og visse andre virksomheder, der er involveret i udstedelse, udbud til offentligheden og optagelse til handel af kryptoaktiver, eller som leverer kryptoaktivtjenester, skal være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Til nr. 41 (§ 372, stk. 1, i lov om finansiel virksomhed)

Den gældende § 372, stk. 1, i lov om finansiel virksomhed indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet retter sig til. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet i medfør af lov om finansiel virksomhed og en række EU-retsakter på det finansielle område.

Det foreslås i *§ 372, stk. 1*, at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver samt regler udstedt i medfør heraf.

Det foreslåede medfører, at afgørelser truffet af Finanstilsynet i medfør af DORA-forordningen eller regler udstedt i medfør samt i medfør af MiCA og regler udstedt i medfør heraf, kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, som afgørelsen retter sig til.

Til nr. 42 (§ 372 a, stk. 1, i lov om finansiel virksomhed)

Den gældende § 372 a, stk. 1, i lov om finansiel virksomhed er en generel bemyndigelsesbestemmelse, der bemyndiger erhvervsministeren til at fastsætte regler, som er nødvendige for at anvende eller gennemføre de afgørelser eller retsakter, som vedtages af Europa-Kommissionen i medfør af en række direktiver og forordninger.

Det foreslås i *§ 372 a, stk. 1,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den ændrede bestemmelse vil give erhvervsministeren bemyndigelse til at fastsætte regler, som er nødvendige for at anvende eller gennemføre de afgørelser eller retsakter, som vedtages af Europa-Kommissionen i medfør af MiCA og DORA-forordningen.

Bestemmelsen indføres for at kunne efterleve artikel 139 i MiCA, der tillægger Europa-Kommissionen beføjelser til at udstede en række delegerede retsakter.

Til nr. 43 (§ 373, stk. 1, i lov om finansiel virksomhed)

Det gældende § 373, stk. 1, i lov om finansiel virksomhed, fastsætter, hvilke overtrædelser af lov om finansiel virksomhed samt en række EU-retsakter, der kan straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås i *§ 373, stk. 1,* at ændre »samt artikel 3« til: », artikel 3«, og efter »om europæiske crowdfundingtjenesteudbydere for erhvervslivet« at indsætte: »samt artikel 14, stk. 3, artikel 16, stk. 1, artikel 23, stk. 1 og 4, artikel 36, stk. 1-3 og 5-7, artikel 38, stk. 1 og 3, artikel 39, stk. 2, artikel 40, stk. 1 og 2, artikel 48, stk. 1, artikel 49, stk. 4, artikel 50, stk. 1 og 2, artikel 54, artikel 59, stk. 1, artikel 60, stk. 1-6, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, artikel 75, stk. 7, artikel 76, stk. 1, 2 og 5-8, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver «.

Det foreslåede vil indebære, at overtrædelser af de nævnte artikler i MiCA, straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Artikel 14, stk. 3, i MiCA fastsætter krav om returnering af midler til erhververne af kryptoaktiverne i de tilfælde, hvor udbuddet af

kryptoaktiverne bliver annulleret. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, til offentligheden. Den strafbare handling består i, at udbydere ikke returnerer de indsamlede midler til indehaverne af de udbudte kryptoaktiver eller de potentielle indehavere, senest 25 kalenderdage efter udbuddets annullationsdato.

Artikel 16, stk. 1, i MiCA fastsætter krav om tilladelse til at udbyde aktivbaserede tokens til offentligheden og til at ansøge om optagelse til handel. Ansvarssubjektet for overtrædelse af bestemmelsen er personer, der udbyder aktivbaserede tokens til offentligheden eller anmoder om optagelse af aktivbaserede tokens til handel i EU. Den strafbare handling består eksempelvis i, at udstedere af aktivbaserede tokens udbyder disse tokens til offentligheden, uden at være meddelt tilladelse hertil af Finanstilsynet i overensstemmelse med artikel 21 i MiCA.

Artikel 23, stk. 1 og 4, i MiCA fastsætter begrænsninger på udstedelser af aktivbaserede tokens, der i udbredt grad anvendes som vekslingsmiddel. Aktivbaserede tokens benyttes som vekslingsmiddel, når de anvendes til betaling af gæld, herunder i forbindelse med transaktioner med handlende. Derimod bør transaktioner, der knytter sig til investeringsfunktioner og -tjenester, såsom veksling til midler eller andre kryptoaktiver ikke anses som benyttelse som vekslingsmiddel, medmindre den aktivbaserede token anvendes til afvikling af transaktioner i andre kryptoaktiver. Der vil foreligge en anvendelse til afvikling af transaktioner i andre kryptoaktiver i tilfælde, hvor en transaktion, der involverer to elementer af kryptoaktiver, som er forskellige fra de aktivbaserede tokens, afvikles i de aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen ikke ophører udstedelsen af de aktivbaserede tokens, som har overskredet tærskelværdierne i artikel 23, stk. 1.

Artikel 36, stk. 1-3 og 5-7, i MiCA omhandler forpligtigelser for udstedere af aktivbaserede tokens vedrørende udstederens reserve af aktiver og sammensætning og forvaltning af denne. Ansvarssubjektet for overtrædelser af stk. 1-3, 5 og 7, er udstedere af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af stk. 6, er ledelsesorganerne for udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen ikke har sikret, at reserven af aktiver er operationelt adskilt fra udstederens realformue og fra reserven af aktiver for andre aktivbaserede tokens.

Artikel 38, stk. 1 og 3, i MiCA fastsætter krav til udstedere af aktivbaserede tokens i forbindelse med investering af reserven af aktiver. Ansvarssubjektet

for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstedere investerer reserven af aktiver i andet end meget likvide finansielle instrumenter med minimal markedsrisiko, kreditrisiko og koncentrationsrisiko.

Artikel 39, stk. 2, i MiCA omhandler de permanente indløsningsrettigheder forbundet med aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelsen er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstedere af aktivbaserede tokens, efter anmodning fra en indehaver, ikke genindløser de aktivbaserede tokens enten ved at betale et beløb i andre midler end elektroniske penge svarende til markedsværdien af de aktiver, som de aktivbaserede tokens, der besiddes, henviser til, eller ved at levere de aktiver, som disse tokens henviser til.

Artikel 40, stk. 1 og 2, i MiCA fastsætter et forbud mod rentetilskrivning. Ansvarssubjekterne for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens og udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udstedere af aktivbaserede tokens overfører aktivbaserede tokens eller andre kryptoaktiver til holdere af udstederens aktivbaserede tokens, som vederlag for den tid, i hvilken en indehaver af udstederens aktivbaserede tokens besidder sådanne. Et andet eksempel på den strafbare handling består i, at udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder, tilbyder disse kunder renter eller andet vederlag for den tid, udbyderens kunder deponerer aktivbaserede tokens hos udbyderen. Den strafbare handling består eksempelvis i, at en udbyder af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver, tilbyder indehavere af aktivbaserede tokens et vederlag eller andre ydelser for den tid, i hvilken en indehaver af aktivbaserede tokens deponerer sådanne aktivbaserede tokens hos udbyderen.

Artikel 48, stk. 1, i MiCA fastsætter krav til personer, der udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel. Ansvarssubjektet for overtrædelse af bestemmelsen er pengeinstitutter, der udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU. Ansvarssubjektet kan endvidere være andre personer, der efter skriftligt samtykke fra pengeinstituttet udbyder eller anmoder om optagelse til handel af e-pengetokens. Den strafbare handling består eksempelvis i, at et pengeinstitut udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU, uden at pengeinstituttet har givet meddelelse til Finanstilsynet om en hvidbog om kryptoaktiver og har offentliggjort denne hvidbog om kryptoaktiver i overensstemmelse med artikel 51 i MiCA.

Artikel 49, stk. 4, i MiCA omhandler kravene til at genindløse e-pengetokens til kurs pari. Ansvarssubjektet for overtrædelse af bestemmelsen er pengeinstitutter, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et pengeinstitut, der udsteder e-pengetokens, opkræver et gebyr eller anden betaling for at indløse indehaveres e-pengetokens.

Artikel 50, stk. 1 og 2, i MiCA omhandler forbud mod rentetilskrivning. Ansvarssubjekterne for overtrædelse af bestemmelserne er et pengeinstitut, der udsteder e-pengetokens, og udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at et pengeinstitut, der udsteder e-pengetokens, overfører e-pengetokens eller andre kryptoaktiver til holdere af disse e-pengetokens, som vederlag for den tid, i hvilken en indehaver af e-pengetokens besidder sådanne. Et andet eksempel på den strafbare handling består i, at udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder, tilbyder disse kunder renter eller andet vederlag.

Artikel 54 i MiCA fastsætter krav vedrørende investering af pengemidler modtaget som betaling for e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelsen er et pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et pengeinstitut, der udsteder e-pengetokens, investerer alle de modtagne midler i sikre aktiver med lav risiko og dermed undlader at indsætte mindst 30% af de modtagne pengemidler på en særskilt konto i et pengeinstitut.

Artikel 59, stk. 1, i MiCA omhandler tilladelseskrav til at udbyde kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver fysisk eller juridisk person, der udbyder kryptoaktivtjenester, uden den nødvendige tilladelse. Den strafbare handling består i at udbyde kryptoaktivtjenester uden enten at være meddelt tilladelse efter artikel 63 eller uden at have tilladelse til at levere kryptoaktivtjenester efter artikel 60 i MiCA.

Artikel 60, stk. 1-6, i MiCA fastsætter krav om underretning af Finanstilsynet førend visse finansielle virksomheder kan levere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelserne er pengeinstitutter, værdipapircentraler, investeringsselskaber, e-pengeinstitutter, UCITS-administrationsselskaber, forvaltere af alternative investeringsfonde og markedsoperatører. Den strafbare handling består eksempelvis i, at et pengeinstitut påbegynder levering af en kryptoaktivtjeneste uden at have underrettet Finanstilsynet med de

oplysninger, der er anført i artikel 60, stk. 7, mindst 40 arbejdsdage før pengeinstituttet leverer disse tjenester første gang.

Artikel 70, stk. 1-4, i MiCA omhandler krav vedrørende opbevaring af kundernes kryptoaktiver og midler. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester, der opbevarer kryptoaktiver på vegne af deres kunder, ikke træffer passende foranstaltninger til at forhindre, at kundernes kryptoaktiver anvendes til handel for deres egen regning.

Artikel 72, stk. 1, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester ikke opretholder og anvender effektive politikker til at identificere mellem dem selv og personerne opregnet i artikel 72, stk. 1, litra a-e.

Artikel 75, stk. 1, 2 og 7, i MiCA indebærer specifikke krav til udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, som udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at udbydere, der leverer deponering og administration af kryptoaktiver på vegne af kunder, ikke holder deres kunders kryptoaktiver adskilt fra udbydernes egne kryptoaktiver.

Artikel 76, stk. 1, 2, og 5-8, i MiCA fastsætter specifikke krav til udbydere af kryptoaktivtjenester, der driver en handelsplatform for kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, der driver en handelsplatform for kryptoaktiver. Den strafbare handling består eksempelvis i, at udbydere, der driver handelsplatforme, handler for egen regning på den handelsplatform for kryptoaktiver, som de driver.

Den foreslåede ændring supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en række udbydere, der beskæftiger sig med kryptoaktiver, skal leve op til forordningens krav.

Til nr. 44 (§ 373, stk. 2, i lov om finansiel virksomhed)

Den gældende § 373, stk. 2, i lov om finansiel virksomhed fastsætter, hvilke overtrædelser af lov om finansiel virksomhed samt en række EU-retsakter, der kan straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås i *§ 372, stk. 2*, at udgår »§ 71 c, stk. 1, 2. pkt.,«, efter »312 b« indsættes: »§ 333 a, stk. 1-3, § 333 b, stk. 1-6, § 333 d, stk. 1-4, § 333 e, stk. 1-12, § 333 f, stk. 1-8, § 333 g, stk. 1-3, § 333 h, stk. 1-13, § 333 i, stk. 1 og 2, § 333 j, stk. 1-3,«, og at »samt artikel 4« ændres til: », artikel 4«, og at efter »om europæiske crowdfundingtjenesteudbydere for erhvervslivet« indsættes: », artikel 4, stk. 1, stk. 3, 3. pkt., og stk. 6, artikel 5, stk. 2 og 3, artikel 6, stk. 1-10, artikel 7, stk. 1 og 2, artikel 8, stk. 1-2 og 4-6, artikel 9, artikel 10, artikel 12, stk. 1-4 og 6-9, artikel 13, stk. 2 og 3, artikel 14, artikel 16, stk. 1, 2. afsnit, artikel 17, stk. 1 og 2, artikel 19, stk. 1-9, artikel 22, stk. 1 og 3, artikel 25, stk. 1, 2 og 4, artikel 27, artikel 28, artikel 29, stk. 1-3 og 6, artikel 30, artikel 31, stk. 1-4, artikel 32, stk. 1-4, artikel 33, artikel 34, stk. 1-12, artikel 35, stk. 1, artikel 36, stk. 8-12, artikel 37, stk. 1 og 2, artikel 39, stk. 1, 2. pkt., artikel 41, stk. 1 og 2, artikel 46, stk. 1 og 2, artikel 47, stk. 1-3, artikel 48, stk. 6 og 7, artikel 49, stk. 5, artikel 51, stk. 1-9, 11-13 og stk. 14, 1. pkt., artikel 53 stk. 1-3, 5 og 6, artikel 55, artikel 59, stk. 2, 5 og 8, artikel 64, stk. 8, artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 67, stk. 1, 5 og 6, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9, artikel 76, stk. 3, 4 og 9-15, artikel 77, artikel 78, artikel 79, artikel 80, stk. 1-3, artikel 81, stk. 1-14, artikel 82, stk. 1, artikel 83, stk. 1 og 2, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver samt artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede vil indebære, at overtrædelse af de nævnte bestemmelser i henholdsvis lov om finansiel virksomhed, MiCA og DORA-forordningen kan straffes med bøde.

I det følgende redegøres for de nævnte artikler i MiCA.

Artikel 4, stk. 1 i MiCA fastsætter krav til personer, der udbyder kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, til

offentligheden. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver person, som udbyder de ovennævnte kryptoaktiver. Den strafbare handling består i, at en person udbyder kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, til offentligheden, uden at opfylde kravene i artikel 4, stk. 1, litra a-g.

Artikel 4, stk. 3, 3. pkt., og stk. 6, i MiCA omhandler krav til udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Kravene er rettet mod udbydere, som enten er omfattet af undtagelsen om udbud af utility tokens, der giver adgang til en vare eller tjenesteydelse i artikel 4, stk. 3, litra c, eller af undtagelsen om begrænset netværk i artikel 4, stk. 3, litra d. Ansvarssubjektet for overtrædelse af bestemmelserne er enhver person, som udbyder de ovennævnte kryptoaktiver. Den strafbare handling består eksempelvis i, at udbydere af utility tokens, som giver adgang til en vare eller tjenesteydelse, som endnu ikke eksisterer eller endnu ikke udbydes, overskrider den maksimale gyldighedsperiode på 12 måneder. Det vil ligeledes efter bestemmelsen være strafbart, hvis en udbyder af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, som er omfattet af undtagelsen om begrænset netværk, ikke notificerer Finanstilsynet med en meddelelse, der indeholder en beskrivelse af udbuddet og en redegørelse for, hvorfor udbuddet er undtaget fra afsnit 2 i MiCA, i henhold til artikel 4, stk. 3, litra d, når udbuddet til offentligheden i EU overstiger 1.000.000 EUR for hver periode på 12 måneder regnet fra det oprindelige udbuds begyndelse.

Artikel 5, stk. 2 og 3, i MiCA omhandler krav til operatører af handelsplatforme, som, helt eller delvist på eget initiativ, ønsker at optage et kryptoaktiv til handel på operatørens handelsplads. Ansvarssubjektet for overtrædelse af bestemmelserne er operatører af handelsplatforme. Den strafbare handling består eksempelvis i, at en operatør af en handelsplatform ikke opfylder kravene i artikel 5, stk. 1, når handelsplatformen på eget initiativ optager et kryptoaktiv, som ikke har en tilhørende hvidbog offentliggjort, til handel.

Artikel 6, stk. 1-10, i MiCA omhandler kravene til indhold og form af hvidbøger for kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelserne er enhver person, der udbyder et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til offentligheden, eller enhver person, der anmoder om optagelse til handel af et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens eller en operatør af en handelsplatform, der på eget initiativ optager et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til handel. Den strafbare handling består eksempelvis i, at en udbyder offentliggør en hvidbog, som ikke oplyser om de rettigheder og

forpligtelser, der er knyttet til de udbudte kryptoaktiver, eller at udbyderen offentliggør en hvidbog med vildledende oplysninger.

Artikel 7, stk. 1 og 2, i MiCA omhandler krav til markedsføringskommunikation, som enten vedrører et udbud til offentligheden af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, eller optagelse af sådanne kryptoaktiver til handel. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens eller personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet kan endvidere være en operatør af en handelsplatform, som på eget initiativ optager et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til handel. Den strafbare handling består eksempelvis i, at en handelsplatform, som optager et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til handel på eget initiativ, offentliggør markedsføringskommunikation, hvor oplysningerne i markedsføringskommunikationen ikke stemmer overens med de oplysninger, som fremgår af hvidbogen.

Artikel 8, stk. 1-2 og 4-6, i MiCA omhandler forpligtigelsen til at meddele Finanstilsynet eller anden relevant kompetent myndighed om hvidbogen om kryptoaktiver og om markedsføringskommunikationen. Ansvarssubjektet er udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens eller personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet kan endvidere være en operatør af en handelsplatform, som på eget initiativ optager et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til handel. Den strafbare handling består eksempelvis i, at en udbyder af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, ikke mindst 20 arbejdsdage før offentliggørelsen af hvidbogen om kryptoaktiver giver meddelelse til Finanstilsynet om de elementer, der er beskrevet i artikel 8, stk. 1 og 4.

Artikel 9 i MiCA omhandler krav vedrørende offentliggørelse af hvidbogen om kryptoaktiver og offentliggørelse af markedsføringskommunikationen. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, eller personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet kan endvidere være en operatør af en handelsplatform, som på eget initiativ optager et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til handel. Den strafbare handling består eksempelvis i, at en udbyder offentliggør en hvidbog om kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, som ikke er identisk med den version, udbyderen har meddelt

Finanstilsynet, i overensstemmelse med artikel 8 eller i givet fald med den version, der er ændret i overensstemmelse med artikel 12.

Artikel 10 i MiCA fastsætter krav for afslutning af et udbud til offentligheden og beskyttelsesforanstaltninger i forbindelse hermed. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Den strafbare handling består eksempelvis i, at en udbyder ikke offentliggør resultatet af udbuddet på udbyderens websted senest 20 arbejdsdage efter tegningsperiodens afslutning, i de tilfælde hvor udbuddet har været tidsbegrænset.

Artikel 12, stk. 1-4 og 6-9, i MiCA fastsætter krav i forbindelse med ændring af offentliggjorte hvidbøger om kryptoaktiver og af offentliggjort markedsføringskommunikation. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens eller personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet kan endvidere være en operatør af en handelsplatform, som på eget initiativ optager et kryptoaktiv, undtagen aktivbaserede tokens eller e-pengetokens, til handel. Den strafbare handling består eksempelvis i, at udbyderen ikke tidsstempler den ændrede hvidbog om kryptoaktiver.

Artikel 13, stk. 2 og 3, i MiCA omhandler krav til fortrydelsesretten ved køb af kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktiver, undtaget aktivbaserede tokens og e-pengetokens, og udbydere af kryptoaktivtjenester bestående af placering af kryptoaktiver. Den strafbare handling består eksempelvis i, at en udbyder af kryptoaktiver pålægger detailindehavere, som ønsker at gøre brug af deres fortrydelsesret efter artikel 13, stk. 1, gebyrer eller andre omkostninger i forbindelse hermed.

Artikel 14, stk. 1 og 2, i MiCA fastsætter forpligtelser for udbydere og personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere og personer, der anmoder om optagelse til handel af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens. Ansvarssubjektet kan endvidere være en operatør af en handelsplatform, der på eget initiativ optager kryptoaktiver, undtagen aktivbaserede tokens og e-pengetokens, til handel. Den strafbare handling består eksempelvis i, at en udbyder kommunikerer med indehavere og potentielle indehavere af kryptoaktiver, undtagen aktivbaserede tokens eller e-pengetokens, på en vildledende måde.

Artikel 16, stk. 1, 2. afsnit, i MiCA fastsætter krav om skriftligt samtykke, hvis andre end udstederen udbyder aktivbaserede tokens til offentligheden eller ansøger om optagelse til handel. Ansvarssubjektet for overtrædelse af bestemmelsen er personer, som udbyder aktivbaserede tokens, og personer, der anmoder om optagelse af aktivbaserede tokens til handel i EU, som ikke er udstederen. Den strafbare handling består i, at tredjemand enten anmoder om at få optaget en aktivbaseret token til handel eller udbyder aktivbaserede tokens uden skriftligt samtykke fra udstederen, eller hvor tredjemand i forbindelse hermed ikke efterlever artikel 27, 29 og 40 i MiCA.

Artikel 17, stk. 1 og 2, i MiCA fastsætter krav til pengeinstitutter for udbud eller optagelse til handel af aktivbaserede tokens udstedt af disse. Ansvarssubjektet for overtrædelse af bestemmelserne er pengeinstitutter. Den strafbare handling består eksempelvis i, at et pengeinstitut udsteder en aktivbaseret token uden først at meddele Finanstilsynet de oplysninger, som fremgår af artikel 17, stk. 1, litra b, nr. 1-8.

Artikel 19, stk. 1-9, i MiCA fastsætter krav til indhold og form af hvidbogen for aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at hvidbogen ikke indeholder de oplysninger, som er opregnet i artikel 19, stk. 1, at oplysningerne i hvidbogen er vildledende, eller at hvidbogen indeholder påstande om de aktivbaserede tokens fremtidige værdi.

Artikel 22, stk. 1 og 3, i MiCA fastsætter krav til udstedere af aktivbaserede tokens om indberetning af oplysninger til Finanstilsynet. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at en udsteder af aktivbaserede tokens, hvis samlede udstedelser overstiger en værdi af 100 millioner EUR, undlader hvert kvartal at meddele Finanstilsynet de oplysninger, som er oplistet i artikel 22, stk. 1, litra a-d.

Artikel 25, stk. 1, 2 og 4, i MiCA fastsætter krav i forbindelse med ændring af offentliggjorte hvidbøger for aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen undlader at give meddelelse til Finanstilsynet om en påtænkt ændring af udstederens forretningsmodel, som kan tænkes at få væsentlig indflydelse på enhver faktisk eller potentiel indehavers købsbeslutning vedrørende aktivbaserede tokens, når ændringen indtræffer efter den i artikel 21 omhandlede tilladelse.

Artikel 27 i MiCA omhandler udstedere af aktivbaserede tokens forpligtelse til at handle ærligt, redeligt og professionelt og i den bedste interesse for

indehavere af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelsen er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstedere af aktivbaserede tokens fortrinsbehandler visse indehavere af deres udstedte tokens, når der ikke foreligger oplysninger om fortrinsbehandlingen i hvidbogen om kryptoaktiver.

Artikel 28 i MiCA fastsætter krav om offentliggørelse af hvidbøger for aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelsen er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen offentliggør den godkendte hvidbog på udstederens websted senere end begyndelsesdagen for udbuddet til offentligheden.

Artikel 29, stk. 1-3 og 6, i MiCA fastsætter krav til markedsføringskommunikation, der vedrører udbud til offentligheden eller optagelse til handel af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at markedsføringskommunikationen er vildledende eller ikke stemmer overens med oplysningerne i hvidbogen.

Artikel 30 i MiCA fastsætter krav om løbende oplysninger til indehavere af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelsen er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen ikke ajourfører oplysningerne anført i artikel 30, stk. 1, 2. pkt., mindst hver måned.

Artikel 31, stk. 1-4, i MiCA fastsætter krav til klagebehandlingsprocedure for udstedere af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen opkræver gebyrer for at behandle klager fra indehavere af aktivbaserede tokens.

Artikel 32, stk. 1-4, i MiCA omhandler krav om identificering, forebyggelse, håndtering og oplysning i forbindelse med interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen ikke træffer alle relevante foranstaltninger til at identificere interessekonflikter mellem udstederen og udstederens aktionærer, ansatte eller indehavere af aktivbaserede tokens.

Artikel 33 i MiCA omhandler kravet om indberetning af ændringer i ledelsesorganet. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består i, at en

udbyder af kryptoaktivtjenester ikke øjeblikkeligt giver meddelelse til Finanstilsynet om enhver ændring i udbyderens direktionen eller bestyrelse. Eller hvor meddelelsen ikke indeholder alle de oplysninger, der er nødvendige for Finanstilsynets vurdering af overholdelsen af artikel 34, stk. 2, i MiCA.

Artikel 34, stk. 1-12, i MiCA omhandler krav til udstedere af aktivbaserede tokens ledelsesordninger. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens og medlemmer af ledelsesorganet hos udbydere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at ledelsesorganet hos udstedere af aktivbaserede tokens ikke evaluerer effektiviteten af den politik og de ordninger og procedurer, der er indført for at efterleve kapitel 2, 3, 5 og 6 i MiCA.

Artikel 35, stk. 1, i MiCA fastsætter krav til kapitalgrundlaget for udstedere af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelsen er udstedere af aktivbaserede tokens. Den strafbare handling består i, at udstedere af aktivbaserede tokens ikke har et kapitalgrundlag, som er i overensstemmelse med artikel 35, stk. 1. Det indebærer eksempelvis, at udstederen af aktivbaserede tokens ikke har et kapitalgrundlag svarende til et beløb, der svarer til mindst det højeste af følgende: 350 000 EUR, 2 % af det gennemsnitlige beløb af reserven af aktiver som omhandlet i artikel 36, eller en fjerdedel af det foregående års faste omkostninger.

Artikel 36, stk. 8-12, i MiCA omhandler forpligtelser for udstedere af aktivbaserede tokens vedrørende udstederens reserve af aktiver og sammensætning og forvaltning af denne. Bestemmelserne fastsætter blandt andet krav om, at udstedere af aktivbaserede tokens skal have en klar og detaljeret politik, der beskriver stabiliseringsmekanismen for sådanne tokens, og at udstederne skal give autorisation til gennemførelsen af en uafhængig revision af reserven af aktiver hver sjette måned. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at politikken, der beskriver stabiliseringsmekanismen, ikke indeholder en detaljeret vurdering af de risici, herunder kreditrisiko, markedsrisiko, koncentrationsrisiko og likviditetsrisiko, som følger af reserven af aktiver.

Artikel 37, stk. 1 og 2, i MiCA omhandler forpligtigelser til udstedere af aktivbaserede tokens i forbindelse med deponering af reserven af aktiver. Ansvarssubjektet for overtrædelse af bestemmelsen er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstederen ikke har tilstrækkelige politikker og procedurer eller indgået i

kontraktlige ordninger, som til enhver tid sikrer, at kravene i artikel 37, stk. 1, litra a-e, er opfyldt.

Artikel 39, stk. 1, 2. pkt., i MiCA fastsætter udstedere af aktivbaserede tokens forpligtigelser til at fastlægge, opretholde og gennemføre klare og detaljerede politikker og procedurer for indehavernes permanente genindløsningsrettigheder. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at udstedere af aktivbaserede tokens ikke har tilstrækkeligt klare og detaljerede politikker for sikring af indehaveres permanente genindløsningsrettigheder.

Artikel 41, stk. 1 og 2, i MiCA omhandler forpligtigelsen til at give meddelelse til Finanstilsynet ved erhvervelser eller afhændelser af kvalificerede andele i udstedere af aktivbaserede tokens. Ansvarssubjektet for overtrædelse af bestemmelserne er enhver fysisk eller juridisk person eller sådanne personer, som handler i forståelse med hinanden, og som har besluttet direkte eller indirekte at erhverve eller afhænde en kvalificeret andel i en udsteder af aktivbaserede tokens. Den strafbare handling består eksempelvis i, at en erhverver af en kvalificeret andel ikke på forhånd giver skriftlig meddelelse til Finanstilsynet herom.

Artikel 46, stk. 1 og 2, i MiCA omhandler krav til udstedere af aktivbaserede tokens om at udarbejde og opretholde en genopretningsplan, samt underrette Finanstilsynet om genopretningsplanen. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens og udstedere af e-pengetokens. Den strafbare handling består eksempelvis i, at udstederens genopretningsplan ikke indeholder passende betingelser og procedurer for at sikre rettidig gennemførelse af genopretningsforanstaltninger.

Artikel 47, stk. 1-3, i MiCA omhandler udstedere af aktivbaserede tokens forpligtigelse til at udarbejde og opretholde en operationel plan til støtte for en velordnet genindløsning af hver aktivbaseret token. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere af aktivbaserede tokens og udstedere af e-pengetokens. Den strafbare handling består eksempelvis i, at udstederens genindløsningsplan ikke sikrer kontinuitet i kritiske aktiviteter, der udføres af udstederen eller af eventuelle tredjepartsenheder, og som er nødvendige for en velordnet genindløsning.

Artikel 48, stk. 6 og 7, i MiCA omhandler pligten til at underrette Finanstilsynet, inden et pengeinstitut udbyder e-pengetokens til offentligheden eller anmoder om at få e-pengetokens optaget til handel. Ansvarssubjektet for overtrædelse af bestemmelserne er et pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et

pengeinstitut, der udsteder e-pengetokens, ikke underretter Finanstilsynet senest 40 arbejdsdage før den dato, hvor det har til hensigt at udbyde disse e-pengetokens til offentligheden eller anmode om e-pengenes optagelse til handel.

Artikel 49, stk. 5, i MiCA omhandler oplysningspligten vedrørende betingelserne for genindløsningen. I denne lov skal "genindløsning" forstås i overensstemmelse med § 96 i lov om betalinger. Ansvarssubjektet for overtrædelse af bestemmelsen er et pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består i, at et pengeinstitut, der udsteder e-pengetokens, ikke oplyser om betingelserne for genindløsning på en fremtrædende plads i hvidbogen om kryptoaktiver.

Artikel 51, stk. 1-9, 11-13 og stk. 14, 1. pkt., i MiCA omhandler kravene til indhold og form af hvidbogen om kryptoaktiver vedrørende e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelserne er et pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at hvidbogen ikke indeholder alle oplysninger, som fremgår af artikel 51, stk. 1, i MiCA, eller at oplysningerne i hvidbogen er vildledende.

Artikel 53, stk. 1-3, 5 og 6, i MiCA omhandler markedsføringskommunikation, der vedrører et udbud til offentligheden af e-pengetokens eller optagelse af sådanne e-pengetokens til handel. Ansvarssubjektet for overtrædelse af bestemmelserne er et pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at markedsføringskommunikationen ikke indeholder en klar og utvetydig erklæring om, at indehavere af e-pengetokens har ret til, når som helst, at genindløse disse e-pengetokens over for udstederen til pariværdi.

Artikel 55 i MiCA fastsætter at udstedere af e-pengetokens er omfattet af kravene i artikel 46 og 47 i MiCA. Derudover fastsætter bestemmelsen datoen, hvorpå genopretningsplanen senest skal meddeles Finanstilsynet. Ansvarssubjektet for overtrædelse af bestemmelsen er et pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et pengeinstitut, der udsteder e-pengetokens, ikke har udarbejdet eller opretholdt en genopretningsplan, som er i overensstemmelse med kravene i artikel 46 og 47.

Artikel 59, stk. 2, 5 og 8, i MiCA fastsætter krav vedrørende hjemsted, anvendelse af navn og selskabsform for udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelserne er enhver person, som udbyder kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at en kryptoaktivtjenesteudbyder med registreret hjemsted i Danmark ikke udfører nogen af dens aktiviteter fra Danmark. Ligeledes straffes en person,

der uden at have tilladelse til at udbyde kryptoaktivtjenester, anvender et navn eller et firmanavn, udsender markedsføringskommunikation eller anvender nogen anden proces, der antyder, at den pågældende er kryptoaktivtjenesteudbyder.

Artikel 64, stk. 8, i MiCA regulerer udbydere af kryptoaktivtjenesters forpligtigelse til at sikre overførelse af deres kunders kryptoaktiver og midler, i tilfælde af, at udbyderens tilladelse bliver inddraget. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at en udbyder af en kryptoaktivtjeneste ikke har passende procedurer for, hvorledes kryptoaktiver, som opbevares på vegne af deres kunder, vil blive overført til en anden udbyder af en kryptoaktivtjeneste i tilfælde af inddragelse af udbyderens tilladelse.

Artikel 65, stk. 4, i MiCA omhandler oplysningskrav ved grænseoverskridende levering af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består i, at en udbyder af en kryptoaktivtjeneste påbegynder leveringen af kryptoaktivtjenester i en anden medlemsstat end Danmark inden 15 kalenderdage efter at have indgivet oplysninger efter artikel 65, stk. 1, eller inden at have modtaget meddelelse fra Finanstilsynet efter artikel 65, stk. 2.

Artikel 66, stk. 1-5, i MiCA omhandler udbydere af kryptoaktivtjenesters forpligtelse til at handle ærligt, redeligt og professionelt i kundernes bedste interesse. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester giver deres kunder vildledende oplysninger.

Artikel 67, stk. 1, i MiCA omhandler tilsynsmæssige krav til udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester på et givent tidspunkt ikke opfylder kravet om at have indført forsigtighedshensyn svarende til minimum det højeste beløb af den permanente minimumskapital, der er anført i bilag 4, eller en fjerdedel af det foregående års faste omkostninger, jf. artikel 67, stk. 1, litra b.

Artikel 67, stk. 5 og 6, i MiCA omhandler kravene til forsikringspolicers dækning og offentliggørelse i de tilfælde, hvor udbydere af kryptoaktivtjenester vælger at benytte forsikringspolicer eller tilsvarende garantier til at efterleve kravene i artikel 67, stk. 1. Ansvarssubjektet for

overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbyderen af kryptoaktivtjenester ikke offentliggør den i artikel 67, stk. 4, litra b, omhandlede forsikringspolice, eller at den offentliggjorte forsikringspolice ikke omfatter dækning af risiciene oplistet i artikel 67, stk. 6, litra a-g.

Artikel 68, stk. 4-9 i MiCA omhandler kravene til ledelsesordninger og indretningen af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af artikel 68, stk. 4, 5 og 7-9, er udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af artikel 68, stk. 6, er ledelsesorganet hos udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbyderen ikke har vedtaget procedurer, som er tilstrækkelige til at sikre overholdelsen af MiCA. Den strafbare handling kan endvidere bestå i, at ledelsesorganer hos en udbyder af kryptoaktivtjenester ikke regelmæssigt vurderer og evaluerer effektiviteten af den politik og de ordninger og procedurer, der er indført for at opfylde forpligtelserne i artikel 66-83 i MiCA, herunder ikke træffer passende foranstaltninger til at afhjælpe eventuelle mangler.

Artikel 69 i MiCA omhandler krav til at meddele Finanstilsynet eventuelle ændringer i ledelsesorganet hos en udbyder af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester ikke giver Finanstilsynet alle oplysninger, som er nødvendige for Finanstilsynets vurdering af overholdelsen af artikel 68 i MiCA, inden nye medlemmerne af ledelsesorganet tiltræder deres stilling.

Artikel 71, stk. 1-4, i MiCA fastsætter krav til udbydere af kryptoaktivtjenesters klagebehandlingsprocedurer. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester kræver betaling af gebyr eller anden afgift i forbindelse med behandling af klager fra deres kunder.

Artikel 72, stk. 2-4, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester ikke oplyser deres kunder og potentielle kunder om de skridt, udbyderen har taget for at begrænse interessekonflikter.

Artikel 73, stk. 2 og 3, i MiCA regulerer udbydere af kryptoaktivtjenesters outsourcing af tjenester eller aktiviteter til tredjeparter. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester ikke træffer alle rimelige foranstaltninger for at undgå yderligere operationel risiko, eller at udbydere af kryptoaktiver ikke sikrer at betingelserne i artikel 73, stk. 1, litra a-g, til enhver tid er opfyldt.

Artikel 74 i MiCA omhandler velordnet afvikling af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester, som udfører de i artikel 75-79 i MiCA beskrevne aktiviteter. Den strafbare handling består eksempelvis i, at den i artikel 74 nævnte plan for velordnet afvikling ikke godtgør, at udbyderen af kryptoaktivtjenesten har evnen til at gennemføre en velordnet afvikling uden at påføre sine kunder unødig økonomisk skade.

Artikel 75, stk. 3-6 og 9, i MiCA fastsætter forpligtelser for udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, som udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at kryptoaktivtjenesteudbyderens politik for deponering, som anført i artikel 75, stk. 3, ikke minimerer risikoen for tab af kunders kryptoaktiver som følge af svig, cybertrusler eller forsømmelighed.

Artikel 76, stk. 3, 4 og 9-15, i MiCA fastsætter en række krav til drift af handelsplatforme for kryptoaktiver, herunder krav til indholdet af handelsplatformens driftsregler, krav om offentliggørelse af handelsoplysninger, krav vedrørende afvikling af kryptoaktivtransaktioner, mv. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, der driver en handelsplatform for kryptoaktiver. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester, der driver handelsplatforme for kryptoaktiver, ikke offentliggør pris, volumen og tidspunkt for de transaktioner, der udføres i forbindelse med kryptoaktiver handlet på deres handelsplatforme.

Artikel 77 i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der veksler mellem kryptoaktiver og midler eller andre kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester, der veksler mellem kryptoaktiver og midler eller andre kryptoaktiver. Den strafbare handling består eksempelvis i, at udbydere ikke udfører kundernes ordrer til de viste priser på det tidspunkt, hvor ordren vedrørende veksling var endelig.

Artikel 78 i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der udfører ordrer vedrørende kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester, der udfører ordrer vedrørende kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at udbyderen ikke har udarbejdet og gennemført en politik for ordreudførelse, der sikrer, at udbyderen er i stand til at opnå det bedst mulige resultat i forbindelse med kundeordrer.

Artikel 79 i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der placerer kryptoaktiver, herunder krav om underretning af udbydere af kryptoaktiver, personer, der anmoder om optagelse af kryptoaktiver til handel, eller enhver tredjepart, der handler på disses vegne, om de oplysningerne, som fremgår af artikel 79, stk. 1, litra a-d. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester, der placerer kryptoaktiver. Placering af kryptoaktiver er defineret i artikel 3, stk. 1, nr. 21, i MiCA. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester i forbindelse med placering af kryptoaktiver ikke underretter en udbyder af kryptoaktiver om oplysningerne i artikel 79, stk. 1, litra a-d, inden der indgås kontrakt om placering af kryptoaktiver.

Artikel 80, stk. 1-3, i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der modtager og formidler ordrer vedrørende kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, der modtager og formidler ordrer vedrørende kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at en udbyder af en kryptoaktivtjeneste, der modtager og formidler ordrer, ikke indfører procedurer og ordninger, der sikrer hurtig og korrekt formidling af kunders ordrer til udførelse på en handelsplatform for kryptoaktiver.

Artikel 81, stk. 1-14, i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der yder rådgivning om kryptoaktiver og udbydere af kryptoaktivtjenester, som yder porteføljepleje af kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelserne er både udbydere af kryptoaktivtjenester, som yder rådgivning om kryptoaktiver, og udbydere af kryptoaktivtjenester, som yder porteføljepleje af kryptoaktiver. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester, der yder rådgivning om kryptoaktiver eller porteføljepleje af kryptoaktiver, undlader at advare deres kunder eller potentielle kunder om de forhold, som er oplistet i artikel 81, stk. 9, litra a-f.

Artikel 82, stk. 1, i MiCA fastsætter krav til indholdet af den aftale udbydere af kryptoaktivtjenester, der udbyder overførselstjenester på vegne af kunder, skal indgå med deres kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, der udbyder overførselstjenester på vegne af kunder. Den strafbare handling består eksempelvis i, at udbydere af overførelsestjenester ikke indgår en aftale med deres kunder, som indeholder de punkter, der er oplistet i artikel 82, stk. 1, litra a-e.

Artikel 83, stk. 1 og 2, i MiCA fastsætter krav til meddelelse af Finanstilsynet i forbindelse med erhvervelser af kvalificerede ejerandele i udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelserne er enhver fysisk eller juridisk person eller sådanne personer, som handler i forståelse med hinanden, og som har besluttet direkte eller indirekte at erhverve eller afhænde en kvalificeret andel i en udbyder af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at en fysisk person erhverver eller afhænder en kvalificeret andel i en udbyder af kryptoaktivtjenester uden forinden at meddele Finanstilsynet herom.

De foreslåede ændringer, for så vidt angår indsættelse af henvisning til artikler i MiCA, supplerer artikel 111, stk. 1, afsnit 2, i MiCA.

Disse ændringer foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en række aktører, som beskæftiger sig med kryptoaktiver, skal leve op til kravene i forordningen.

I det følgende redegøres for de nævnte artikler i DORA-forordningen.

Med den foreslåede ændring strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der

stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor er en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der hermed penge- og realkreditinstitutter, udbydere af kryptoaktivtjenester, crowdfundingtjenesteudbydere, securitiseringsregistre og kreditvurderingsbureauer, jf. artikel 2, stk. 1, litra a, s, t og q, jf. artikel 2, stk. 2, i DORA-forordningen.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en

kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke

etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der er pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov

og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og

med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e), skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til

artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks.

hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6,

litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller

for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet. Er der eksempelvis tale om et pengeinstitut, kan en kerneaktivitet være muligheden for at udstede lån til kunder. En gennemgang og en analyse af en it-relateret hændelse har til formål at mindske risikoen for, at en lignende hændelse opstår igen.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om

ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i

forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året

aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1, nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1 er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at der hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier

mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1, bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed

ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse

har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer,

herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkelig hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den

finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-

tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige

tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller

vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i

deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til nr. 45 (§ 373, stk. 9, i lov om finansiel virksomhed)

Det følger af § 373, stk. 9, i lov om finansiel virksomhed, at forældelsesfristen er 10 år for overtrædelse af de oplistede bestemmelser.

Overtrædelse af de oplistede bestemmelser er enten grove, da de kan have alvorlige økonomiske konsekvenser for en virksomhed, indskyderne, investorerne m.v., eller være egnet til at skade tilliden til den finansielle sektor.

Det foreslås i *§ 373 stk. 9, 2. pkt.,* at Forældelsesfristen er ligeledes 10 år for overtrædelse af artikel 16, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Artikel 16, stk. 1, i MiCA fastsætter, at en person ikke må udbyde en aktivbaseret token til offentligheden eller anmode om optagelse til handel heraf i Unionen, medmindre denne person er udstederen af denne aktivbaserede token og er en juridisk person eller virksomhed, der er etableret i Unionen, og er meddelt tilladelse hertil af den kompetente myndighed i sit hjemland i overensstemmelse med artikel 21, eller et kreditinstitut, der opfylder kravene i artikel 17 i forordningen.

Den foreslåede ændring vil medføre, at forældelsesfristen for strafansvar bliver 10 år for overtrædelse af art. 16, stk. 1i MiCA.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udstedelse af aktivbaserede tokens skal leve op til en række krav i forordningen.

Til nr. 46 (bilag 1, nr. 13, i lov om finansiel virksomhed)

Det gældende bilag 1 i lov om finansiel virksomhed indeholder en liste med de aktiviteter, som en virksomhed med tilladelse som pengeinstitut kan udføre. Det fremgår ikke, at et pengeinstitut kan udstede e-pengetokens.

Det foreslås at nyaffatte *bilag 1, nr. 13,* således: »Udstedelse af elektroniske penge, herunder elektroniske pengetokens, som defineret i artikel 3, stk. 1, nr. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

Det foreslåede vil medføre, at pengeinstitutter kan udstede elektroniske penge, herunder e-pengetokens, som defineret i artikel 3, stk. 1, nr. 7, i MiCA.

Bestemmelsen supplerer artikel 146 i MiCA.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udstedere af e-pengetokens skal leve op til en række krav i forordningen.

Til nr. 47 (bilag 1, nr. 14 og 15, i lov om finansiel virksomhed)

Det gældende bilag 1 i lov om finansiel virksomhed indeholder en liste med de aktiviteter, som en virksomhed med tilladelse som pengeinstitut kan udføre. Det fremgår ikke, at et pengeinstitut kan udstede aktivbaserede tokens som defineret i artikel 3, stk. 1, nr. 6, i MiCA og udbyde kryptoaktivtjenester som defineret i artikel 3, stk. 1, nr. 16, i MiCA.

Det foreslås, at der i bilag 1 til lov om finansiel virksomhed indsættes nyt *nr. 14,* hvorefter pengeinstitutvirksomhed omfatter udstedelse af aktivbaserede tokens som defineret i artikel 3, stk. 1, nr. 6, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslås, at der i bilag 1 til lov om finansiel virksomhed indsættes nyt *nr. 15,* hvorefter pengeinstitutvirksomhed omfatter udbud af kryptoaktivtjenester som defineret i artikel 3, stk. 1, nr. 16, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslåede vil medføre, at en virksomhed med tilladelse som pengeinstitut kan udstede aktivbaserede tokens og udbyde kryptoaktivtjenester i medfør af MiCA.

Bestemmelsen supplerer artikel 146 i MiCA.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter pengeinstitutter, der udsteder aktivbaserede tokens eller udbyder kryptoaktivtjenester, skal leve op til en række krav i forordningen.

Til nr. 48 (bilag 2, nr. 11-13, i lov om finansiel virksomhed)

Det gældende bilag 2 i lov om finansiel virksomhed indeholder en liste med de aktiviteter, som en virksomhed med tilladelse som kreditinstitut kan udføre. Det fremgår ikke, at et kreditinstitut kan udstede aktivbaserede tokens som defineret i artikel 3, stk. 1, nr. 6, i MiCA, udstede e-pengetokens, som defineret i artikel 3, stk. 1, nr. 7 og udbyde kryptoaktivtjenester som defineret i artikel 3, stk. 1, nr. 15, i MiCA.

Det foreslås, at der i bilag 2 til lov om finansiel virksomhed indsættes nyt *nr. 11*, hvorefter kreditinstitutvirksomhed omfatter udstedelse af elektroniske penge, herunder elektroniske pengetokens som defineret i artikel 3, stk. 1, nr. 7, i Europa-Parlamentets og Rådets (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslås, at der i bilag 2 til lov om finansiel virksomhed indsættes nyt *nr. 12*, hvorefter kreditinstitutvirksomhed omfatter udstedelse af aktivbaserede tokens som defineret i artikel 3, stk. 1, nr. 6, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslås, at der i bilag 2 til lov om finansiel virksomhed indsættes nyt *nr. 13*, hvorefter kreditinstitutvirksomhed omfatter udbud af kryptoaktivtjenester som defineret i artikel 3, stk. 1, nr. 16, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslåede vil medføre, at en virksomhed med tilladelse som kreditinstitut kan udstede elektroniske penge, herunder elektroniske pengetokens, aktivbaserede tokens og udbyde kryptoaktivtjenester i medfør af MiCA.

Det foreslåede indsættes med henblik på, at en udenlandsk virksomhed, som kan udføre aktiviteter i Danmark i henhold til §§ 30 og 31, i lov om finansiel virksomhed, også kan udstede elektroniske penge, herunder elektroniske pengetokens, aktivbaserede tokens og udbyde kryptoaktivtjenester i medfør af MiCA.

Bestemmelsen supplerer endvidere artikel 146 i MiCA.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter kreditinstitutter, der udsteder aktivbaserede tokens, udsteder e-pengetokens eller udbyder kryptoaktivtjenester, skal leve op til en række krav i forordningen.

Til § 2

Til nr. 1 (fodnoten i lov om betalinger)

Lov om betalinger gennemfører i dag dele af NIS-direktivet.

Det foreslås i *fodnoten*, at ændre »og dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019 om ændring af direktiv 2013/36/EU, for så vidt angår fritagne enheder, finansielle holdingselskaber, blandede finansielle holdingselskaber, aflønning, tilsynsforanstaltninger og -beføjelser og kapitalbevaringsforanstaltninger, EU-Tidende 2019, nr. L 150, side 253 (CRD V)« til: », dele af Europa-Parlamentets og Rådets direktiv 2019/878/EU af 20. maj 2019 om ændring af direktiv 2013/36/EU, for så vidt angår fritagne enheder, finansielle holdingselskaber, blandede finansielle holdingselskaber, aflønning, tilsynsforanstaltninger og -beføjelser og kapitalbevaringsforanstaltninger, EU-Tidende 2019, nr. L 150, side 253 (CRD V) og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

Med den foreslåede ændring til fodnoten indsættes en henvisning til, at der med denne lov foretages en gennemførelse af dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor. Denne henvisning tilføjes, idet lovforslaget gennemfører artikel 3 i direktivet, der fastsætter ændringer til Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked. Direktivet er et følgedirektiv til DORA-forordningen. Med forslaget til § 3, nr. 12, foreslås det, at Finanstilsynet skal påse overholdelsen af DORA-forordningen.

Der henvises til lovforslagets § 2, nr. 14.

Til nr. 2 (§ 5, stk. 1, nr. 10, i lov om betalinger)

Det følger af det gældende § 5, stk. 1, nr. 10, at loven ikke finder anvendelse på tjenester leveret af en udbyder af tekniske tjenester, der understøtter udbuddet af betalingstjenester, såfremt udbyderen ikke på noget tidspunkt er i besiddelse af de midler, som skal overføres, og der ikke er tale om tjenester omfattet af bilag 1, nr. 7 og 8, jf. dog § 122.

Det foreslås, at *§ 5, stk. 1, nr. 10*, nyaffattes, så loven ikke finder anvendelse på tjenester leveret af en udbyder af tekniske tjenester, der understøtter

udbuddet af betalingstjenester, når udbyderen ikke på noget tidspunkt er i besiddelse af de midler, som skal overføres, og der ikke er tale om tjenester omfattet af bilag 1, nr. 7 og 8, jf. dog § 122.

Bestemmelsen sikrer en direktivnær implementering af artikel 3, stk. 1, litra j, i 2. betalingstjenestedirektiv, som er i overensstemmelse med Europa-Parlamentets og Rådets direktiv 2022/2556 (EU) af 13. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor. Dette direktiv ændrer artikel 3, stk. 1, litra j, i det 2. betalingstjenestedirektiv og medfører, at også tjenester leveret af en udbyder af informations- og kommunikationsteknologi (it) er undtaget lov om betalinger, når denne på intet tidspunkt er i besiddelse af de midler, som skal overføres, og der ikke er tale om tjenester omfattet af bilag 1, nr. 7 og 8.

Det foreslåede vil medføre, at undtagelsen i § 5, nr. 10, omfatter en række tjenester leveret af tekniske leverandører. Det drejer sig eksempelvis om håndtering og lagring af data, databeskyttelse- og validering, levering af informations- og kommunikationsteknologi (it), drift af kommunikationsnetværk samt levering og vedligeholdelse af betalingsterminaler. Disse tjenester er kendetegnet ved, at de pågældende leverandører på intet tidspunkt er i besiddelse af midlerne, der overføres i betalingstransaktionen. Det er yderligere en betingelse, at den tekniske tjeneste understøtter udbuddet af betalingstjenester. Undtagelsen gælder derfor ikke, hvis det er udbyderen af den tekniske tjeneste, der indgår aftalen om betalingstjenester med betaler eller betalingsmodtager, desuagtet at udbyderen ikke kommer i besiddelse af midlerne på noget tidspunkt.

Som eksempel på virksomheder, der udbyder denne type tjenester, kan nævnes pengeinstitutternes datacentraler og leverandører af kortterminaler i fysisk handel eller betalingsmoduler til brug ved internethandel.

Dog gælder § 122 om urimelige priser og avancer desuagtet. Bestemmelsen viderefører § 4, stk. 1, nr. 10, i den gældende lov om betalingstjenester og elektroniske penge og gennemfører samtidig 2. betalingstjenestedirektivs artikel 3, stk. 1, litra j.

Til nr. 3 (§ 11, stk. 1, nr. 11, i lov om betalinger)

§ 11 i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til et e-pengeinstitut eller et betalingsinstitut skal indeholde til brug for Finanstilsynets vurdering af, om kravene til at opnå en tilladelse hertil i henhold til § 10 i lov om betalinger er opfyldt.

Det fremgår af § 11, stk. 1, nr. 11, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange og interne kontrolmekanismer, herunder administrative, risikostyringsmæssige og regnskabsmæssige og regnskabsmæssige procedurer, jf. § 25 i lov om betalinger.

Bestemmelsen gennemfører artikel 5, stk. 1, litra e, i 2. betalingstjenestedirektivet og artikel 3, stk. 1, i 2. e-pengedirektiv, jf. artikel 111, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5 også finder anvendelse på en ansøgning som e-pengeinstitut.

Det foreslås i *§ 11, stk. 1, nr. 11,* at ændre bestemmelsen således, at det fremgår, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange og interne kontrolmekanismer, herunder administrative, risikostyringsmæssige og regnskabsmæssige procedurer samt ordninger for brug af it-tjenester i overensstemmelse medEuropa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.
Forordningen finder bl.a. anvendelse på betalingsinstitutter og e-pengeinstitutter, jf. artikel 2, stk. 1, litra b og d.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra a, i, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der ændrer i artikel 5, stk. 1, litra e, i 2. betalingstjenestedirektivet.

Til nr. 4 (§ 11, stk. 1, nr. 12, i lov om betalinger)

§ 11 i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til et e-pengeinstitut eller et betalingsinstitut skal indeholde til brug for Finanstilsynets vurdering af, om kravene til at opnå en tilladelse hertil i henhold til § 10 i lov om betalinger er opfyldt.

Det fremgår af § 11, stk. 1, nr. 12, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange for håndtering og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder procedurer for indberetning af sikkerhedshændelser, jf. § 127 i lov om betalinger.

§ 127 i lov om betalinger fastsætter regler om, at en udbyder af betalingstjenester skal underrette Finanstilsynet om større drifts- og sikkerhedshændelser.

Bestemmelsen gennemfører artikel 5, stk. 1, litra f, i 2. betalingstjenestedirektivet og artikel 3, stk. 1, i 2. e-pengedirektiv, jf. artikel 111, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5 også finder anvendelse på en ansøgning som e-pengeinstitut.

Det foreslås i *§ 11, stk. 1, nr. 12,* at ændre: »§ 127« til: »kapitel III i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede medfører, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange for håndtering og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder procedurer for indberetning af sikkerhedshændelser, jf. kapitel III i DORA-forordningen.

Kapitel III i DORA-forordningen indeholder regler om styring, klassificering og indberetning af it-relaterede hændelser. it-relaterede hændelser er defineret som hændelser, der kompromitterer sikkerheden i net- og informationssystemerne og har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de tjenester, som den finansielle enhed leverer, jf. artikel 3, nr. 8, i DORA-forordningen.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra a, ii, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der ændrer i artikel 5, stk. 1, litra f, i 2. betalingstjenestedirektivet.

Der henvises i øvrigt til lovforslagets § 2, nr. 12, og bemærkningerne hertil.

Til nr. 5 (§ 11, stk. 1, nr. 15, i lov om betalinger)

§ 11 i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til et e-pengeinstitut eller et betalingsinstitut skal indeholde til brug for Finanstilsynets vurdering af, om kravene til at opnå en tilladelse hertil i henhold til § 10 i lov om betalinger er opfyldt.

Det fremgår af § 11, stk. 1, nr. 15, at en ansøgning som minimum skal indeholde virksomhedens beredskabsplan, herunder en klar beskrivelse af de kritiske funktioner, effektive beredskabsplaner og procedurer til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige.

§ 11, stk. 1, nr. 15, skal ses i sammenhæng med § 10, stk. 1, nr. 7, som stiller krav om, at virksomheden har forsvarlige og effektive organisatoriske strukturer, forretningsgange og procedurer.

I forbindelse med ansøgningen skal virksomheden som minimum indsende en kopi af virksomhedens beredskabsplan også kaldet "business continuity arrangements", jf. Folketingstidende 2016-2017, tillæg A, L 157 som fremsat, side 117.

Bestemmelsen gennemfører artikel 5, stk. 1, litra h, i 2. betalingstjenestedirektivet og artikel 3, stk. 1, i 2. e-pengedirektiv, jf. artikel 111, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5 også finder anvendelse på en ansøgning som e-pengeinstitut.

Det foreslås at nyaffatte *§ 11, stk. 1, nr. 15*, således, at en ansøgning som minimum skal indeholde virksomhedens beredskabsplan, herunder en klar beskrivelse af de kritiske funktioner, effektive politikker og planer for it-driftsstabilitet og planer for it-indsats- og genopretning og procedurer til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige og effektive i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra a, iii, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, som er et følgedirektiv til DORA, der ændrer i artikel 5, stk. 1, litra h, i 2. betalingstjenestedirektivet.

DORA-forordningen finder bl.a. anvendelse på betalingsinstitutter og e-pengeinstitutter, jf. artikel 2, stk. 1, litra b og d.

I forordningen er kritiske eller vigtige funktioner defineret som en funktion, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret, jf. artikel 3, nr. 22.

Forordningen indeholder bl.a. regler om indsats og genopretning, herunder indførelse af en politik for it-driftsstabilitet og gennemførelse af denne politik ved hjælp af planer, procedurer og mekanismer, der bl.a. tager sigte

på at sikre, at den finansielle enheds kritiske eller vigtige funktioner er stabile, jf. artikel 11, stk. 1 og 2. Desuden indeholder artikel 11, stk. 3, krav om, at de finansielle enheder gennemfører planer for it-indsats og genopretning. Artikel 11, stk. 6, litra a, indeholder krav om test af planer for it-driftsstabilitet og planer for it-indsats og genopretning.

Til nr. 6 (§ 11, stk. 1, nr. 17, 2. pkt., i lov om betalinger)

§ 11 i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til et e-pengeinstitut eller et betalingsinstitut skal indeholde til brug for Finanstilsynets vurdering af, om kravene til at opnå en tilladelse hertil i henhold til § 10 i lov om betalinger er opfyldt.

Det fremgår af § 11, stk. 1, nr. 17, 1. pkt., at en ansøgning som minimum skal indeholde virksomhedens sikkerhedspolitik, en detaljeret risikovurdering i tilknytning til de betalingstjenester, som virksomheden påtænker at udbyde, og en beskrivelse af de foranstaltninger, som virksomheden har foretaget for at imødegå de identificerede risici, herunder svig og misbrug af følsomme betalingsdata og personoplysninger. Videre fremgår det af 2. pkt., at beskrivelsen af foranstaltningerne skal indeholde oplysninger om, hvordan virksomheden sikrer et højt niveau af teknisk sikkerhed og databeskyttelse, herunder vedrørende de software- og it-systemer, der anvendes af ansøgeren eller de virksomheder, som ansøgeren outsourcer alle eller dele af sine aktiviteter til.

§ 11, stk. 1, nr. 17, 1. pkt., gennemfører artikel 5, stk. 1, litra j, i 2. betalingstjenestedirektiv, og 2. pkt. gennemfører artikel 5, stk. 1, tredje afsnit, i 2. betalingstjenestedirektiv. Bestemmelsen gennemfører også artikel 3, stk. 1, i 2. e-pengedirektiv, jf. artikel 111, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5 også finder anvendelse på en ansøgning som e-pengeinstitut.

Det foreslås af nyaffatte *§ 11, stk. 1, nr. 17, 2. pkt.*, således, at beskrivelsen af de foranstaltninger, som virksomheden har foretaget for at imødegå de identificerede risici, herunder svig og misbrug af følsomme betalingsdata og personoplysninger, jf. 1. pkt., skal indeholde oplysninger om, hvordan virksomheden sikrer et højt niveau af digital operationel modstandsdygtighed i overensstemmelse med kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, navnlig med hensyn til teknisk sikkerhed og databeskyttelse, herunder vedrørende de software- og it-systemer, der anvendes af ansøgeren eller de

virksomheder, som ansøgeren outsourcer alle eller dele af sine aktiviteter til.

§ 11, stk. 1, nr. 17, skal ses i sammenhæng med § 10, stk. 1, nr. 7, som stiller krav om, at virksomheden har forsvarlige og effektive organisatoriske strukturer, forretningsgange og procedurer.

Virksomheden skal have betryggende kontrol- og sikringsforanstaltninger på it-området, jf. § 25, stk. 1, nr. 8, i lov om betalinger. Disse skal tage udgangspunkt i beskrivelsen af virksomhedens it-anvendelse, samt hvilke iboende risici virksomheden har på it-området. Dokumenterne omtalt i nr. 17, skal gøre Finanstilsynet i stand til at vurdere om virksomheden lever op til dette krav. Yderligere kræves det at outsourcing af væsentlige driftsmæssige funktioner kun må ske under visse betingelser, jf. §§ 39-41. Virksomheden skal ved outsourcing af væsentlige driftsmæssige funktioner sikre sig, at outsourcing ikke indebærer en væsentlig forringelse af kvaliteten af betalingsinstituttets interne kontrol og ledelsesrapportering eller Finanstilsynets mulighed for at overvåge, om instituttet overholder lov om betalingstjenester og elektroniske penge. Betalingsinstitutter og e-pengeinstitutter skal ifølge lovforslagets §§ 122 og 124, udarbejde og indføre en række foranstaltninger og kontrolmekanismer med henblik på at imødegå operationelle og sikkerhedsmæssige risici, der er forbundet med de betalingstjenester der udbydes. § 11, stk. 1, nr. 17, skal således ses i sammenhæng med §§ 122 og 124, og den dokumentation en virksomhed, der søger om tilladelse som betalings eller e-pengeinstitut, skal vedlægge skal gøre det muligt for Finanstilsynet at sikre, at virksomheden lever op til kravene i lovforslagets §§ 122 og 124, jf. Folketingstidende 2016-2017, tillæg A, L 157 som fremsat, side 118.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra b, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, som er et følgedirektiv til DORA, der ændrer i artikel 5, stk. 1, 3. afsnit, i 2. betalingstjenestedirektivet.

Med nyaffattelsen indsættes der en henvisning til kapitel II i DORA-forordningen i forhold til at sikre et højt niveau af digital operationel modstandsdygtighed.

Digital operationel modstandsdygtighed er i artikel 3, nr. 1, i DORA-forordningen defineret ved en finansiel enheds evne til at opbygge, sikre og gennemgå sin operationelle integritet og pålidelighed ved enten direkte eller indirekte gennem anvendelse af tjenester, der leveres af en tredjepartsudbyder af it-tjenester, at sikre det fulde spektrum af nødvendige it-relaterede kapaciteter med henblik på at varetage sikkerheden i de net- og

informationssystemer, som en finansiel enhed anvender, og som understøtter det løbende udbud af finansielle tjenesteydelser og kvaliteten heraf, herunder i forbindelse med forstyrrelser

Kapitel II i DORA-forordningen vedrører it-risikostyring. Artikel 5, stk. 1, fastsætter bl.a. krav om, at finansielle enheder, herunder e-pengeinstitutter og betalingsinstitutter, skal have indført en intern forvaltnings- og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko for at opnå et højt niveau af digital operationel modstandsdygtighed. Videre fremgår det bl.a. også af artikel 6, stk. 1, at finansielle enheder, skal indføre en robust, omfattende og veldokumenteret ramme for it-risikostyring som en del af deres samlede risikostyringssystem, der sætter dem i stand til at håndtere it-risikoen hurtigt, effektivt og fyldestgørende, og som sikrer et højt niveau af digital operationel modstandsdygtighed.

Til nr. 7 (§ 54, nr. 8, litra c, i lov om betalinger)

§ 54 i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om begrænset tilladelse til at udbyde betalingstjenester betalingsinstitut eller udstede elektroniske penge skal indeholde til brug for Finanstilsynets vurdering af, om kravene til at opnå en tilladelse hertil i henhold til § 52 i lov om betalinger er opfyldt.

Det fremgår af § 54, nr. 8, litra c, at en ansøgning som minimum skal indeholde oplysninger om virksomhedens forretningsgange og interne kontrolmekanismer, herunder administrative, risikostyringsmæssige s regnskabsmæssige procedurer, der omfatter virksomhedens forretningsgange for håndtering af og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder for indberetning af sikkerhedshændelser, jf. §§ 126 og 127.

§ 127 i lov om betalinger fastsætter regler om, at en udbyder af betalingstjenester skal underrette Finanstilsynet om større drifts- og sikkerhedshændelser. § 127, stk. 1 og 2, bliver ophævet med § 3, nr. 12, i nærværende lovforslag.

Kravet i § 54, nr. 8, litra c, svarer til kravet i § 11, stk. 1, nr. 12, 1. pkt., i lov om betalinger om, at en ansøgning om tilladelse som betalingsinstitut eller e-pengeinstitut som minimum skal indeholdevirksomhedens forretningsgange for håndtering og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder procedurer for indberetning af sikkerhedshændelser, jf. § 127.

§ 11, stk. 1, nr. 12, gennemfører artikel 5, stk. 1, litra f, i 2. betalingstjenestedirektiv. Bestemmelsen gennemfører også artikel 3, stk. 1, i 2. e-pengedirektiv, jf. artikel 111, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5 også finder anvendelse på en ansøgning som e-pengeinstitut.

Artikel 7, nr. 2, litra a, ii, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, ændrer i artikel 5, stk. 1, litra f, i 2. betalingstjenestedirektivet og dermed også en ændring af § 11, stk. 1, nr. 12, jf. de specielle bemærkninger til § 3, nr. 4, i nærværende lovforslag.

Det foreslås, at *§ 54, nr. 8, litra c,* ændres således, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange for håndtering af og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder for indberetning af sikkerhedshændelser, jf. § 126 og kapitel III i DORA-forordningen. Med ændringen udgår henvisningen til § 127 af bestemmelsen.

Med ændringen udgår § 127 af bestemmelsen, og der indsættes i stedet en henvisning til kapitel III i DORA-forordningen. Da kapitel III i DORA-forordningen også finder anvendelse på betalingsinstitutter og e-pengeinstitutter med begrænset tilladelse, jf. artikel 2, stk. 1, litra b og d, i forordningen, findes det hensigtsmæssigt også at ændre i § 54, stk. 1, nr. 8, litra c.

Kapitel III i DORA-forordningen indeholder regler om styring, klassificering og indberetning af it-relaterede hændelser. It-relaterede hændelser er defineret som hændelser, der kompromitterer sikkerheden i net- og informationssystemerne og har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de tjenester, som den finansielle enhed leverer, jf. artikel 3, nr. 8, i DORA-forordningen.

Til nr. 8 (§ 60, stk. 3, nr. 5, i lov om betalinger)

§ 60, stk. 3, i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til udbyder af kontooplysningstjenester skal indeholde, for at Finanstilsynet kan vurdere, om kravene til at opnå en tilladelse hertil i henhold til § 60, stk. 2, er opfyldt.

Det fremgår af § 60, stk. 3, nr. 5, at en ansøgning som minimum skal indeholde oplysninger om virksomhedens forretningsgange og interne

kontrolmekanismer, herunder administrative, risikostyringsmæssige og regnskabsmæssige procedurer.

Bestemmelsen gennemfører artikel 33, stk. 1, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5, stk. 1, litra e, også finder anvendelse på udbydere af kontooplysningstjenester.

Det foreslås i *§ 60, stk. 3, nr. 5,* at ændre bestemmelsen således, at det fremgår, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange og interne kontrolmekanismer, herunder administrative, risikostyringsmæssige og regnskabsmæssige procedurer samt ordninger for brug af it-tjenester i overensstemmelse med DORA-forordningen.

Forordningen finder bl.a. anvendelse på udbydere af kontooplysningstjenester, jf. artikel 2, stk. 1, litra c.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra a, i, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der ændrer i artikel 5, stk. 1, litra e, i 2. betalingstjenestedirektivet.

Der henvises i øvrigt til lovforslagets § 2, nr. 4, og bemærkningerne hertil.

Til nr. 9 (§ 60, stk. 3, nr. 6, i lov om betalinger)

§ 60, stk. 3, i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til udbyder af kontooplysningstjenester skal indeholde, for at Finanstilsynet kan vurdere, om kravene til at opnå en tilladelse hertil i henhold til § 60, stk. 2, er opfyldt.

Det fremgår af § 60, stk. 3, nr. 6, at en ansøgning som minimum skal indeholde oplysninger om virksomhedens forretningsgange for håndtering af og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder procedurer for indberetning af sikkerhedshændelser, jf. § 126, i lov om betalinger.

§ 126 fastsættes en række forpligtelser med hensyn til håndtering af operationelle og sikkerhedsmæssige risici for en udbyder af betalingstjenester.

Bestemmelsen gennemfører artikel 33, stk. 1, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel

5, stk. 1, litra f, også finder anvendelse på udbydere af kontooplysningstjenester.

Det foreslås at ændre *§ 60, stk. 3, nr. 6*, således, at en ansøgning som minimum skal indeholde virksomhedens forretningsgange for håndtering og opfølgning på sikkerhedshændelser og sikkerhedsrelaterede kundeklager, herunder procedurer for indberetning af sikkerhedshændelser, jf. kapitel III i DORA-forordningen.

Kapitel III i DORA-forordningen indeholder regler om styring, klassificering og indberetning af it-relaterede hændelser. It-relaterede hændelser er defineret som hændelser, der kompromitterer sikkerheden i net- og informationssystemerne og har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de tjenester, som den finansielle enhed leverer, jf. artikel 3, nr. 8, i DORA-forordningen.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra a, ii, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der ændrer i artikel 5, stk. 1, litra f, i 2. betalingstjenestedirektivet.

Der henvises i øvrigt til lovforslagets § 2, nr. 4, og bemærkningerne hertil.

Til nr. 10 (§ 60, stk. 3, nr. 8, i lov om betalinger)

§ 60, stk. 3, i lov om betalinger indeholder regler om de oplysninger, som en ansøgning om tilladelse til udbyder af kontooplysningstjenester skal indeholde, for at Finanstilsynet kan vurdere, om kravene til at opnå en tilladelse hertil i henhold til § 60, stk. 2, er opfyldt.

Det følger af stk. 3, nr. 8, at en ansøgning som minimum skal indeholde en beskrivelse af virksomhedens beredskabsplan, herunder en klar beskrivelse af de kritiske funktioner, effektive beredskabsplaner og procedurer til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige.

Formålet med bestemmelsen er at sikre, at virksomheden har tilstrækkelige beredskabsplaner eksempelvis i tilfælde af kritiske nedbrud af kritiske it-funktioner. Virksomheden skal jævnligt udføre test af beredskabsplanen, jf. Folketingstidende 2016-2017, tillæg A, L 157 som fremsat, side 182.

Bestemmelsen gennemfører artikel 33, stk. 1, i 2. betalingstjenestedirektiv, hvorefter kravene til en ansøgning som betalingsinstitut i medfør af artikel 5, stk. 1, litra h, også finder anvendelse på udbydere af kontooplysningstjenester.

Det foreslås at nyaffatte *§ 60, stk. 3, nr. 8,* således, at en ansøgning som minimum skal indeholde virksomhedens beredskabsplan, herunder en klar beskrivelse af de kritiske funktioner, effektive politikker og planer for it-driftsstabilitet og planer for it-indsats- og genopretning og procedurer til regelmæssigt at teste og evaluere, om sådanne planer er tilstrækkelige og effektive i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring gennemfører artikel 7, nr. 2, litra a, iii, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, som er et følgedirektiv til DORA, der ændrer i artikel 5, stk. 1, litra h, i 2. betalingstjenestedirektivet.

DORA-forordningen finder bl.a. anvendelse på udbydere af kontooplysningstjenester, jf. artikel 2, stk. 1, litra c.

I forordningen er kritiske eller vigtige funktioner defineret som en funktion, hvis forstyrrelse i væsentlig grad kan forringe en finansiel enheds finansielle resultater, eller robustheden eller kontinuiteten af dens tjenester og aktiviteter, eller som, hvis den pågældende funktion afbrydes, er fejlbehæftet eller mislykkes, i væsentlig grad kan forringe en finansiel enheds opfyldelse af de betingelser og forpligtelser, der er forbundet med dens tilladelse, eller af dens andre forpligtelser i henhold til gældende finansiel tjenesteydelsesret, jf. artikel 3, nr. 22.

Forordningen indeholder bl.a. regler om indsats og genopretning, herunder indførelse af en politik for it-driftsstabilitet og gennemførelse af denne politik ved hjælp af planer, procedurer og mekanismer, der bl.a. tager sigte på at sikre, at den finansielle enheds kritiske eller vigtige funktioner er stabile, jf. artikel 11, stk. 1 og 2. Desuden indeholder artikel 11, stk. 3, krav om, at de finansielle enheder gennemfører planer for it-indsats og genopretning. Artikel 11, stk. 6, litra a, indeholder krav om test af planer for it-driftsstabilitet og planer for it-indsats og genopretning.

Der henvises i øvrigt til lovforslagets § 3, nr. 5, og bemærkningerne hertil.

Til nr. 11 (§ 126 stk. 2, i lov om betalinger)

Det fremgår af § 126, stk. 1, nr. 1 og 2, at en udbyder af betalingstjenester skal fastlægge og opretholde procedurer og kontrolmekanismer til styring af drifts- og sikkerhedsrisici, der er forbundet med de betalingstjenester, som

de udbyder og have effektive procedurer for håndtering af drifts- og sikkerhedshændelser.

Bestemmelsen gennemfører artikel 95, stk. 1, i 2. betalingstjenestedirektiv.

Det foreslås i *§ 126* at indsætte et nyt *stk. 2,* hvoraf det fremgår, at stk. 1, nr. 1 og 2, ikke berører anvendelsen af kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Bestemmelsen gennemfører artikel 7, stk. nr. 4, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, som er et følgedirektiv til DORA, hvoraf det fremgår, at artikel 95, stk. 1, ikke berører anvendelsen af kapitel II i DORA-forordningen for så vidt betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester.

Kapitel II i DORA-forordningen fastsætter bl.a. krav om, at finansielle enheder, herunder betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester, skal have interne forvaltnings- og kontrolrammer til at sikre en effektiv og forsigtig styring af risiciene.

Til nr. 12 og 13 (§ 127, stk. 1, 2 og 4, i lov om betalinger)

Det fremgår af § 127, stk. 1, at en udbyder af betalingstjenester snarest muligt skal underrette Finanstilsynet om større drifts- og sikkerhedshændelser. Finanstilsynet skal uden unødig forsinkelse vurdere underretningen og videregive oplysninger, der er relevante, til ECB, EBA og relevante tilsynsmyndigheder i de lande, der er berørt af hændelsen. Videre fremgår det af stk. 2, at i den situation, hvor hændelsen har eller kan få indvirkning på brugerne af betalingstjenestens økonomiske interesser, skal udbyderen snarest muligt orientere brugerne om denne og om de tilgængelige foranstaltninger, som de kan træffe for at begrænse hændelsens negative følger. Til sidst fremgår det af § 127, stk. 4, at Finanstilsynet fastsætter nærmere regler om den tekniske gennemførelse af indberetningspligten i henhold til bl.a. stk. 1 og 2.

Bestemmelsen gennemfører artikel 96, stk. 1, og artikel 96, stk. 2, 1. afsnit, i 2. betalingstjenestedirektiv om indberetning af hændelser.

Det fremgår af § 127, stk. 4, at Finanstilsynet fastsætter nærmere regler om den tekniske gennemførelse af indberetningspligten i henhold til stk. 1-3.

Det foreslås, at *§ 127, stk. 1* og *2*, ophæves.

Det foreslås i *§ 127, stk. 4*, der bliver stk. 2, at ændre »stk. 1-3« til: »stk. 1«.

Det foreslåede medfører, at Finanstilsynet ikke længere skal kunne fastsætte nærmere regler om indberetningspligten i henhold til stk. 1 og 2, men derimod kun i henhold til stk. 3, der bliver til stk. 1. Ændringen bevirker, at Finanstilsynet herefter kun kan fastsætte nærmere regler om, hvordan udbydere en gang årligt skal indrapportere statistik om drift og misbrug af de betalingstjenester, som denne udbyder, til Finanstilsynet

Bestemmelsen gennemfører artikel 7, nr. 5, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, som er et følgedirektiv til DORA, hvorefter bl.a. artikel 96, stk. 1, og artikel 96, stk. 2, 1. afsnit, i 2. betalingstjenestedirektivet ikke længere skal finde anvendelse på betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester.

DORA-forordningen, der bl.a. finder anvendelse på betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester, jf. artikel 2, stk. 1, litra b, c og d, indeholder i artikel 19, stk. 1, krav om indberetning af større it-relaterede hændelser til de kompetente myndigheder, dvs. Finanstilsynet. Når Finanstilsynet modtager en underretning om en større it-hændelse, skal Finanstilsynet rettidigt forelægge nærmere oplysninger om hændelsen for andre myndigheder, for hvem hændelsen er relevant, jf. artikel 19, stk. 6, i DORA-forordningen. Artikel 19, stk. 6, nævner de myndigheder, som Finanstilsynet kan forelægge en hændelse for, herunder CSIRT, dvs. Center for Cybersikkerhed.

Til nr. 14 (§ 130, stk. 1, 2. pkt., i lov om betalinger)

Det gældende § 130, stk. 1, 1. og 2. pkt., i lov om betalinger fastlægger Finanstilsynets generelle beføjelse til at påse overholdelsen af loven, regler udstedt i medfør heraf samt overholdelsen af nærmere angivne forordninger.

Det foreslås, at der i *§ 130, stk. 1, 2. pkt.*, indsættes en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022

om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.

Forordningen finder bl.a. anvendelse på betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester, jf. artikel 2, stk. 1, litra b, c og d. Formålet med den foreslåede bestemmelse er, at Finanstilsynet bliver udpeget som kompetent myndighed efter forordningen til at føre tilsyn med overholdelsen af forordningen.

Med den foreslåede ændring vil Finanstilsynet desuden kunne påse overholdelsen af de forordninger, som Kommissionen har hjemmel til at udstede i medfør af DORA-forordningen.

Efter artikel 46, litra b, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af 2. betalingstjenestedirektiv, sikre overholdelsen af DORA-forordningen for betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester.

Den foreslåede ændring vil medføre, at Finanstilsynet bl.a. vil kunne udstede påbud og påtaler for overtrædelser af DORA-forordningen.

Bestemmelsen supplerer artikel 46, litra b, i DORA-forordningen.

Til nr. 15 (§ 130, stk. 1, 3. pkt., i lov om betalinger)

Det gældende § 130, stk. 1, i lov om betalinger fastlægger Finanstilsynets generelle beføjelse til at påse overholdelsen af loven, regler udstedt i medfør heraf samt overholdelsen af nærmere angivne forordninger.

Det foreslås at der i *§ 130, stk. 1*, indsættes et *3.pkt.*, hvorefter Finanstilsynet påser udstedere af e-pengetokens overholdelse af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf.

Den foreslåede bestemmelse vil indebære, at Finanstilsynet vil have beføjelse til at påse overholdelsen af MiCA, herunder give påbud og påtaler og evt. politianmelde for overtrædelse heraf.

Med den foreslåede bestemmelse vil Finanstilsynet blive udpeget i henhold til artikel 93, stk. 1, i MiCA, som den kompetente myndighed, der er

ansvarlig for at udføre de i MiCA fastsatte funktioner og opgaver, herunder til at påse udstedere af e-pengetokens overholdelse af MiCA.

Kommissionen er i medfør af MiCA bemyndiget til at udstede reguleringsmæssige tekniske standarder, som Finanstilsynet i medfør af den foreslåede bestemmelse også skal føre tilsyn med.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udstedere af e-pengetokens vil være underlagt Finanstilsynets tilsyn i henhold til MiCA.

Til nr. 16 (§ 135, stk. 1, nr. 7, i lov om betalinger)

Det gældende § 135, stk. 1, nr. 7, i lov om betalinger fastsætter, at Finanstilsynet kan inddrage en virksomheds tilladelse som e-pengeinstitut eller betalingsinstitut eller en begrænset tilladelse til udstedelse af elektroniske penge eller udbud af betalingstjenester, hvis virksomheden gør sig skyldig i grove eller gentagne overtrædelser af hvidvaskloven.

Det foreslås i *§ 135, stk. 1, nr. 7,* efter »af hvidvaskloven« at indsætte »eller Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.«

Det foreslåede vil medføre, at Finanstilsynet kan inddrage en virksomheds tilladelse som e-pengeinstitut, hvis virksomheden gør sig skyldig i grove eller gentagne overtrædelser af MiCA.

Der forudsættes en høj grad af væsentlighed, hvis inddragelse af tilladelse skal finde sted med henvisning hertil. Vurderingen skal foretages på baggrund af overtrædelsens grovhed og de risici, det medfører for forbrugere, samfundet og den finansielle stabilitet. Der må tages hensyn til overtrædelsens karakter, omfang, tidsmæssige aspekt osv. En afgørelse om inddragelse af en virksomheds tilladelse er af indgribende karakter for virksomheden. Medmindre forholdet er af meget væsentlig karakter, eller inddragelsen sker efter anmodning fra virksomheden, forudsættes det derfor, at inddragelse af tilladelse typisk kun bliver aktuel, efter der har været givet frist til berigtigelse af forholdet, og at berigtigelse ikke er sket.

Til nr. 17 (§ 136, stk. 6, nr. 27, i lov om betalinger)

Det fremgår af § 136, stk. 1, i lov om betalinger, at Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e bl.a. er forpligtet til at hemmeligholde fortrolige oplysninger, som de får kendskab til gennem tilsynsvirksomheden.

§ 136, stk. 6, er en undtagelse til tavshedspligten i § 136, stk. 1. Bestemmelsen fastsætter til hvem og i hvilke tilfælde, Finanstilsynet kan videregive fortrolige oplysninger, uanset § 136, stk. 1.

I medfør af § 136, stk. 1, har Finanstilsynet ikke mulighed for at videregive oplysninger til Center for Cybersikkerhed, Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 136, stk. 6,* at indsætte *nr. 27,* hvorefter Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til Center for Cybersikkerhed, SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større it-relateret hændelse fra et betalingsinstitut, et e-pengeinstitut, en udbyder af kontooplysningstjenester eller en virksomhed med begrænset tilladelse til enten at udstede elektroniske penge eller udbyde betalingstjenester, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. de centrale kontaktpunkter eller CSIRT'er, der er udpeget eller oprettet i overensstemmelse med NIS 2-direktivet, dvs. Center for Cybersikkerhed. Bestemmelsen nævner også SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 18 (§ 136, stk. 6, i lov om betalinger)

[udestår]

Til nr. 19 (§ 138, stk. 1, 8. pkt., i lov om betalinger)

Det følger af § 138, stk. 1, 8. pkt., at reaktioner givet af Finanstilsynets bestyrelse i henhold til lovens § 130, stk. 2, jf. § 345, stk. 12, nr. 6, i lov om finansiel virksomhed, dvs. beslutninger om at overgive sager af principiel karakter, og sager der har videregående betydelige følger til politimæssig efterforskning, og Finanstilsynets beslutninger om at overgive sager efter denne lov eller regler udstedt i medfør af loven eller efter forordninger udstedt i medfør af Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked, artikel 3-4 i Europa-Parlamentets og Rådets forordning 924/2009/EF af 16. september 2009 om grænseoverskridende betalinger i Fællesskabet og Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro til politimæssig efterforskning skal offentliggøres på Finanstilsynets hjemmeside med angivelse af virksomhedens navn, jf. dog stk. 3.

Det foreslås i *§ 138, stk. 1, 8. pkt.,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) og forordninger udstedt i medfør heraf.

Med ændringen vil Finanstilsynet også skulle offentliggøre beslutninger truffet af bestyrelsen eller af Finanstilsynet efter delegation fra bestyrelsen

om at overgive sager om overtrædelse af bestemmelser i DORA-forordningen, som er strafbelagte til politimæssig efterforskning. Der henvises i det hele til bemærkningerne til § 138 tidligere § 137, jf. Folketingstidende 2016-2017, tillæg A, L 157 som fremsat, side 298-303.

Der henvises i øvrigt til § 2, nr. 25, i lovforslaget, der nævner de bestemmelser i forordningen, der er strafbelagte.

Til nr. 20 (§ 138, stk. 1, 10. pkt., i lov om betalinger)

§ 138, stk. 1, 1. pkt., i lov om betalinger fastsætter regler om offentliggørelse af reaktioner, som Finanstilsynets bestyrelse har truffet beslutning om, eller som Finanstilsynet har givet efter delegation fra Finanstilsynets bestyrelse. Bestemmelsen regulerer ikke det tilfælde, hvor det alene er Finanstilsynet, der har truffet en afgørelse om at give en reaktion til en virksomhed omfattet af loven.

I medfør af § 138, stk. 1, 2. pkt., skal en virksomhed, der har modtaget en reaktion, offentliggøre oplysningerne herom på sin eventuelle hjemmeside på et sted, hvor de naturligt hører hjemme. Finanstilsynet skal også offentliggøre reaktionen på Finanstilsynets hjemmeside i medfør af § 138, stk. 1, 7. pkt.

Videre fremgår det af § 138, stk. 1, 9. pkt., at indbringes en reaktion, der offentliggøres i henhold til 1. pkt., for Erhvervsankenævnet eller domstolene, skal dette fremgå af Finanstilsynets offentliggørelse, og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Det foreslås i *§ 138, stk. 1,* at indsætte et 9. pkt., hvoraf fremgår, at reaktioner givet i henhold til DORA-forordningen skal offentliggøres på Finanstilsynets hjemmeside.

Med den foreslåede ændring vil Finanstilsynet skulle offentliggøre reaktioner, der er givet af Finanstilsynet til en virksomhed for en overtrædelse af DORA-forordningen. Ved reaktioner forstås f.eks. påbud eller påtaler. Reaktionen skal offentliggøres på Finanstilsynets hjemmeside. Derimod er virksomheden ikke selv forpligtet til at offentliggøre reaktionen. Virksomheden vil kun være forpligtet til at offentliggøre reaktionen, hvis bestyrelsen har truffet beslutning herom i henhold til DORA-forordningen, jf. § 138, stk. 1, 2. pkt.

Desuden foreslås det i *§ 138, stk. 1., 9. pkt.,* der bliver 10. pkt., at indsætte en henvisning til 9. pkt., hvorefter det skal fremgå af Finanstilsynets

offentliggørelse, at en reaktion, der offentliggøres i henhold til enten stk. 1, 1. pkt., eller 9. pkt., indbringes for Erhvervsankenævnet eller domstolene, og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Den foreslåede ændring gennemfører artikel 54, stk. 1, i DORA-forordningen, hvormed de kompetente myndigheder uden unødigt ophold på deres officielle websteder skal offentliggøre enhver afgørelse om pålæggelse af en administrativ sanktion, som ikke kan påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen. En administrativ sanktion kan bl.a. kan være et påbud eller en påtale.

Det fremgår dog videre af artikel 54, stk. 5, i DORA-forordningen, at hvis den kompetente myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

Artikel 54, stk. 1 og 5, svarer derfor til kravet om offentliggørelse af reaktioner i henhold til DORA-forordningen og den efterfølgende offentliggørelse af indbringelse af en reaktion til enten Erhvervsankenævnet eller domstolene i henhold til ovennævnte forslag i § 138, stk. 1, 9. og 10. pkt.

For nærmere om § 138 og offentliggørelse henvises der i det hele til de specielle bemærkningerne til § 138 tidligere § 137, jf. Folketingstidende 2016-2017, tillæg A, L 157 som fremsat, side 298-303.

Til nr. 21 (§ 142, stk. 1, i lov om betalinger)

Det følger af § 142, stk. 1, at som part i forhold til Finanstilsynet anses virksomheder eller personer, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af denne lov eller regler udstedt i medfør af denne lov, jf. dog stk. 2.

Det foreslås i *§ 142, stk. 1*, at indsætte en henvisning til forordninger udstedt i medfør af Europa-Parlamentets og Rådets direktiv 2015/2366/EU af 25. november 2015 om betalingstjenester i det indre marked, artikel 3-4 i Europa-Parlamentets og Rådets forordning 924/2009/EF af 16. september 2009 om grænseoverskridende betalinger i Fællesskabet og om ophævelse

af forordning (EF) nr. 2560/2001, Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro og Europa-Parlamentets, Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og forordninger udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning nr. 2023/1114 (EU) om markeder for kryptoaktiver og regler udstedt i medfør heraf.«.

Det foreslåede medfører, at virksomheder eller personer, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af forordninger udstedt i medfør af 2. betalingstjenestedirektiv, artikel 3-4 i Europa-Parlamentets og Rådets forordning 924/2009/EF af 16. september 2009 om grænseoverskridende betalinger i Fællesskabet og om ophævelse af forordning (EF) nr. 2560/2001, Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro, DORA-forordningen eller forordninger udstedt i medfør heraf samt MiCA og regler udstedt i medfør heraf, også vil være at anse som parter i afgørelsessager.

Til nr. 22 (§ 143 i lov om betalinger)

Den gældende § 143 i lov om betalinger, indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet retter sig mod. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet i henhold til lov om betalinger og en række EU-retsakter på det finansielle område.

Det foreslås i *§ 143* at indsætte efter »udstedt i medfør heraf«: »Europa-Parlamentets og Rådets forordning (EU) nr. 260/2012 af 14. marts 2012 om tekniske og forretningsmæssige krav til kreditoverførsler og direkte debiteringer i euro og Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.«

Det foreslåede vil medføre, at afgørelser truffet af Finanstilsynet i medfør af DORA-forordningen og MiCA kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, som afgørelsen retter sig til.

Til nr. 23 (§ 144, stk. 1, 3. pkt., i lov om betalinger)

Det gældende § 144, stk. 1, i lov om betalinger fastsætter, hvilke bestemmelser i loven Forbrugerombudsmanden fører tilsyn med, samt hvilke beføjelser Forbrugerombudsmanden har i denne forbindelse.

Det foreslås i *§ 144, stk. 1,* at indsætte et *3. pkt.,* hvorefter Forbrugerombudsmanden også fører også tilsyn med, at virksomheder overfor forbrugere overholder artikel 49, 53 og 55 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslåede vil medføre, at Forbrugerombudsmanden kan påse, at udstedere af e-pengetokens overfor forbrugere overholder artikel 49, 53 og 55 i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det omfatter bestemmelser om genindløsning af e-pengetokens, markedsføringskommunikation samt genindløsningsplaner for udstedere af e-pengetokens.

Det foreslåede viderefører den hidtidige kompetencefordeling mellem Finanstilsynet og Forbrugerombudsmanden, og sikrer, at Forbrugerombudsmanden får kompetencer til at påse overholdelsen af de forbrugerbeskyttende regler i forbindelse med udstedelse af e-penge i form af e-pengetokens omfattet af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver. Finanstilsynet fører tilsyn med bestemmelserne, når forholdet omkring udstedelse af e-pengetokens er mellem erhvervsdrivende.

Det foreslåede vil medføre, at Forbrugerombudsmanden udpeges som den kompetente myndighed i henhold til artikel 93, stk. 1, i MiCA, hvorefter Forbrugerombudsmanden er ansvarlig for at udføre de i MiCA fastsatte funktioner og opgaver for så vidt angår artikel 49, 53 og 55, når e-pengeinstitutter udsteder e-pengetokens til forbrugere.

Da markedsføringsloven supplerer anden lovgivning, kan Forbrugerombudsmanden som led i sit tilsyn anvende markedsføringsloven, medmindre andet følger af lovgivningen.

Forbrugerombudsmandens tilsyn udøves i øvrigt efter reglerne i markedsføringsloven, herunder bekendtgørelse nr. 1249 af 25. november 2014 om regler for Forbrugerombudsmandens virksomhed. Det fremgår bl.a. af bekendtgørelsen, at Forbrugerombudsmanden ikke er forpligtet til at

behandle klager vedrørende de i stk. 1 nævnte regler, men har adgang til at prioritere, hvilke klager Forbrugerombudsmanden vil behandle.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udstedere af e-pengetokens vil være underlagt Forbrugerombudsmandens tilsyn i henhold til artikel 49, 53 og 55 i MiCA for så vidt angår udstedelse af e-pengetokens til forbrugere.

Til nr. 24 (§ 152, stk. 1, i lov om betalinger)

Den gældende § 152, stk. 1, i lov om betalinger bestemmer, at en række overtrædelser af lov om betalinger kan straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås i *§ 152, stk. 1,* efter »og § 60, stk. 1« at indsætte: » i denne lov og artikel 48, stk. 1, artikel 49, stk. 4, artikel 50, stk. 1 og 2, artikel 54, artikel 59, stk. 1, artikel 60, stk. 4, artikel 67, stk. 4, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

Det foreslåede vil medføre, at overtrædelse af de nævnte artikler i MiCA kan straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Artikel 48, stk. 1, i MiCA fastsætter krav til personer, der udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel. Ansvarssubjektet for overtrædelse af bestemmelsen er et e-pengeinstitut, der udbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU. Ansvarssubjektet kan endvidere være andre personer, der efter skriftligt samtykke fra e-pengeinstituttet udbyder eller anmoder om optagelse til handel af e-pengetokens, Den strafbare handling består eksempelvis i, at et e-pengeinstitutudbyder e-pengetokens til offentligheden eller anmoder om optagelse af e-pengetokens til handel i EU, uden at e-pengeinstituttet er udstederen af disse e-pengetokens.

Artikel 49, stk. 4, i MiCA omhandler kravene til at genindløse e-pengetokens til kurs pari. Ansvarssubjektet for overtrædelse af bestemmelsen er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et e-pengeinstitut, der udsteder e-pengetokens, opkræver et gebyr eller anden betaling for at indløse indehaveres e-pengetokens.

Artikel 50, stk. 1 og 2, i MiCA omhandler forbud mod rentetilskrivning. Ansvarssubjekterne for overtrædelse af bestemmelserne er et e-pengeinstitut, der udsteder e-pengetokens, og udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at et e-pengeinstitut, der udsteder e-pengetokens, overfører e-pengetokens eller andre kryptoaktiver til holdere af udstederens e-pengetokens som vederlag for den tid, i hvilken en indehaver af e-pengetokens besidder sådanne. Den strafbare handling kan endvidere bestå i, at udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder, tilbyder disse kunder renter eller andet vederlag.

Artikel 54 i MiCA fastsætter krav vedrørende investering af pengemidler modtaget som betaling for e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelsen er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et e-pengeinstitut, der udsteder e-pengetokens, investerer alle de modtagne midler i sikre aktiver med lav risiko og dermed undlader at indsætte mindst 30% af de modtagne pengemidler på en særskilt konto i et pengeinstitut.

Artikel 59, stk. 1, i MiCA omhandler tilladelseskrav til at udbyde kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver fysisk eller juridisk person, der udbyder kryptoaktivtjenester, uden den nødvendige tilladelse. Den strafbare handling består i at udbyde kryptoaktivtjenester uden enten at være meddelt tilladelse efter artikel 63 eller uden at have tilladelse til at levere kryptoaktivtjenester efter artikel 60 i MiCA.

Artikel 60, stk. 4, i MiCA fastsætter krav om underretning af Finanstilsynet førend e-pengeinstitutter kan udbyde deponering og administration af kryptoaktiver på kunders vegne og overførsler af kryptoaktiver på kunders vegne, med hensyn til de e-pengetokens, de udsteder. Ansvarssubjektet for overtrædelsen af bestemmelserne er e-pengeinstitutter. Den strafbare handling består eksempelvis i, at et e-pengeinstitut påbegynder levering af de benævnte kryptoaktivtjenester uden at have underrettet Finanstilsynet med de oplysninger, der er anført i artikel 60, stk. 7, i MiCA, mindst 40 arbejdsdage inden e-pengeinstituttet leverer disse tjenester første gang.

Artikel 70, stk. 1-4, i MiCA omhandler krav vedrørende opbevaring af kundernes kryptoaktiver og midler. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester, der opbevarer kryptoaktiver på vegne af deres kunder, ikke træffer passende

foranstaltninger til at forhindre, at kundernes kryptoaktiver anvendes til handel for deres egen regning.

Artikel 72, stk. 1, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er udbydere af kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktivtjenester ikke opretholder og anvender effektive politikker til at identificere mellem dem selv og personerne opregnet i artikel 72, stk. 1, litra a-e.

Artikel 75, stk. 1, 2 og 7, i MiCA indebærer specifikke krav til udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er udbydere af kryptoaktivtjenester, som udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at udbydere, der leverer deponering og administration af kryptoaktiver på vegne af kunder, ikke holder deres kunders kryptoaktiver adskilt fra udbydernes egne kryptoaktiver.

Den foreslåede ændring supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter udstedere af e-pengetokens og udbydere af kryptoaktivtjenester skal efterleve en række krav i forordningen.

Til nr. 25 (§ 152, stk. 2, i lov om betalinger)

Det gældende § 152, stk. 2, i lov om betalinger fastsætter, hvilke overtrædelser af lov om betalinger, der kan straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås i *§ 152, stk. 2,* efter: »(SEPA-forordningen)« at indsætte: », artikel 46, stk. 1 og 2, artikel 47, stk. 1-3, artikel 48, stk. 6 og 7, artikel 49, stk. 5, artikel 51, stk. 1-9, 11-13 og stk. 14, 1. pkt., artikel 53, stk. 1-3, 5 og 6, artikel 55, artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9 og artikel 82, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30,

stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.«.

Det foreslåede vil medføre, at overtrædelse af de oplistede artikler i MiCA og DORA-forordningen straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

I det følgende redegøres for de nævnte artikler i MiCA.

Artikel 46, stk. 1 og 2, i MiCA omhandler krav til udstedere af aktivbaserede tokens om at udarbejde og opretholde en genopretningsplan, samt underrette Finanstilsynet om genopretningsplanen. Det fremgår i artikel 55 i MiCA, at tilsvarende krav finder anvendelse på udstedere af e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelserne er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at udstederens genopretningsplan ikke indeholder passende betingelser og procedurer for at sikre rettidig gennemførelse af genopretningsforanstaltninger.

Artikel 47, stk. 1-3, i MiCA omhandler udstedere af aktivbaserede tokens forpligtigelse til at udarbejde og opretholde en operationel plan til støtte for en velordnet genindløsning af hver aktivbaseret token. Det fremgår af artikel 55 i MiCA, at tilsvarende krav finder anvendelse på udstedere af e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelserne er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at udstederens genindløsningsplan ikke sikrer kontinuitet i kritiske aktiviteter, der udføres af udstederen eller af eventuelle tredjepartsenheder, og som er nødvendige for en velordnet genindløsning.

Artikel 48, stk. 6 og 7, i MiCA omhandler pligten til at underrette Finanstilsynet, inden e-pengeinstitut udbyder e-pengetokens til offentligheden eller anmoder om at få optaget e-pengetokens til handel. Ansvarssubjektet for overtrædelse af bestemmelserne er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et e-pengeinstitut, der udsteder e-pengetokens, ikke underretter Finanstilsynet senest 40 arbejdsdage før den dato, hvor det har til hensigt at udbyde disse e-pengetokens til offentligheden eller anmode om e-pengenes optagelse til handel.

Artikel 49, stk. 5, i MiCA omhandler oplysningspligten vedrørende betingelserne for genindløsningen. I denne lov skal ”genindløsning” forstås i overensstemmelse med § 96 i lov om betalinger. Ansvarssubjektet for overtrædelse af bestemmelsen er et e-pengeinstitut, der udsteder e-

pengetokens. Den strafbare handling består i, at et e-pengeinstitut, der udsteder e-pengetokens, ikke oplyser om betingelserne for genindløsning på en fremtrædende plads i hvidbogen om kryptoaktiver.

Artikel 51, stk. 1-9, 11-13 og stk. 14, 1. pkt., i MiCA omhandler kravene til indhold og form af hvidbogen om kryptoaktiver vedrørende e-pengetokens. Ansvarssubjektet for overtrædelse af bestemmelserne er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at hvidbogen ikke indeholder alle oplysninger, som fremgår af artikel 51, stk. 1, i MiCA eller at oplysningerne i hvidbogen er vildledende.

Artikel 53, stk. 1-3, 5 og 6, i MiCA omhandler markedsføringskommunikation, der vedrører et udbud til offentligheden af e-pengetokens eller optagelse af sådanne e-pengetokens til handel. Ansvarssubjektet for overtrædelse af bestemmelserne er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at markedsføringskommunikationen ikke indeholder en klar og utvetydig erklæring om, at indehavere af e-pengetokens har ret til, når som helst, at genindløse disse e-pengetokens over for udstederen til pariværdi.

Artikel 55 i MiCA fastsætter at udstedere af e-pengetokens er omfattet af kravene i artikel 46 og 47 i MiCA. Derudover fastsætter bestemmelsen datoen, hvorpå genopretningsplanen senest skal meddeles Finanstilsynet. Ansvarssubjektet for overtrædelse af bestemmelsen er et e-pengeinstitut, der udsteder e-pengetokens. Den strafbare handling består eksempelvis i, at et e-pengeinstitut, der udsteder e-pengetokens, ikke har udarbejdet eller opretholdt en genopretningsplan, som er i overensstemmelse med kravene i artikel 46 og 47.

Artikel 65, stk. 4, i MiCA omhandler oplysningskrav ved grænseoverskridende levering af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som udbyder kryptoaktivtjenester efter artikel 60, stk. 4, i MiCA. Den strafbare handling består i, at e-pengeinstitut påbegynder leveringen af kryptoaktivtjenester i en anden medlemsstat end Danmark inden 15 kalenderdage efter at have indgivet oplysninger, efter artikel 65, stk. 1, eller inden at have modtaget meddelelse fra Finanstilsynet den efter artikel 65, stk. 2.

Artikel 66, stk. 1-5, i MiCA omhandler udbydere af kryptoaktivtjenesters forpligtelse til at handle ærligt, redeligt og professionelt i kundernes bedste interesse. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som udbyder kryptoaktivtjenester efter artikel 60, stk. 4, i MiCA. Den strafbare handling består eksempelvis i, at e-pengeinstitutter giver deres kunder vildledende oplysninger.

Artikel 68, stk. 4-9, i MiCA omhandler kravene til ledelsesordninger og indretningen af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af artikel 68, stk. 4, 5 og stk. 7-9, er e-pengeinstitutter. Ansvarssubjektet for overtrædelse af artikel 68, stk. 6, er ledelsesorganet hos e-pengeinstitutter. Den strafbare handling består eksempelvis i, at e-pengeinstitutter ikke har vedtaget procedurer, som er tilstrækkelige til at sikre overholdelsen af MiCA. Den strafbare handling kan endvidere bestå i, at ledelsesorganer hos et e-pengeinstitut ikke regelmæssigt vurderer og evaluerer effektiviteten af den politik og de ordninger og procedurer, der er indført for at opfylde forpligtelserne i artikel 66-83 i MiCA, herunder ikke træffer passende foranstaltninger til at afhjælpe eventuelle mangler.

Artikel 69 i MiCA omhandler krav til at meddele Finanstilsynet eventuelle ændringer i ledelsesorganet hos en udbyder af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som udbyder kryptoaktivtjenester efter artikel 60, stk. 4, i MiCA. Den strafbare handling består eksempelvis i, at e-pengeinstitutter ikke giver Finanstilsynet alle oplysninger, som er nødvendige for Finanstilsynets vurdering af overholdelsen af artikel 68 i MiCA, inden nye medlemmer af ledelsesorganet tiltræder deres stilling.

Artikel 71, stk. 1-4, i MiCA fastsætter krav til udbydere af kryptoaktivtjenesters klagebehandlingsprocedurer. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som udbyder kryptoaktivtjenester efter artikel 60, stk. 4, i MiCA. Den strafbare handling består eksempelvis i, at et e-pengeinstitut kræver betaling af gebyr eller anden afgift i forbindelse med behandling af klager fra deres kunder.

Artikel 72, stk. 2-4, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som udbyder kryptoaktivtjenester efter artikel 60, stk. 4, i MiCA. Den strafbare handling består eksempelvis i, at et e-pengeinstitut ikke oplyser sine kunder og potentielle kunder om de skridt, e-pengeinstituttet har taget for at begrænse interessekonflikter.

Artikel 73, stk. 2 og 3, i MiCA regulerer udbydere af kryptoaktivtjenesters outsourcing af tjenester eller aktiviteter til tredjeparter. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som udbyder kryptoaktivtjenester efter artikel 60, stk. 4, i MiCA. Den strafbare handling består eksempelvis i, at et e-pengeinstitut ikke træffer alle rimelige foranstaltninger for at undgå yderligere operationel risiko, eller at et e-

pengeinstitut ikke sikrer at betingelserne i artikel 73, stk. 1, litra a-g, til enhver tid er opfyldt.

Artikel 74 i MiCA omhandler velordnet afvikling af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er e-pengeinstitutter, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at den i artikel 74, nævnte plan for velordnet afvikling ikke godtgør, at e-pengeinstituttet har evnen til at gennemføre en velordnet afvikling uden at påføre sine kunder unødig økonomisk skade.

Artikel 75, stk. 3-6 og 9, i MiCA fastsætter forpligtelser for udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er e-pengeinstitutter, som udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at e-pengeinstituttets politik for deponering, som anført i artikel 75, stk. 3, ikke minimerer risikoen for tab af kunders kryptoaktiver som følge af svig, cybertrusler eller forsømmelighed.

Artikel 82, stk. 1, i MiCA fastsætter krav til indholdet af den aftale udbydere af kryptoaktivtjenester, der udbyder overførselstjenester på vegne af kunder, skal indgå med deres kunder. Ansvarssubjektet for overtrædelse af bestemmelserne er e-pengeinstitutter, der udbyder overførselstjenester på vegne af kunder. Den strafbare handling består eksempelvis i, at e-pengeinstitutter ikke indgår en aftale med deres kunder, der indeholder de punkter, som er oplistet i artikel 82, stk. 1, litra a-e.
s
Den foreslåede ændring for så vidt angår henvisninger til MiCA supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Disse ændringer foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

I det følgende redegøres for de nævnte artikler i DORA-forordningen.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der hermed betalingsinstitutter, e-pengeinstitutter, udbydere af kontooplysningstjenester og virksomheder med begrænset tilladelse til at udstede elektroniske penge eller udbyde betalingstjenester, jf. artikel 2, stk. 1, litra b, d, c, jf. artikel 2, stk. 2, i DORA-forordningen.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne

kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten,
integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på den kompetente myndigheds anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -

procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig

forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og

efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer

for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen

af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen

af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til

Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette den Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med

artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan

også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1 er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som

til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h), at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g), og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g), og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret

overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i, at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf.

litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de

leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkelig hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b), nr. i), som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b), nr. ii), som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-

tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.
Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e), fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle

enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og

risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr.i.

Dernæst fastsætter artikel 30, stk. 3, litra e), nr. ii-iv), retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at

migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 3

Til nr. 1 (fodnoten i lov om kapitalmarkeder)

Lov om kapitalmarkeder gennemfører i dag dele af NIS-direktivet, herunder bestemmelser om udpegning af operatører af væsentlige tjenester, jf. § 58 a i loven, og bestemmelser om Finanstilsynets og Center For Cybersikkerheds orientering af offentligheden om hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge eller håndtere igangværende hændelser, jf. § 236 a.

Det foreslås i *fodnoten* til lovens titel, at »dele af Europa-Parlamentets og Rådets direktiv 2016/1148/EU af 6. juli 2016, EU-Tidende 2016, nr. L 194, side 1,« udgår, og at »og dele af Europa-Parlamentets og Rådets direktiv 2019/879/EU af 20. maj 2019 (BRRD II), EU-Tidende 2019, nr. L 150, side 296« ændres til: »dele af Europa-Parlamentets og Rådets direktiv 2019/879/EU af 20. maj 2019 (BRRD II), EU-Tidende 2019, nr. L 150, side 296, og dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, EU-Tidende 2022, nr. L 333, side 153-163«.

Det foreslåede medfører, at henvisning til NIS direktivet udgår fra fodnoten. Det skal ses i sammenhæng med, at NIS 2-direktivet ophæver NIS-direktivet. Det betyder også, at de dele af NIS-direktivet, der er gennemført i lov om kapitalmarkeder, foreslås ophævet i nærværende lovforslag, herunder bestemmelserne om udpegning af operatører af væsentlige tjenester og orientering af offentligheden om hændelser.

Det foreslåede medfører desuden, at der indsættes en henvisning til, at der med denne lov foretages en gennemførelse af dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor. Denne henvisning tilføjes, idet lovforslaget gennemfører dele af artikel 6 i direktivet, der vedrører ændringer til 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter (MiFID II) i lov om kapitalmarkeder. Direktivet er

et følgedirektiv til DORA-forordningen. Med forslaget til § 2, nr. 12, foreslås det, at Finanstilsynet skal påse overholdelsen af DORA-forordningen. Der henvises til lovforslagets § 3, nr. 16.

Til nr. 2 (§ 58 a i lov om kapitalmarkeder)

Det fremgår af § 58 a, stk. 1, at Finanstilsynet mindst hvert andet år udpeger de operatører af markedspladser og centrale modparter (CCP'er), der er operatører af væsentlige tjenester. Det fremgår af stk. 2, hvilke kriterier Finanstilsynet skal lægge vægt på i forbindelse med udpegningen efter stk. 1. Videre fremgår det af stk. 3, at Finanstilsynet på sin hjemmeside offentliggør, hvilke operatører af markedspladser og centrale modparter (CCP'er) der er udpeget som operatører af væsentlige tjenester.

Bestemmelsen gennemfører NIS-direktivets artikel 5, stk. 1-3 og 5, hvorefter medlemsstaterne identificerer operatører af væsentlige tjenester ud fra, at de tjenester der leveres er væsentlige for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, at leveringen af tjenesterne afhænger af net- og informationssystemer, og at en hændelse vil få væsentlige forstyrrende virkninger for leveringen af tjenesterne.

Med en hændelse forstås enhver begivenhed, der har en negativ indvirkning på sikkerheden i en operatørs net- og informationssystemer. Med sikkerhed i net- og informationssystemer forstås net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Til sidst fremgår det af stk. 4, at Finanstilsynet kan fastsætte nærmere regler om udpegningen og kriterierne herfor i medfør af stk. 1 og 2, og regler om hændelsesrapportering, herunder om, at Finanstilsynet og Center for Cybersikkerhed underrettes ved en hændelse, der har en negativ indvirkning på sikkerheden i virksomhedens net- og informationssystemer.

Bestemmelsen gennemfører NIS-direktivets artikel 14, stk. 3, hvorefter en operatør af væsentlige tjenester hurtigst muligt skal foretage en underretning til den kompetente myndighed eller CSIRT, af hændelser, der har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som virksomheden leverer. Ved CSIRT forstås en national it-beredskabsenhed, der håndterer hændelser, og som har ansvar for at sikre samarbejdet om sikkerheden i net- og informationssystemer i EU, jf. definitionen heraf i § 2, nr. 17, i lov om net- og informationssikkerhed for domænenavnssystemer

og visse digitale tjenester. I Danmark er det Forsvarets Efterretningstjeneste, herunder Center for Cybersikkerhed, der er udpeget som CSIRT.

Der henvises i det hele til de specielle bemærkningerne til § 58 a i Folketingstidende 2017-18, tillæg A, L 144 som fremsat, side 33-35.

Det foreslås at ophæve *§ 58 a.*

Ophævelsen foreslås, da NIS 2-direktivet ophæver NIS-direktivet, herunder reglerne i artikel 5 om medlemsstaternes identifikation af operatører af væsentlige tjenester og kriterierne herfor, og kravene i artikel 14, stk. 3, om underretning af hændelser til den kompetente myndighed eller CSIRT.

Kravet om underretning af hændelser i artikel 14, stk. 3, i NIS-direktivet bliver erstattet af kravet om indberetning af større informations- og kommunikationsteknologirelaterede hændelser i medfør af artikel 19, stk. 1, i DORA-forordningen, der gælder for finansielle enheder, herunder operatører af markedspladser og centrale modparter (CCP'er), jf. artikel 2, stk. 1, litra h og i. Når Finanstilsynet modtager en underretning om en større it-hændelse, skal Finanstilsynet rettidigt forelægge nærmere oplysninger om hændelsen for andre myndigheder, for hvem hændelsen er relevant, jf. artikel 19, stk. 6, i DORA-forordningen. Artikel 19, stk. 6, nævner de myndigheder, som Finanstilsynet kan forelægge en hændelse for, herunder CSIRT, dvs. Center for Cybersikkerhed.

Til nr. 3 (§ 60, stk. 1, nr. 7, i lov om kapitalmarkeder)

Det gældende § 60, stk. 1, nr. 7, i lov om kapitalmarkeder fastsætter, at Finanstilsynet kan inddrage en tilladelse efter lovens § 59, når en operatør af et reguleret marked groft eller gentagne gange har tilsidesat sine forpligtelser efter denne lov, bestemmelser fastsat i medfør af denne lov, påbud i henhold til lovforslagets kapitel 37 eller pligter efter Europa-Parlamentets og Rådet forordning nr. 600/2014 (EU) om markeder for finansielle instrumenter og om ændring af forordning nr. 648/2012 (EU) (MiFIR) og bestemmelser fastsat i medfør heraf.

Det foreslås i *§ 60, stk. 1, nr. 7,* at ændre »eller pligter efter Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og regler fastsat i medfør heraf.« til », pligter efter Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter og regler fastsat i medfør heraf eller pligter efter Europa-Parlamentets og Rådets (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler fastsat i medfør heraf.«

Den foreslåede ændring vil medføre, at Finanstilsynet kan inddrage en tilladelse efter lovens § 59, når en operatør af et reguleret marked groft eller gentagne gange har tilsidesat sine forpligtelser efter MiCA. Inddragelsen af tilladelsen må kun ske, hvis der ikke findes en mindre vidtgående reaktion, som vil kunne opnå samme resultat.

Ændringen foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en række aktører skal efterleve kravene i forordningen.

Til nr. 4 (§ 71, stk. 2, nr. 3, i lov om kapitalmarkeder)

§ 71 i lov om kapitalmarkeder fastsætter regler for en operatør af et reguleret markeds ansvar for en betryggende og hensigtsmæssig drift af det regulerede marked. Stk. 2 i bestemmelsen fastsætter en række organisatoriske krav til det regulerede marked, som operatøren af det regulerede marked er ansvarlig for efterleves både generelt og i konkrete sager.

Bestemmelsen gennemfører artikel 47, stk. 1, i Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter (MiFID II).

Det følger af § 71, stk. 2, nr. 3, i lov om kapitalmarkeder, at en operatør af et reguleret marked skal sikre en ordentlig forvaltning af den tekniske funktion af markedspladsens systemer, herunder etablere effektive nødsystemer.

Bestemmelsen gennemfører artikel 47, stk. 1, litra c, i MiFID II.

Det foreslås, at *§ 71, stk. 2, nr. 3,* affattes således, at det fremgår, at en operatør af et reguleret marked skal kunne styre it-risici i overensstemmelse med kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring gennemfører artikel 6, nr. 3, litra a, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der er et følgedirektiv til DORA, der ændrer i artikel 47, stk. 1, i MiFID II.

Kapitel II i DORA-forordningen fastsætter bl.a. krav om, at finansielle enheder, herunder operatører af et reguleret marked, skal kunne styre it-risici. Kapitlet indeholder bl.a. regler om interne forvaltnings- og

kontrolrammer til at sikre en effektiv og forsigtig styring af risiciene, anvendelse og vedligeholdelse af opdaterede systemer og løbende overvågning og kontrol hermed samt indførelse af en politik for driftsstabilitet.

Overtrædelse af § 71, stk. 2, nr. 3, er strafbelagt, jf. § 247 i lov om kapitalmarkeder. Ansvarssubjektet for overtrædelse af bestemmelsen er operatøren af et reguleret marked. Med indsættelsen af den nye bestemmelse i nr. 3, vil den strafbare handling bestå i manglende styring af it-risici i henhold til reglerne herom i kapitel II i DORA-forordningen. Som eksempel herpå kan nævnes det tilfælde, hvor operatøren af et reguleret marked ikke indfører en ramme for it-risikostyring, der som minimum omfatter strategier, politikker, procedurer, it-protokoller og -værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad at beskytte alle informationsaktiver og it-aktiver, jf. artikel 6, stk. 2, i DORA-forordningen.

Der henvises i øvrigt til § 3, nr. 19, i nærværende forslag og bemærkningerne hertil.

Til nr. 5-7 (§ 114 og § 114, nr. 1 og 5, i lov om kapitalmarkeder)

§ 114 stiller en række krav til systemer, procedurer og ordninger hos operatøren af en markedsplads, der skal sikre, at markedspladsens handelssystemer kan fungere i perioder med spidsbelastninger og alvorlig markedsstress.

Det følger af § 114, at en operatør af en markedsplads skal have systemer, procedure og ordninger, der sikrer, at markedspladsens handelssystemer 1) er fleksible, 2) har tilstrækkelig kapacitet til at håndtere perioder med spidsbelastning med hensyn til ordrer og meddelelser, 3) kan sikre korrekt handel i tilfælde af alvorlig markedsstress, 4) er fuldt gennemprøvede og 5) er omfattet af driftsstabilitetsordninger, der effektivt sikrer, at markedets tjenester kan opretholdes, i tilfælde af at markedspladsens handelssystem svigter.

Bestemmelsen gennemfører artikel 18, stk. 5, og artikel 48, stk. 1, i MiFID II. Artikel 48, stk. 1, retter sig mod operatører af et reguleret marked. Det fremgår af artikel 18, stk. 5, at artikel 48, stk. 1, også gælder for operatører af en multilateral handelsfacilitet (MHF) eller en organiseret handelsfacilitet (OHF).

Det foreslås at ændre *§ 114*, hvorefter en operatør af en markedsplads skal etablere og opretholde operationel modstandsdygtighed i overensstemmelse med kravene i kapitel II i DORA-forordningen.

Kapitel II i DORA-forordningen fastsætter krav om, at finansielle enheder, herunder operatører af et reguleret marked, skal kunne styre it-risici. Kapitlet indeholder bl.a. regler om interne forvaltnings- og kontrolrammer til at sikre en effektiv og forsigtig styring af risiciene, anvendelse og vedligeholdelse af opdaterede systemer og løbende overvågning og kontrol hermed samt indførelse af en politik for driftsstabilitet.

Desuden foreslås det i *§ 114, nr. 1,* at ændre »fleksible« til: »modstandsdygtige«.

Til sidst foreslås det at ændre *§ 114, nr. 5,* hvorefter en operatør af en markedsplads skal sikre, at markedspladsens handelssystemer er omfattet af driftsstabiliseringsordninger, herunder politikker og planer for it-driftsstabilitet og planer for it-indsats- og genopretning udarbejdet i overensstemmelse med artikel 11 i DORA-forordningen, der effektivt sikrer, at markedets tjenester kan opretholdes, i tilfælde af at markedspladsens handelssystem svigter.

Artikel 11 i DORA-forordningen fastsætter regler om indsats og genopretning af informations- og kommunikationsteknologi, herunder regler om, at finansielle enheder, som bl.a. operatører af markedspladser, indfører en politik og planer for driftsstabilitet og planer for indsats- og genopretning.

De foreslåede ændringer gennemfører artikel 6, nr. 4, litra a, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der er et følgedirektiv til DORA, der ændrer i artikel 48, stk. 1, i MiFID II.

Overtrædelse af § 114 er strafbelagt, jf. § 247 i lov om kapitalmarkeder. Ansvarssubjektet for overtrædelse af bestemmelsen er operatøren, der driver den pågældende markedsplads. Den strafbare handling består i drift af en markedsplads uden tilstedeværelse af systemer, procedurer og ordninger for markedspladsens handelssystem, der opfylder kravene i nr. 1-5, jf. de specielle bemærkninger til § 114, Folketingstidende 2016-17, tillæg A, L 155 som fremsat, side 220. Med de foreslåede ændringer vil den strafbare handling også kunne bestå i manglende etablering og opretholdelse af operationel modstandsdygtighed i overensstemmelse med kravene i kapitel II i DORA-forordningen, i at handelssystemerne ikke er modstandsdygtige, eller at operatøren ikke indfører politikker og planer for it-driftsstabilitet og planer for it-indsats- og genopretning i overensstemmelse med artikel 11 i DORA-forordningen.

Der henvises i øvrigt til § 2, nr. 19, i nærværende forslag og bemærkningerne hertil.

Til nr. 8 (§ 118, stk. 2, nr. 1, i lov om kapitalmarkeder)

§ 118 i lov om kapitalmarkeder fastsætter krav til de systemer, procedurer og ordninger, som en operatør af en markedsplads skal have til at forhindre ureglementerede handelsvilkår som følge af algoritmiske handelssystemer. I medfør af § 118, stk. 2, nr. 1, skal de ordninger, som en operatør af en markedsplads skal have, som minimum sikre og lette medlemmers afprøvning af algoritmer.

Bestemmelsen gennemfører artikel 18, stk. 5, og artikel 48, stk. 1, i MiFID II. Artikel 48, stk. 1, der retter sig mod operatører af et reguleret marked. Det fremgår af artikel 18, stk. 5, at artikel 48, stk. 6, også gælder for operatører af en multilateral handelsfacilitet (MHF) eller en organiseret handelsfacilitet (OHF).

Det foreslås i *§ 118, stk. 2, nr. 1,* efter »afprøvning af algoritmer«, at indsætte: »i overensstemmelse med kravene til it-risikostyring af informations- og kommunikationsteknologi og til test af digital operationel modstandsdygtighed i kapitel II og IV i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede medfører, at en operatør af en markedsplads skal have ordninger som minimum skal sikre og lette medlemmers afprøvning af algoritmer i overensstemmelse med kravene til it-risikostyring og til test af digital operationel modstandsdygtighed i II og IV i DORA-forordningen.

Kapitel II i DORA-forordningen fastsætter krav om, at finansielle enheder, herunder operatører af et reguleret marked, skal kunne styre it-risici. Kapitlet indeholder bl.a. regler om interne forvaltnings- og kontrolrammer til at sikre en effektiv og forsigtig styring af risiciene, anvendelse og vedligeholdelse af opdaterede systemer og løbende overvågning og kontrol hermed samt indførelse af en politik for driftsstabilitet.

Kapitel IV i DORA-forordningen fastsætter krav om test af digital operationel modstandsdygtighed i forhold til håndteringen af it-hændelser. Hændelser er defineret som hændelser, der kompromitterer sikkerheden i net- og informationssystemerne og har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de tjenester, som den finansielle enhed leverer, jf. artikel 3, nr. 8, i forordningen.

Den foreslåede ændring gennemfører artikel 6, nr. 4, litra b, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der er et følgedirektiv til DORA, der ændrer i artikel 48, stk. 6, i MiFID II.

Overtrædelse af § 118, stk. 2, nr. 1, er strafbelagt, jf. § 247 i lov om kapitalmarkeder. Ansvarssubjektet for overtrædelse af bestemmelsen er operatøren, der driver den pågældende markedsplads. Den strafbare handling består i, at en operatør af en markedsplads ikke har ordninger, der sikrer og letter medlemmers afprøvning af algoritmer. Med den foreslåede ændring vil den strafbare handling bestå i ikke at have ordninger, der sikrer og letter medlemmers afprøvning af algoritmer i overensstemmelse med kravene i kapitel II og IV i DORA-forordningen.

Der henvises i øvrigt til § 3, nr. 19, i nærværende forslag og bemærkningerne hertil for så vidt angår.
Til nr. 9 (§ 129, stk. 2, nr. 12, i lov om kapitalmarkeder)

§ 129, stk. 2, i lov om kapitalmarkeder regulerer hvilke positioner, der ikke skal medregnes i opgørelsen af en persons nettoposition i landbrugsråvarederivater og kritiske eller væsentlige råvarederivater og medfører, at visse finansielle virksomheder har mulighed for at blive undtaget fra reglerne om positionslofter.

Det foreslås at nyaffatte *§ 129, stk. 2,* så det i nr. 1-3 kommer til at fremgå, at de positioner, som kan undtages fra opgørelsen af en persons nettoposition, er positioner, som objektivt kan måles til dels at reducere de risici, der er direkte tilknyttet den ikkefinancielle enheds forretningsmæssige aktivitet og dels at hidrøre fra transaktioner, der er indgået for at opfylde en forpligtelse til at tilføre en markedsplads likviditet.

Det fremgår ikke af den nyaffattelse som skete ved § 2, nr. 2, i lov nr. 2383 af 14. december 2021 om ændring af lov om finansiel virksomhed, hvorfor bestemmelsen affattes på ny. Der er således tale om en præcisering af bestemmelsen, så direktivteksten bliver korrekt implementeret i dansk ret.

Den foreslåede affattelse af § 129, stk. 2, er en videreførelse af den nugældende bestemmelse med ovennævnte tilføjelse for så vidt angår nr. 1-3, hvor nr. 4 er helt enslydende med den nugældende.

Det foreslås i *nr. 1,* at positioner, der besiddes af eller på vegne af en ikkefinansiel enhed, og som objektivt kan måles til at reducere de risici, der er direkte knyttet til den ikkefinansielle enheds forretningsmæssige aktivitet, ikke skal medregnes i opgørelsen af en persons nettoposition.

Undtagelsen af positioner nævnt i nr. 1 skal give ikkefinansielle virksomheder som eksempelvis landmænd og energiselskaber mulighed for fortsat at anvende råvarederivater til at nedbringe de risici, der er forbundet med deres kommercielle forretningsaktiviteter. Eksempelvis afdækning af risikoen for fald i kornpriserne, der er ukendt på såningstidspunktet. Sigtet med at introducere positionslofter for handel med råvarederivater har primært været at begrænse handlen med råvarederivater i spekulationsøjemed, hvilket i et vist omfang er blevet associeret med hyppigere observerede udsving i råvarepriserne.

Det foreslås i *nr. 2*, at positioner, der besiddes af eller på vegne af en finansiel enhed, der indgår i en overvejende kommerciel koncern, såfremt den finansielle enhed handler på vegne af en ikkefinansiel enhed i koncernen, og positionerne objektivt kan måles til at reducere de risici, der er knyttet til den pågældende ikkefinansielle enheds forretningsmæssige aktivitet, ikke skal medregnes i opgørelsen af en persons nettoposition.

Et eksempel herpå er et energiselskab, der har registreret en del af selskabet som en finansiel virksomhed. Hvis denne udelukkende anskaffer sig positioner i råvarederivater for at afdække udsving i energipriserne og afdække den samlede koncerns risici, vil dens positioner fremadrettet være undtaget fra reglerne om positionslofter.

Det foreslås i *nr. 3*, at positioner, der besiddes af finansielle og ikkefinansielle modparter med hensyn til positioner, som objektivt kan måles til at hidrøre fra transaktioner, der er indgået for at opfylde en forpligtelse til at tilføre en markedsplads likviditet, ikke skal medregnes i opgørelsen af en persons nettoposition.

Et eksempel herpå er en bank, der agerer market maker i et råvarederivat, hvormed de øger likviditeten på markedet ved at understøtte handel mellem købere og sælgere. Positioner opnået i forbindelse med denne aktivitet vil fremadrettet være undtaget fra reglerne om positionslofter.

Det foreslås i *nr. 4*, at værdipapirer som nævnt i § 4, nr. 1, litra c, der vedrører en råvare eller et underliggende aktiv som nævnt i § 4, nr. 10, ikke skal medregnes i opgørelsen af en nettoposition.

Bestemmelsen gennemfører artikel 57, stk. 1, andet afsnit, litra a-d, i Europa-Parlamentets og Rådets direktiv 2014/65/EU om markeder for finansielle instrumenter (MiFID II), som blev ændret ved artikel 1, stk. 10, litra a, i Europa-Parlamentets og Rådets direktiv (EU) 2021/338 af 16. februar 2021 om ændring af direktiv 2014/65/EU, for så vidt angår

oplysningskrav, produktstyring og positionslofter, og direktiv 2013/36/EU og (EU) 2019/878, for så vidt angår deres anvendelse på investeringsvirksomheder med henblik på at bidrage til genopretningen efter covid-19-krisen (CMRP MiFID II-del).

Til nr. 10 (§ 130, stk. 1, nr. 5, i lov om kapitalmarkeder)

Det følger af den gældende § 130, stk. 1, nr. 5, i lov om kapitalmarkeder, at en operatør af en markedsplads i forbindelse med positionskontrol kan kræve, at en person midlertidigt tilbagefører likviditet til markedspladsen til en aftalt pris og en aftalt mængde.

Det foreslås at ændre *§ 130, stk. 1, nr. 2,* så en operatør af en markedsplads i forbindelse med positionskontrol kan kræve, at en person midlertidigt tilbagefører likviditet til markedspladsen til en aftalt pris og en aftalt mængde med det udtrykkelige formål at afbøde virkningen af en stor og dominerende position.

Ændringen sørger for, at bestemmelsen er direktivnært implementeret, således at det nu fremgår, at det skal være med det udtrykkelige formål at afbøde virkningen af en stor og dominerende position. Det har ikke tidligere fremgået.

Formålet med § 130, stk. 1, er at sikre, at en operatør af en markedsplads, der skal kontrollere og indberette om de enkelte positionslofter, skal kunne indhente den korrekte information til at udføre dette hverv.

Bestemmelsen gennemfører artikel 57, stk. 8, første afsnit, litra d, i Europa-Parlamentets og Rådets direktiv 2014/65/EU om markeder for finansielle instrumenter (MiFID II).

Til nr. 11-13 (§ 135, stk. 1, nr. 1, litra a, § 135, stk. 1, nr. 3 og 4, i lov om kapitalmarkeder)

§ 135 fastsætter krav til de handelssystemer, som et fondsmæglerselskab, der benytter sig af algoritmisk handel, anvender.

Det fremgår af § 135, stk. 1, nr. 1, litra a, at et fondsmæglerselskab, der benytter sig af algoritmisk handel, skal have effektive systemer og risikokontrolforanstaltninger, der sikrer, at vedkommendes handelssystemer er modstandsdygtige over for forstyrrelser på markedet og har tilstrækkelig kapacitet til at håndtere perioder med spidsbelastning.

Videre fremgår det af § 135, stk. 1, nr. 3 og 4, at et fondsmæglerselskab, der benytter sig af algoritmisk handel, skal have effektive ordninger, der sikrer, at fondsmæglerselskabet kan håndtere en brist i fondsmæglerselskabets handelssystemer, og sikre, at fondsmæglerselskabets systemer er grundigt afprøvet, og underlægge sine handelssystemer behørig overvågning, der sikrer, at kravene i nr. 1-3 er overholdt.

Bestemmelsen gennemfører artikel 17, stk. 1, i MiFID II.

Det foreslås i *§ 135, stk. 1, nr. 1, litra a,* at ændre »til at håndtere perioder med spidsbelastning« til: »i overensstemmelse med kravene til it-risikostyring i kapitel II i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede medfører, at et fondsmæglerselskab, der benytter sig af algoritmisk handel, skal have effektive systemer og risikokontrolforanstaltninger, der sikrer, at vedkommendes handelssystemer er modstandsdygtige over for forstyrrelser på markedet og har tilstrækkelig kapacitet i overensstemmelse med kravene til it-risikostyring i kapitel II i DORA-forordningen.

Kapitel II i DORA-forordningen fastsætter krav om, at finansielle enheder, herunder fondsmæglerselskaber, skal kunne styre it-risici. Kapitlet indeholder bl.a. regler om interne forvaltnings- og kontrolrammer til at sikre en effektiv og forsigtig styring af risiciene, anvendelse og vedligeholdelse af opdaterede systemer og løbende overvågning og kontrol hermed samt indførelse af en politik for driftsstabilitet.

Desuden foreslås i *§ 135, stk. 1, nr. 3,* efter »handelssystemer,« at indsætte: »herunder planer for it-driftsstabilitet og planer for it-indsats og genopretning i overensstemmelse med artikel 11 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede medfører, at et fondsmæglerselskab, der benytter sig af algoritmisk handel, skal have effektive ordninger, der sikrer, at fondsmæglerselskabet kan håndtere en brist i fondsmæglerselskabets handelssystemer, herunder planer for it-driftsstabilitet og planer for it-indsats- og genopretning indenfor informations- og kommunikationsteknologi i henhold til artikel 11 i DORA-forordningen, og sikrer, at fondsmæglerselskabets systemer er grundigt afprøvet.

Artikel 11 i DORA-forordningen fastsætter regler om it-indsats og genopretning, herunder regler om, at finansielle enheder, som bl.a. fondsmæglerselskaber, indfører en politik og planer for driftsstabilitet og planer for indsats- og genopretning.

Til sidst foreslås i *§ 135, stk. 1, nr. 4,* efter »kravene i nr. 1-3« at indsætte: »og kravene til it-risikostyring og til test af digital operationel modstandsdygtighed i kapitel II og IV i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede medfører, at et fondsmæglerselskab, der benytter sig af algoritmisk handel, skal underlægge sine handelssystemer behørig overvågning, der sikrer, at kravene i nr. 1-3 og kravene til it-risikostyring og til test af digital operationel modstandsdygtighed i kapitel II og IV i DORA-forordningen er overholdt.

Kapitel II i DORA-forordningen fastsætter krav om, at finansielle enheder, herunder fondsmæglerselskaber, skal kunne styre it-risici. Kapitlet indeholder bl.a. regler om interne forvaltnings- og kontrolrammer til at sikre en effektiv og forsigtig styring af risiciene, anvendelse og vedligeholdelse af opdaterede systemer og løbende overvågning og kontrol hermed samt indførelse af en politik for driftsstabilitet.

Kapitel IV i DORA-forordningen fastsætter krav om test af digital operationel modstandsdygtighed i forhold til håndteringen af it-relaterede hændelser. It-relaterede hændelser er defineret som hændelser, der kompromitterer sikkerheden i net- og informationssystemerne og har en negativ indvirkning på tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data eller på de tjenester, som den finansielle enhed leverer, jf. artikel 3, nr. 8, i forordningen.

De foreslåede ændringer gennemfører artikel 6, nr. 2, litra a, i Europa-Parlamentets og rådets direktiv (EU) 2022/2556 af 14. december 2022, der ændrer i artikel 17, stk. 1, i MiFID II.

Overtrædelse af § 135 er strafbelagt, jf. § 247 i lov om kapitalmarkeder. Ansvarssubjektet for overtrædelsen af bestemmelsen er det fondsmæglerselskab, der benytter sig af algoritmisk handel. Den strafbare handling består i at benytte algoritmisk handel uden at have systemer, kontrolforanstaltninger og ordninger, der i tilstrækkelig grad sikrer et sikkerhedsniveau i overensstemmelse med kravene i bestemmelsen. Med den foreslåede ændring vil den strafbare handling i medfør af § 135, stk. 1, nr. 1, litra a, bestå i enten ikke at have effektive systemer og

risikokontrolforanstaltninger, der sikrer, at vedkommendes handelssystemer er modstandsdygtige over for forstyrrelser på markedet og har tilstrækkelig kapacitet i overensstemmelse med kravene i kapitel II i DORA-forordningen. I medfør af § 135, stk. 1, nr. 3 og 4, vil den strafbare handling kunne bestå i ikke at have effektive planer til at kunne håndtere en brist i handelssystemerne, herunder planer for it-driftsstabilitet og planer for it-indsats- og genopretning i henhold til artikel 11 i DORA-forordningen. Til sidst vil en strafbar handling i medfør af § 135, stk. 1, nr. 4, kunne bestå i ikke at overholde kravene i kapitel II og IV i DORA.

Der henvises i øvrigt til § 3, nr. 19, i nærværende forslag og bemærkningerne hertil.

Til nr. 14 (§ 180 g, stk. 3, i lov om kapitalmarkeder)

Det fremgår af § 180 g, stk. 1, at en it-operatør af et detailbetalingssystem er ansvarlig for, at it-driften af det pågældende detailbetalingssystem udføres på en betryggende måde. I medfør af § 180 g, stk. 2, nr. 1, skal en it-operatør kunne styre de risici, som it-driften af detailbetalingssystemet indebærer, og i medfør af stk. 2, nr. 2, skal en it- operatøren også have betryggende kontrol- og sikringsforanstaltninger på it-området. Stk. 3 i bestemmelsen indeholder en bemyndigelse til, at Finanstilsynet kan fastsætte nærmere regler om de foranstaltninger, som en it-operatør skal træffe for at have betryggende kontrol- og sikringsforanstaltninger på it-området, jf. stk. 2, nr. 2. De nærmere regler herom fremgår af bilag 5 til bekendtgørelse nr. 1103 af 30. juni 2022 om og ledelse og styring af pengeinstitutter m.fl. (ledelsesbekendtgørelsen). Der henvises også til de specielle bemærkninger til § 180 g, Folketingstidende 2021-22, tillæg A, L 12 som fremsat, side 112.

Det foreslås i *§ 180 g, stk. 3,* at Finanstilsynet kan fastsætte nærmere regler om de foranstaltninger, som en it-operatør af et detailbetalingssystem, der ikke er udpeget som finansiel digital infrastruktur, jf. § 333, stk. 3, i lov om finansiel virksomhed, skal træffe for at have betryggende kontrol- og sikringsforanstaltninger på it-området, jf. stk. 2, nr. 2.

Bestemmelsen er en konsekvens af, at Finanstilsynet i medfør af forslag til nyt § 333, stk. 1, i lov om finansiel virksomhed kan udpege virksomheder, der udbyder digital infrastruktur eller forvalter it-tjenester, som omhandlet i bilag I i NIS 2-direktivet, og hvis væsentligste aktiviteter består i at drive, administrere eller udvikle tjenester, der er nødvendige for finansielle virksomheders kritiske og vigtige forretningsfunktioner, som en finansiel digital infrastruktur. Det fremgår af forslaget til § 333, stk. 3, at bl.a. it-

operatører af detailbetalingssystemer kan udpeges som finansielle digitale infrastrukturer efter stk. 1.

I det tilfælde, hvor en it-operatør af et detailbetalingssystem bliver udpeget som en finansiel digital infrastruktur, vil det i stedet være de nærmere regler om it- og cyberrisikostyring og kontrol- og sikringsforanstaltninger i finansielle digitale infrastrukturer, som Finanstilsynet får bemyndigelse til at fastsætte i medfør af forslaget til nyt § 333 p, stk. 1, i lov om finansiel virksomhed, der vil finde anvendelse på it-operatøren. Der henvises i det hele til forslaget til § 333 p og de specielle bemærkninger hertil.

Til nr. 15 (§ 180 h i lov om kapitalmarkeder)

Det fremgår af § 180 h i lov om kapitalmarkederm at Finanstilsynet fastsætter bestemmelser om intern it-revision og om systemrevisionens gennemførelse for en it-operatør af et detailbetalingssystem. Finanstilsynet har i dag fastsat regler herom i bekendtgørelse nr. 1581 af 22. december 2022 om systemrevisionens gennemførelse i fælles datacentraler m.fl., der også finder anvendelse for it-operatører af detailbetalingssystemer, jf. § 1, stk. 1, i bekendtgørelsen.

Ved systemrevision forstås intern og ekstern revision af, at de generelle it-kontroller fungerer betryggende. Ved de generelle it-kontroller forstås styringen af den grundlæggende it-sikkerhed, men ikke sikkerheden i specifikke it-systemer. Finanstilsynet fører tilsyn med, at systemrevisionen opfylder forpligtelserne i bekendtgørelsen, jf. de specielle bemærkninger til § 180 h, Folketingstidende 2021-22, tillæg A, L 12 som fremsat, side 113.

Det foreslås i *§ 180 h*, at Finanstilsynet fastsætter bestemmelser om intern it-revision og om systemrevisionens gennemførelse for en it-operatør af et detailbetalingssystem, der ikke er udpeget som finansiel digital infrastruktur, jf. § 333, stk. 3, i lov om finansiel virksomhed.

Bestemmelsen er en konsekvens af, at Finanstilsynet i medfør af forslag til et nyt § 333, stk. 1, i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 24, kan udpege virksomheder, der udbyder digital infrastruktur eller forvalter it-tjenester, som omhandlet i bilag I i NIS 2-direktivet, og hvis væsentligste aktiviteter består i at drive, administrere eller udvikle tjenester, der er nødvendige for finansielle virksomheders kritiske og vigtige forretningsfunktioner, som en finansiel digital infrastruktur. Det fremgår af forslaget til § 333, stk. 3, at bl.a. it- operatører af detailbetalingssystemer kan udpeges som finansielle digitale infrastrukturer efter stk. 1.

I det tilfælde, hvor en it-operatør af et detailbetalingssystem bliver udpeget som en finansiel digital infrastruktur, vil det i stedet være de nærmere regler om it- og cyberrisikostyring og kontrol- og sikringsforanstaltninger i finansielle digitale infrastrukturer, herunder i forhold til den interne og eksterne systemrevision i finansielle digitale infrastrukturer, som Finanstilsynet får bemyndigelse til at fastsætte i medfør af forslaget til nyt § 333 p, stk. 1, litra d, i lov om finansiel virksomhed, der vil finde anvendelse på it-operatøren. Der henvises i det hele til forslaget til § 333 p og de specielle bemærkninger hertil.

Til nr. 16 (§ 211, stk. 2, nr. 15 og 16, i lov om kapitalmarkeder)

Det fremgår af § 211, stk. 1, i lov om kapitalmarkeder, at Finanstilsynet påser overholdelsen af denne lov og regler fastsat i medfør heraf. Det fremgår videre af § 211, stk. 2, at Finanstilsynet påser overholdelsen af en række regler og forordninger.

Det foreslås, at der *i § 211, stk. 2,* indsættes *nr. 15*, hvorefter Finanstilsynet påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslås, at der i § 211, stk. 2, indsættes *nr. 16,* hvorefter Finanstilsynet påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Formålet med de foreslåede bestemmelser er, at Finanstilsynet bliver udpeget som kompetent myndighed til at føre tilsyn med overholdelsen af forordningerne og regler udstedt i medfør heraf.

Finanstilsynet får med bestemmelsen bl.a. også mulighed for at give påbud for overtrædelser af forordningerne, jf. § 220, stk. 1, i lov om kapitalmarkeder og mulighed for at offentliggøre et påbud til en virksomhed eller en fysisk person, jf. § 234, stk. 1, i lov om kapitalmarkeder. Se nærmere om Finanstilsynets mulighed for offentliggørelse af reaktioner i medfør af kapitalmarkedsloven i bemærkningerne til §§ 234-240, jf. Folketingstidende 2016-2017, tillæg A, L 155 som fremsat, side 339 ff.

I tilfælde af, at en virksomhed undlader at efterkomme et påbud fra Finanstilsynet, vil virksomheden kunne straffes med bøde i medfør af § 235, stk. 1, 1. pkt., i lov om kapitalmarkeder.

DORA-forordningen finder bl.a. anvendelse på operatører af markedspladser, værdipapircentraler (CSD'er), centrale modparter

(CCP'er), transaktionsregistre, udbydere af dataindberetningstjenester og administratorer af benchmarks, jf. artikel 2, stk. 1, litra g, h, i, j, m og r.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningen, jf. § 214 i lov om kapitalmarkeder.

Efter artikel 46, litra e, f og h, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler og Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre, sikre overholdelsen af DORA-forordningen for værdipapircentraler (CSD'er), centrale modparter (CCP'er), transaktionsregistre. Efter artikel 46, litra g, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af MiFID II, sikre overholdelsen af DORA-forordningen for markedspladser og udbydere af dataindberetningstjenester. Efter artikel 46, litra o, i DORA-forordningen skal den kompetente myndighed, der er udpeget efter Europa-Parlamentets og Rådets forordning (EU) nr. 1011/2016 af 8. juni 2016 om indeks, der bruges som benchmarks i finansielle instrumenter og finansielle kontrakter eller med henblik på at måle investeringsfondes økonomiske resultater og regler fastsat i medfør heraf, sikre overholdelsen af DORA-forordningen for administratorer af benchmark.

Det foreslåede nr. 15 foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter Finanstilsynet påser, at en række aktører efterlever kravene i forordningen.

Det foreslåede nr. 16 supplerer artikel 46, litra e, f, g, h, i og o, i DORA-forordningen.

Til nr. 17 (§ 226, nr. 17, i lov om kapitalmarkeder)

I medfør af § 224, stk. 1, i lov om kapitalmarkeder er Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger, som de får kendskab til gennem tilsynsvirksomheden.

§ 226 i lov om kapitalmarkeder er en undtagelse til tavshedspligten i § 224, stk. 1. Bestemmelsen fastsætter i hvilke tilfælde, der ikke er noget til hinder

for, at fortrolige oplysninger videregives til en række institutioner, myndigheder og organer mv. i et andet EU/EØS-land mv.

I medfør af § 226 har Finanstilsynet ikke mulighed for at videregive oplysninger til Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 226* at indsætte et nyt *nr. 17,* hvorefter Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større it-relateret hændelse fra en operatør af en markedsplads, en værdipapircentral (CSD), en central modpart (CCP), et transaktionsregistre, en udbyder af dataindberetningstjenester eller en administratorer af benchmark, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til

Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 18 (§ 236 a i lov om kapitalmarkeder)

Det fremgår af § 236 a, 1. pkt., i lov om kapitalmarkeder, at Finanstilsynet efter høring af en operatør af en markedsplads eller central modpart (CCP), der underretter Finanstilsynet og Center for Cybersikkerhed om en hændelse, som har væsentlige konsekvenser for kontinuiteten af de væsentlige tjenester, som de leverer, kan orientere offentligheden om hændelsen, hvis offentlighedens kendskab hertil er nødvendigt for at forebygge eller håndtere en igangværende hændelse. I 2. og 3. pkt. i bestemmelsen fremgår nærmere om, at en offentliggørelse ikke må indeholde fortrolige oplysninger.

Bestemmelsen gennemfører artikel 14, stk. 6, i NIS-direktivet om, at den kompetente myndighed kan oplyse offentligheden om konkrete hændelser, hvis offentlighedens kendskab hertil er nødvendig for at forebygge en hændelse eller håndtere en igangværende hændelse.

Med NIS 2-direktivet sker der en ophævelse af NIS-direktivet, herunder reglerne i artikel 14, stk. 6.

Det foreslås derfor at ophæve *§ 236 a.*

Til nr. 19 og 20 (§ 248 i lov om kapitalmarkeder)

Den gældende § 248 i lov om kapitalmarkeder fastlægger, hvilke overtrædelser af reglerne i Europa-Parlamentets og Rådets forordning (EU) nr. 600/2014 af 15. maj 2014 om markeder for finansielle instrumenter (MiFIR), der straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Bestemmelsen implementerer artikel 70, stk. 3, litra b, og stk. 4, litra b, i Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter (MiFID II).

Det foreslås at ændre *§ 248,* så overtrædelse af artikel 27 b, stk. 1 og 2, i MiFIR kan straffes med bøde medmindre højere straf er forskyldt efter den øvrige lovgivning.

Konkret foreslås det at lade artikel 27 f, stk. 1-3, artikel 27 g, stk. 1-5, og artikel 27 i, stk. 1-4, når en godkendt offentliggørelsesordning (APA) eller en godkendt indberetningsmekanisme (ARM) har en undtagelse i overensstemmelse med artikel 2, stk. 3, udgå af § 248 for derefter at indsætte de samme bestemmelser inklusiv artikel 27 b, stk. 1 og 2, i et nyt 2. pkt. i § 248.

Forslaget er en konsekvens af, at bl.a. artikel 70, stk. 4, litra b, i MiFID II blev ændret ved artikel 1, stk. 5, litra b, i Europa-Parlamentets og Rådets direktiv (EU) 2019/2177 af 18. december 2019 om ændring af direktiv 2009/138/EF om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II), direktiv 2014/65/EU om markeder for finansielle instrumenter og af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme (omnibusdirektivet). Ændringen medførte, at artikel 27 b i MiFIR blev strafbelagt i henhold til MIFID II.

Artikel 27 b i MiFIR blev indsat ved artikel 4, stk. 6, i Europa-Parlamentets og Rådets forordning (EU) 2019/2175 af 18. december 2019 om ændring af forordning (EU) nr. 1093/2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), forordning (EU) nr. 1094/2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), forordning (EU) nr. 1095/2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), forordning (EU) nr. 600/2014 om markeder for finansielle instrumenter, forordning (EU) 2016/1011 om indeks, der bruges som benchmarks i finansielle instrumenter og finansielle kontrakter eller med henblik på at måle investeringsfondes økonomiske resultater, og forordning (EU) 2015/847 om oplysninger, der skal medsendes ved pengeoverførsler (omnibusforordningen). Artikel 27 b blev indsat som følge af, at udbydere af dataindberetningstjenester pr. 1. januar 2022 blev reguleret i MiFIR i stedet for i national ret. Herefter blev den Europæiske Værdipapir- og Markedstilsynsmyndighed (ESMA) som udgangspunkt den kompetente tilsynsmyndighed for udbydere af dataindberetningstjenester. Dog er nogle godkendte offentliggørelsesordninger (APA'er) eller godkendte indberetningsmekanismer (ARM'er) undtaget fra MiFIR og i stedet meddelt tilladelse og underlagt tilsyn fra Finanstilsynet. Disse er fortsat reguleret i lov om kapitalmarkeder.

Artikel 27 b i MiFIR indeholder betingelser for meddelelse af tilladelse som en APA, en CTP eller en ARM.

En APA er en godkendt offentliggørelsesordning, defineret som en person, der er godkendt efter MiFIR til at udøve virksomhed, der består i at offentliggøre handelsindberetninger på vegne af investeringsselskaber i medfør af artikel 20 og 21 i MiFIR.

En ARM er en godkendt indberetningsmekanisme, defineret som en person, der er godkendt efter MiFIR til på vegne af investeringsselskaber at udøve virksomhed, der består i at levere indberetningsoplysninger om transaktioner til de kompetente myndigheder eller ESMA.

En CTP er en udbyder af konsolideret løbende handelsinformation, defineret som en person, der er godkendt efter MiFIR til at udøve virksomhed, der består i at indsamle handelsindberetninger for finansielle instrumenter fra regulerede markeder, MHF'er, OHF'er og APA'er og i at konsolidere disse i form af en kontinuerlig elektronisk live-datastrøm med data om priser og volumen for hvert enkelt finansielt instrument. En CTP kan dog ikke længere være underlagt nationalt tilsyn og er alene reguleret af reglerne i MiFIR.

Det følger af artikel 27 b, stk. 1, i MiFIR, at en APA eller ARM, der er udpeget i overensstemmelse med den i artikel 2, stk. 3, omhandlede delegerede retsakt, og derfor undtaget fra MiFIR, er underlagt krav om forudgående meddelelse af tilladelse og tilsyn fra den relevante nationale kompetente myndighed.

Af artikel 27, stk. 2, i MIFIR følger det, at et investeringsselskab eller en markedsoperatør, der driver en markedsplads, også kan levere APA-, CTP- eller ARM-tjenesteydelser, under forudsætning af, at ESMA eller den relevante nationale kompetente myndighed først har verificeret, at investeringsselskabet eller markedsoperatøren overholder afsnit IVa i MiFIR. Leveringen af de pågældende tjenesteydelser skal være indeholdt i vedkommendes tilladelse. Ved en fejl blev artikel 27 b i MiFIR ikke skrevet ind i § 248 i lov om kapitalmarkeder, da omnibusdirektivet ved § 8 i lov nr. 1163 af 8. juni 2021 blev implementeret. Derfor foreslås bestemmelsen nu indført i § 248, så overtrædelse bliver strafbelagt. For at tydeliggøre, hvilke bestemmelser, som vedrører APA'er og ARM'er, som er underlagt tilsyn fra Finanstilsynet, foreslås det at lade disse bestemmelser udgå af den nugældende § 248 for i stedet at indsætte disse i et nyt 2. pkt. i § 248, herunder artikel 27 b, stk. 1 og 2.

Ansvarssubjektet for overtrædelse af artikel 27, stk. 1, i MIFIR er den fysiske eller juridiske person, der driver en APA eller ARM. Den strafbare handling består i at drive en APA eller en ARM uden den nødvendige tilladelse.

Ansvarssubjektet for overtrædelse af artikel 27, stk. 2, i MIFIR er et investeringsselskab eller en markedsoperatør, der driver en markedsplads, og som leverer dataindberetningsydelser. Den strafbare handling består i at levere dataindberetningsydelser uden at overholde afsnit IVa i MiFIR, som indeholder reglerne for dataindberetningstjenester.

Det følger af § 255, stk. 3, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter 5. kapitel i straffeloven. Af § 27, stk. 1, 1. pkt., i straffeloven fremgår, at strafansvar for en juridisk person forudsætter, at der inden for dens virksomhed er begået en overtrædelse, der kan tilregnes en eller flere til den juridiske person knyttede personer eller den juridiske person som sådan.

I de tilfælde, hvor de strafbelagte bestemmelser omhandler pligter eller forbud for virksomheden, er de mulige ansvarssubjekter virksomheden og/eller en eller flere personer med tilknytning til virksomheden, som oftest medlemmer af ledelsen. Ved valg af ansvarssubjekt rejses tiltalen som udgangspunkt mod den juridiske person. Der kan i nogle tilfælde være anledning til også at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed.

Det følger endvidere af § 255, stk. 5, at der ved udmåling af bøder efter § 248 skal lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold.

Til nr. 21 (§ 251 b og § 251 c i lov om kapitalmarkeder)

Til § 251 b

Det foreslås at indsætte en bestemmelse i § 251 b i lov om kapitalmarkeder.

Bestemmelsen er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter Finanstilsynet er kompetent myndighed til at påse overholdelsen af MiCA.

Det foreslås i *§ 251 b, stk. 1*, at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde overtrædelse af artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9, artikel

76, stk. 3, 4 og 9-15, artikel 88, stk. 1-3, og artikel 92, stk. 1, i Europa-Parlamentets og Rådets forordning nr. 2023/1114 (EU) om markeder for kryptoaktiver og om ændring af forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 og direktiv 2013/36/EU og (EU) 2019/1937.

Det foreslåede vil medføre, at overtrædelse af de oplistede artikler i MiCA, straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Artikel 65, stk. 4, i MiCA omhandler oplysningskrav ved grænseoverskridende levering af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en værdipapircentral påbegynder leveringen af kryptoaktivtjenester i en anden medlemsstat end Danmark inden 15 kalenderdage efter at have indgivet oplysninger efter artikel 65, stk. 1, eller inden at have modtaget meddelelse fra Finanstilsynet efter artikel 65, stk. 2.

Artikel 66, stk. 1-5, i MiCA omhandler udbydere af kryptoaktivtjenesters forpligtelse til at handle ærligt, redeligt og professionelt i kundernes bedste interesse. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en markedsoperatør giver sine kunder vildledende oplysninger.

Artikel 68, stk. 4-9, i MiCA omhandler kravene til ledelsesordninger og indretningen af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af artikel 68, stk. 4, 5 og 7-9, er en værdipapircentral eller markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Ansvarssubjektet for overtrædelse af artikel 68, stk. 6, er ledelsesorganet hos en værdipapircentral eller ledelsesorganet hos en markedsoperatør. Den strafbare handling består eksempelvis i, at en markedsoperatør ikke har vedtaget procedurer, som er tilstrækkelige til at sikre overholdelsen af MiCA. Den strafbare handling kan endvidere bestå i, at ledelsesorganet hos en markedsoperatør ikke regelmæssigt vurderer og evaluerer effektiviteten af den politik og de ordninger og procedurer, der er indført for at opfylde forpligtelserne i artikel 66-83 i MiCA, herunder ikke træffer passende foranstaltninger til at afhjælpe eventuelle mangler.

Artikel 69 i MiCA omhandler krav om at meddele Finanstilsynet eventuelle ændringer i ledelsesorganet hos en markedsoperatør eller værdipapircentral, der udbyder kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af

bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en markedsoperatør ikke giver Finanstilsynet alle oplysninger, som er nødvendige for Finanstilsynets vurdering af overholdelsen af artikel 68 i MiCA inden nye medlemmerne af ledelsesorganet tiltræder deres stilling.

Artikel 71, stk. 1-4, i MiCA fastsætter krav til udbydere af kryptoaktivtjenesters klagebehandlingsprocedurer. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en markedsoperatør kræver betaling af gebyr eller anden afgift i forbindelse med behandling af klager fra sine kunder.

Artikel 72, stk. 2-4, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en markedsoperatør ikke oplyser sine kunder og potentielle kunder om de skridt, som markedsoperatøren har taget for at begrænse interessekonflikter.

Artikel 73, stk. 2 og 3, i MiCA regulerer udbydere af kryptoaktivtjenesters outsourcing af tjenester eller aktiviteter til tredjeparter. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en markedsoperatør ikke træffer alle rimelige foranstaltninger for at undgå yderligere operationel risiko, eller at en markedsoperatør ikke sikrer, at betingelserne i artikel 73, stk. 1, litra a-g, til enhver tid er opfyldt.

Artikel 74 i MiCA omhandler velordnet afvikling af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA, og som udfører de i artikel 75 og 76, i MiCA, beskrevne aktiviteter. Den strafbare handling består eksempelvis i, at den i artikel 74, nævnte plan for velordnet afvikling ikke godtgør, at markedsoperatøren har evnen til at gennemføre en velordnet afvikling uden at påføre sine kunder unødig økonomisk skade.

Artikel 75, stk. 3-6 og 9, i MiCA fastsætter forpligtelser for udbydere af kryptoaktivtjenester, som leverer deponering og administration af

kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral, der udbyder kryptoaktivtjenester efter artikel 60, stk. 2, i MiCA, som udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at værdipapircentralens politik for deponering, som anført i artikel 75, stk. 3, ikke minimerer risikoen for tab af kunders kryptoaktiver som følge af svig, cybertrusler eller forsømmelighed.

Artikel 76, stk. 3, 4 og 9-15, i MiCA fastsætter en række krav til drift af handelsplatforme for kryptoaktiver, herunder krav til indholdet handelsplatformens driftsregler, krav om offentliggørelse af handelsoplysninger, krav vedrørende afvikling af kryptoaktivtransaktioner, mv. Ansvarssubjektet for overtrædelse af bestemmelsen er en markedsoperatør, der udbyder kryptoaktivtjenester efter artikel 60, stk. 6, i MiCA, som driver en handelsplatform for kryptoaktiver. Den strafbare handling består eksempelvis i, at markedsoperatøren, der driver en handelsplatform for kryptoaktiver, ikke offentliggør pris, volumen og tidspunkt for transaktioner, der udføres i forbindelse med kryptoaktiver handlet på deres handelsplatforme.

Artikel 88, stk. 1-3, i MiCA omhandler pligten til at offentliggøre intern viden. Ansvarssubjektet for overtrædelse af bestemmelserne er udstedere, udbydere og personer, der anmoder om optagelse til handel af kryptoaktiver. Den strafbare handling består eksempelvis i, at udbydere af kryptoaktiver ikke offentliggør intern viden som beskrevet i artikel 87 hurtigst muligt.

Artikel 92, stk. 1, i MiCA omhandler forebyggelse og afsløring af markedsmisbrug. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver person, der som led i sit erhverv organiserer eller udfører transaktioner med kryptoaktiver. Den strafbare handling består eksempelvis i, at en virksomhed, som udfører transaktioner med kryptoaktiver, ikke har indført effektive ordninger og procedurer med henblik på at forebygge og afsløre markedsmisbrug, eller at den pågældende virksomhed undlader straks at underrette Finanstilsynet om enhver begrundet mistanke om en ordre eller transaktion.

Den foreslåede bestemmelse supplerer artikel 111, stk. 1, litra 2. afsnit, i MiCA.

Det foreslås i *§ 251 b, stk. 2,* at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 4 måneder overtrædelse af artikel 59, stk. 1, artikel 60, stk. 2 og 6, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, og artikel 76, stk. 1, 2 og 5-8, i

Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslåede vil medføre, at overtrædelse af de oplistede artikler i MiCA straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Artikel 59, stk. 1, i MiCA omhandler tilladelseskrav til at udbyde kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er en markedsoperatør eller en værdipapircentral, der udbyder kryptoaktivtjenester, uden den nødvendige tilladelse. Den strafbare handling består i, at en markedsoperatør eller en værdipapircentral udbyder kryptoaktivtjenester uden at have tilladelse til at levere kryptoaktivtjenester efter artikel 60 i MiCA.

Artikel 60, stk. 2 og 6, i MiCA fastsætter krav om underretning af Finanstilsynet førend en værdipapircentral eller en markedsoperatør kan levere kryptoaktivtjenester. Ansvarssubjektet for overtrædelsen af bestemmelserne er værdipapircentraler og markedsoperatører. Den strafbare handling består eksempelvis i, at en markedsoperatør påbegynder levering af en kryptoaktivtjeneste uden at have underrettet Finanstilsynet med de oplysninger, der er anført i artikel 60, stk. 7, mindst 40 arbejdsdage før markedsoperatøren leverer disse tjenester første gang.

Artikel 70, stk. 1-4, i MiCA omhandler krav vedrørende opbevaring af kundernes kryptoaktiver og midler. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at markedsoperatører, der opbevarer kryptoaktiver på vegne af deres kunder, ikke træffer passende foranstaltninger til at forhindre, at kundernes kryptoaktiver anvendes til handel for deres egen regning.

Artikel 72, stk. 1, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral eller en markedsoperatør, der udbyder kryptoaktivtjenester efter hhv. artikel 60, stk. 2 eller 6, i MiCA. Den strafbare handling består eksempelvis i, at en markedsoperatør ikke opretholder og anvender effektive politikker til at identificere mellem dem selv og personerne opregnet i artikel 72, stk. 1, litra a-e.

Artikel 75, stk. 1, 2 og 7, i MiCA fastsætter specifikke forpligtigelser for udbydere af kryptoaktivtjenester, som leverer deponering og administration

af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er en værdipapircentral, der udbyder kryptoaktivtjenester efter artikel 60, stk. 2, i MiCA, som udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at en værdipapircentral, der leverer deponering og administration af kryptoaktiver på vegne af kunder, ikke holder sine kunders kryptoaktiver adskilt fra sine egne kryptoaktiver.

Artikel 76, stk. 1, 2 og stk. 5-8, i MiCA fastsætter specifikke krav til udbydere af kryptoaktivtjenester, der driver en handelsplatform for kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelserne er en markedsoperatør, der udbyder kryptoaktivtjenester efter artikel 60, stk. 6, i MiCA, der driver en handelsplatform for kryptoaktiver. Den strafbare handling består eksempelvis i, at en markedsoperatør, der driver handelsplatforme, handler for egen regning på den handelsplatform for kryptoaktiver, som den driver.

Den foreslåede bestemmelse supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Det foreslås i *§ 251 b, stk. 3,* at medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 1 år og 6 måneder overtrædelser af artikel 89, stk. 1 og 3, artikel 90, stk. 1, og artikel 91, stk. 1, i MiCA.

Det foreslåede vil medføre, at overtrædelse af artikel 89, stk. 1 og 3, artikel 90, stk. 1, og artikel 91, stk. 1, i MiCA, straffes med bøde eller fængsel indtil 1 år og 6 måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Artikel 89, stk. 1-3, i MiCA omhandler forbuddet mod insiderhandel. Ansvarssubjektet for overtrædelse af bestemmelserne er enhver fysisk eller juridisk person. En fysisk person kan endvidere gøres ansvarlig i det omfang handlingerne er udført på vegne af og til gavn for den juridiske person. Den strafbare handling består eksempelvis i, at en person er kommet i besiddelse af intern viden og benytter denne viden til at enten afhænde eller erhverve kryptoaktiver, som den pågældende viden vedrører.

Artikel 90, stk. 1, i MiCA omhandler forbud mod uretmæssig videregivelse af intern viden. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver fysisk eller juridisk person, som udfører de strafbare handlinger. Den strafbare handling består i uretmæssigt at videregive intern viden.

Artikel 91, stk. 1, i MiCA omhandler forbuddet mod markedsmanipulation. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver fysisk eller

juridisk person, som udfører de strafbare handlinger opregnet i artikel 91, stk. 2 og 3, i MiCA. Den strafbare handling består eksempelvis i at give eller antages at give urigtige eller vildledende signaler om udbuddet af, efterspørgslen efter eller prisen på et kryptoaktiv.

Den foreslåede § 251 b supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Til § 251 c

Det foreslås i *§ 251 c,* at medmindre højere straf er forskyldt efter den øvrige lovgivning straffes med bøde overtrædelse af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede er i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil

have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der operatører af markedspladser, værdipapircentraler (CSD'er), centrale modparter (CCP'er), transaktionsregistre, udbydere af dataindberetningstjenester og administratorer af benchmarks jf. artikel 2, stk. 1, litra i, g, j, h, m r, i DORA-forordningen, medmindre det fremgår specifikt af den uddybende beskrivelse af indholdet af de enkelte artikler, at ansvarssubjektet kun gælder for en bestemt type virksomhed.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet

skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer,

som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test

af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller

dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-

aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem

regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle

ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder

automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold,

der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a.

skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til

resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente

myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed

om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-

relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-

relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres,

dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse

indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier,

fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de

skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter

kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges,

såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig

ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt

den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise

kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 4

Til nr. 1 (fodnoten til lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Det foreslås i *fodnoten* til lov om fondsmæglerselskaber og investeringsservice og -aktiviteter at indsætte en henvisning til, at der med denne lov foretages en gennemførelse af dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at det vil fremgå af fodnoten, at loven implementerer de dele af direktivet, der omfatter fondsmæglerselskaber. Det drejer sig om artikel 6 i direktivet, der fastsætter ændringer til Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter.

Direktivet er et følgedirektiv til DORA-forordningen. Med nærværende lovforslag bliver Finanstilsynet også udpeget som kompetent myndighed efter forordningen til at føre tilsyn med fondsmæglerselskabers overholdelsen af forordningen.

Der henvises til lovforslagets § 4, nr. 10.

Til nr. 2 (§ 13, stk. 2, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Det gældende § 13, stk. 2, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter fastsætter, hvilke aktiviteter et fondsmæglerselskab må udføre. Bestemmelsen indebærer, at fondsmæglerselskaber kun må yde eller udføre investeringsservice og -aktiviteter nævnt i bilag 1, afsnit A, og i tilknytning hertil en eller flere accessoriske tjenesteydelser nævnt i bilag 1, afsnit B, jf. dog §§ 15-16 om muligheden for at yde og udføre investeringsservice og -aktiviteter med visse instrumenter og kontrakter ud over finansielle instrumenter omfattet af MiFID II. Fondsmæglerselskaber kan endvidere under visse betingelser drive anden virksomhed i fællesskab med andre virksomheder, jf. § 31 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.

Afgrænsningen i bestemmelsen indebærer, at et fondsmæglerselskab efter gældende ret ikke må udføre investeringstjenester og -aktiviteter med kryptoaktiver.

Det foreslås i *§ 13, stk. 2*, at ændre »§§ 15 og 16« til: »§ 13, stk. 6, §§ 15 og 16«.

Ændringen er en konsekvens af, at det i artikel 60, stk. 3, i MiCA bestemmes, at et fondsmæglerselskab skal kunne udføre investeringstjenester og -aktiviteter med kryptoaktiver, såfremt betingelserne angivet i bestemmelsen er opfyldt. Der henvises i øvrigt til bemærkningerne til den foreslåede § 13, stk. 6, jf. lovforslagets § 4, nr. 3, der angiver, hvilke kryptoaktivtjenester et fondsmæglerselskab må udbyde efter MiCA.

Den foreslåede bestemmelse vil medføre, at et fondsmæglerselskab fremadrettet kan udbyde kryptoaktivtjenester, hvis det opfylder betingelserne i artikel 60, stk. 3, i MiCA.

Til nr. 3 (§ 13, stk. 6, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Det gældende § 13, stk. 2, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter fastsætter, hvilke aktiviteter et fondsmæglerselskab må udføre. Afgrænsningen i bestemmelsen indebærer, at et fondsmæglerselskab efter gældende ret ikke må udføre investeringstjenester eller accessoriske tjenesteydelser med kryptoaktiver.

Det foreslås i *§ 13, stk. 6*, at et fondsmæglerselskab kan levere tjenester med kryptoaktiver som angivet i artikel 60, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, svarende til de tjenester, som det specifikt er meddelt

tilladelse til i henhold til denne lov, hvis selskabet giver Finanstilsynet meddelelse mindst 40 arbejdsdage, inden disse tjenester leveres første gang. Meddelelsen skal ledsages af de oplysninger, der er omhandlet i artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Ændringen er en konsekvens af, at det i artikel 60, stk. 3, i MiCA bestemmes, at et fondsmæglerselskab skal kunne udføre disse aktiviteter, såfremt betingelserne angivet i bestemmelsen er opfyldt. Artikel 60, stk. 3, i MiCA benævner investeringsselskaber. Begrebet investeringsselskab er i dansk ret implementeret som fondsmæglerselskab, hvis det har hjemsted i Danmark.

Den foreslåede bestemmelse vil medføre, at et fondsmæglerselskab fremadrettet kan levere kryptoaktivtjenester som nævnt i artikel 60, stk. 3, i MiCA, såfremt det giver Finanstilsynet meddelelse i henhold til artikel 60, stk. 7, i MiCA.

Et fondsmæglerselskab er ikke forpligtet til selvstændigt at ansøge om tilladelse til at udbyde kryptoaktivtjenester, jf. artikel 59, stk. 1, litra b, i MiCA.

Den foreslåede bestemmelse fastlægger, at Finanstilsynet er kompetent myndighed til at vurdere en meddelelse indgivet af et fondsmæglerselskab i henhold til artikel 60, stk. 7, jf. artikel 60, stk. 8, i MiCA.

Et fondsmæglerselskab må ikke begynde at levere kryptoaktivtjenester, så længe meddelelsen er ufuldstændig.

Retten til at levere kryptoaktivtjenester ophæves ved inddragelsen af den tilladelse, der gav et fondsmæglerselskab mulighed for at levere kryptoaktivtjenester, uden at skulle indhente en tilladelse i henhold til artikel 59, jf. artikel 60, stk. 11, i MiCA. Der henvises i øvrigt til bemærkningerne til lovforslagets § 4, nr. 4, der beskriver, at Finanstilsynet kan inddrage en virksomheds tilladelse som fondsmæglerselskab i en række situationer.

Bestemmelsen supplerer artikel 60, stk. 3, i MiCA.

Til nr. 4 (§ 95, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Det fremgår af § 95, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, at et fondsmæglerselskab skal træffe de nødvendige forholdsregler for at sikre sammenhæng og regelmæssighed i

sin virksomhed som værdipapirhandler og anvende ressourcer, systemer og procedurer, der er hensigtsmæssige hertil.

§ 95, stk. 1, gennemfører artikel 16, stk. 4, i Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter (MiFID II).

Det foreslås, at nyaffatte *§ 95, stk. 1*, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, så det følger, at et fondsmæglerselskab inden for rimelighedens grænser skal, træffe de foranstaltninger, som er nødvendige for at sikre kontinuitet og regelmæssighed i ydelsen af investeringsservice og udførelsen af investeringsaktiviteter. Fondsmæglerselskabet skal med henblik herpå anvende hensigtsmæssige og forholdsmæssigt afpassede systemer, herunder it-systemer, som oprettes og styres i overensstemmelse med artikel 7 i Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor, samt hensigtsmæssige og forholdsmæssigt afpassede ressourcer og procedurer.

Bestemmelsen foreslås som følge af, at artikel 6, nr. 1, litra a, i Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, nyaffatter artikel 16, stk. 4, i MiFID II. Med ændringen af § 95, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter foreslås en direktivnær implementering af den nye artikel 16, stk. 4, i MiFID II.

Bestemmelsen vil fortsat indebære, at fondsmæglerselskaber i tillæg til kravene til effektive former for virksomhedsstyring, jf. § 94, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, skal træffe de nødvendige forholdsregler for at sikre sammenhæng og regelmæssighed i sin virksomhed som værdipapirhandler og anvende ressourcer, systemer og procedurer, der er hensigtsmæssige hertil. Det vil dog fremover også følge af bestemmelsen, at fondsmæglerselskabers it-systemer skal oprettes og styres i overensstemmelse med artikel 7 i DORA-forordningen.

Artikel 7 i DORA-forordningen indeholder bl.a. regler om anvendelsen og vedligeholdelsen af opdaterede it-systemer, som et fondsmæglerselskab, skal have for at håndtere og styre it-risici.

Overtrædelse af § 95, stk. 1, kan straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning, jf. § 266, stk. 1, nr. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter. Ansvarssubjektet i forhold til overtrædelse af § 95, stk. 1, er et fondsmæglerselskab. Det betyder, at hvis et fondsmæglerselskab ikke træffer de nødvendige forholds- regler for at sikre sammenhæng og

regelmæssighed i sin virksomhed som værdipapirhandler og anvender ressourcer, systemer og procedurer, der er hensigtsmæssige hertil og her de regler og procedurer, kan fondsmæglerselskabet straffes med bøde. Med den foreslåede ændring vil et fondsmæglerselskab også kunne straffes med bøde, hvis fondsmæglerselskabet ikke har it-systemer i overensstemmelse med artikel 7 i DORA-forordningen.

Til nr. 5 (§ 164, stk. 1, nr. 1, litra f, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 164, stk. 1, nr. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, fastlægger, i hvilke tilfælde Finanstilsynet kan inddrage et fondsmæglerselskabs tilladelse.

Det foreslås at indsætte et *litra f* i *§ 164, stk. 1, nr. 1*, hvorefter Finanstilsynet kan inddrage et fondsmæglerselskabs tilladelse i tilfælde af grove eller gentagne overtrædelser af MiCA.

Det foreslåede vil medføre, at Finanstilsynet kan inddrage et fondsmæglerselskabs tilladelse som fondsmæglerselskab i tilfælde af, at fondsmæglerselskabet gør sig skyldig i grove eller gentagne overtrædelser af MiCA.

Den foreslåede bestemmelse indebærer, at der skal være tale om grove eller gentagne overtrædelser af MiCA. Det forudsættes som udgangspunkt, jf. også forvaltningsretlige principper, at en mindre indgribende reaktion er anvendt over for fondsmæglerselskabet, før Finanstilsynet inddrager fondsmæglerselskabets tilladelse i medfør af bestemmelsen, eller at forholdene i fondsmæglerselskabet indebærer, at fondsmæglerselskabet ikke har mulighed for at rette op på overtrædelserne inden for en tilpas kort tidshorisont. Kan forholdene i fondsmæglerselskabet rettes op ved en mindre indgribende reaktion end at inddrage fondsmæglerselskabets tilladelse, skal den mindre reaktion vælges. En mildere reaktion kan bl.a. være, at Finanstilsynet giver påbud om, at fondsmæglerselskabet retter op på de kritisable forhold i fondsmæglerselskabet eller at forholdet anmeldes til politiet.

Bestemmelsen vil eksempelvis, efter en konkret vurdering, kunne finde anvendelse i tilfælde, hvor et fondsmæglerselskab bevidst systematisk udfører kryptoaktivtjenester, som fondsmæglerselskabet ikke har tilladelse til i henhold til MiCA, eller som fondsmæglerselskabet ikke ville kunne opnå tilladelse til, og som indebærer risiko for kunder, investorer og andre interessenter. Bestemmelsen vil tilsvarende, efter en konkret vurdering, kunne finde anvendelse i tilfælde, hvor et fondsmæglerselskab udfører sin

virksomhed på en groft uforsvarlig måde og i gentagen strid med relevant lovgivning samt kunders, investorers og øvriges interesser.

Til nr. 6 (§ 214, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 214, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter fastsætter, at Finanstilsynet uden ugrundet ophold skal nedskrive eller konvertere hybride kapitalinstrumenter og supplerende kapitalinstrumenter, som opfylder kravene i artikel 9, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) nr. 2019/2033 af 27. november 2019 om tilsynsmæssige krav til investeringsselskaber, i et fondsmæglerselskab, der har tilladelse til at yde eller udføre en eller begge af de i bilag 1, afsnit A, nr. 3 og 6, nævnte investeringsservicer og -aktiviteter, til egentlige kernekapitalinstrumenter. Det samme gælder for nedskrivningsegnede forpligtelser, som opfylder betingelserne i § 205, nr. 4, uanset om forpligtelserne opfylder betingelsen i § 205, nr. 4, litra b, om en restløbetid på mindst 1 år.

Bestemmelsen implementerer artikel 59, stk. 3, litra b, i BRRD.

Bestemmelsen er endvidere en videreførelse af § 272 i lov om finansiel virksomhed for så vidt angår fondsmæglerselskaber, der har tilladelse til at yde eller udføre en eller begge af de i bilag 1, afsnit A, nr. 3 og 6, nævnte investeringsservice og -aktiviteter. Der var ved videreførelsen ikke tilsigtet materielle ændringer i forhold til § 272 i lov om finansiel virksomhed.

Det fremgår imidlertid ikke af den gældende § 214, stk. 1, under hvilke betingelser nedskrivningen eller konverteringen skal ske, i modsætning til § 272, stk. 1, i lov om finansiel virksomhed og artikel 59, stk. 3, litra b, i BRRD.

Det foreslås derfor at ændre *§ 214, stk. 1, 1. pkt.*, således at efter »egentlige kernekapitalinstrumenter« indsættes: »hvis Finanstilsynet vurderer, at fondsmæglerselskabet ikke vil være levedygtigt, medmindre beføjelsen anvendes«.

Det foreslåede medfører i overensstemmelse med artikel 59, stk. 3, litra b, i BRRD, at det er en betingelse for anvendelse af Finanstilsynets beføjelse om nedskrivning eller konvertering, at Finanstilsynet skal vurdere, at den pågældende virksomhed ikke vil være levedygtig, medmindre beføjelsen til nedskrivning eller konvertering anvendes. Denne betingelse fremgår også af de specielle bemærkninger til den gældende § 214, stk. 1, jf.

Folketingstidende 2020-21, Tillæg A, L 207 som fremsat, side 497, ligesom § 214, stk. 2, forudsætter, at § 214, stk. 1, indeholder betingelsen.

Den foreslåede bestemmelse vil medføre at der skabes klarhed om anvendelsesområdet for Finanstilsynets nedskrivnings- og konverteringsbeføjelser for fondsmæglerselskaber.

Til nr. 7 (§ 214, stk. 8 og 9, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Det foreslås i *§ 214, stk. 8,* at kapitalejere og kreditorer, hvis krav er blevet nedskrevet eller konverteret i henhold til § 272, stk. 1, ikke må lide større tab end ved konkursbehandling af fondsmæglerselskabet.

Det foreslås i *§ 214, stk. 9,* at Finanstilsynets vurdering efter stk. 8 foretages på baggrund af værdiansættelsen i § 8 i lov om restrukturering og afvikling af visse finansielle virksomheder. Værdiansættelsen foretages af Finansiel Stabilitet efter anmodning fra Finanstilsynet. Konstateres det, at en kapitalejer eller kreditor, herunder Garantiformuen, har lidt større tab, end den ville have gjort ved konkursbehandling af fondsmæglerselskabet, betales forskellen af Afviklingsformuen.

De foreslåede bestemmelser er nye og skal implementere artikel 59, stk. 1, 3. afsnit, i BRRD for så vidt angår Finanstilsynets nedskrivnings- og konverteringsbeføjelser, jf. § 272, stk. 1.

Princippet om, at ingen kreditorer eller aktionærer må stilles økonomisk værre i afvikling, end hvis der var tale om en konkurssituation (det såkaldte no-creditor-worse-off-princip) er et afgørende princip i krisehåndtering. Bestemmelsen sikrer, at princippet overholdes ved Finanstilsynets nedskrivning eller konvertering i henhold til § 214, stk. 1, på samme måde som det allerede er tilfældet for isolerede nedskrivninger eller konverteringer, som foretages af Finansiel Stabilitet uden for afviklingssituationer efter § 18 a i lov om restrukturering og afvikling af visse finansielle virksomheder.

Til nr. 8 (§ 216, stk. 3, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Efter den gældende § 216, stk. 3, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter finder kravet om kontraktmæssig anerkendelse af bail-in, jf. § 216, stk. 1, ikke anvendelse, hvis forpligtelsen er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder, eller hvis forpligtelsen er et berettiget

indskud, jf. § 2, nr. 7, i lov om restrukturering og afvikling af visse finansielle virksomheder.

Det bemærkes, at henvisningen til § 2, nr. 7, med rette bør være en henvisning til § 2, nr. 5.

§ 217, stk. 3, har til hensigt at implementere artikel 55, stk. 1, 1. afsnit, i BRRD, jf. Folketingstidende 2020-21, tillæg A, L 207 som fremsat, side 501.

Bestemmelsen er endvidere en videreførelse af § 274 i lov om finansiel virksomhed for så vidt angår fondsmæglerselskaber, der har tilladelse til at yde eller udføre en eller begge af de i bilag 1, afsnit A, nr. 3 og 6, nævnte investeringsservice og -aktiviteter. Der var ved videreførelsen ikke tilsigtet materielle ændringer i forhold til § 274 i lov om finansiel virksomhed.

Bestemmelsen omfatter imidlertid alle berettigede indskud, mens artikel 55, stk. 1, 1. afsnit, litra b, i BRRD alene omfatter indskud som omhandlet i BRRD artikel 108, litra a.

Det foreslås derfor at nyaffate *§ 273, stk. 3*, således, at stk. 1 ikke finder anvendelse, hvis 1) forpligtelsen er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder, eller 2) forpligtelsen er en del af et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, jf. § 2, nr. 19, i lov om restrukturering og afvikling af visse finansielle virksomheder, og overstiger beløbsgrænsen for dækkede indskud, jf. § 9 i lov om en indskyder- og investorgarantiordning, eller 3) forpligtelsen ville være et berettiget indskud fra fysiske personer eller mikrovirksomheder, små eller mellemstore virksomheder, hvis ikke det var foretaget gennem filialer af institutter, der er etableret inden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område, når filialen er beliggende uden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område

Den foreslåede ændring vil indskrænke undtagelsen for så vidt angår berettigede indskud, således at den fremover alene vil gælde den del af berettigede indskud fra fysiske personer, mikrovirksomheder eller små eller mellemstore virksomheder, som defineret i § 2, nr. 19, i lov om restrukturering og afvikling af visse finansielle virksomheder, som overstiger beløbsgrænsen for dækkede indskud, jf. § 9 i lov om en indskyder- og investorgarantiordning.

Det foreslåede vil ligeledes medføre, at undtagelsen gælder forpligtelser,

som ville være berettigede indskud fra samme kreds af fysiske personer og virksomheder, hvis de ikke var foretaget gennem filialer af institutter, der er etableret inden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område, når filialen er beliggende uden for Den Europæiske Union eller i et land, som Unionen har indgået aftale med på det finansielle område.

Den foreslåede ændring har til formål at bringe undtagelsen om anerkendelse af kontraktmæssig bail-in i § 274, stk. 1, i overensstemmelse med artikel 55, stk. 1, 1. afsnit, litra b, i BRRD.

Forpligtelser, der er undtaget fra bail-in, kan ikke nedskrives eller konverteres. På den baggrund gælder kravet i stk. 1 ikke kontrakter vedrørende disse forpligtelser.

Berettigede indskud er indestående beløb på en konto i et pengeinstitut m.v., som ikke er udelukket fra dækning efter § 13 i lov om en indskyder- og investorgarantiordning. Dækkede indskud, jf. §§ 9 og 10 i lov om en indskyder- og investorgarantiordning, udgør den del af det berettigede indskud, som er dækket af Garantiformuen. Definitionen af dækkede indskud følger af bemærkningerne til § 7, stk. 8, i lov om en indskyder- og investorgarantiordning, jf. Folketingstidende 2014-15, tillæg A, L 105 som fremsat, side 112. Den tidligere gældende henvisning til § 2, nr. 5, i lov om restrukturering af visse finansielle virksomheder, som rettelig skulle have været til § 2, nr. 7, er udeladt i den foreslåede bestemmelse, idet bestemmelsen henviser til den nævnte § 7, stk. 8, i lov om en indskyder- og investorgarantiordning, som ikke i sig selv definerer dækkede indskud. Med lovforslaget indsættes derfor en mere præcis henvisning til dækkede indskud. Der er ikke tilsigtet nogen materiel ændring på dette punkt.

Det dækkede indskud kan være mindre end det berettigede indskud som følge af de fastsatte maksimumsgrænser for dækning. Dækkede indskud er undtaget fra bail-in, jf. § 25, stk. 3, i lov om restrukturering og afvikling af visse finansielle virksomheder.

Til nr. 9 (§ 217, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Efter § 217, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter skal en virksomhed underrette Finanstilsynet, hvis det ikke er muligt at opfylde § 216, stk. 1, om kontraktmæssig anerkendelse af bail-in, i forhold til en kontrakt vedrørende en forpligtelse omfattet af konkurslovens § 97. Underretningen skal angive kategorien af forpligtelsen og begrundelsen for, at det ikke er muligt at indføre kontraktbestemmelsen.

Bestemmelsen implementerer artikel 55, stk. 2, 1. afsnit, 1. pkt., og stk. 2, 4. afsnit, i BRRD, jf. Folketingstidende 2020-21, tillæg A, L 207 som fremsat, side 504.

Bestemmelsen er endvidere en videreførelse af § 275 i lov om finansiel virksomhed for så vidt angår fondsmæglerselskaber, der har tilladelse til at yde eller udføre en eller begge af de i bilag 1, afsnit A, nr. 3 og 6, nævnte investeringsservice og -aktiviteter. Der er ikke tilsigtet materielle ændringer i forhold til § 275 i lov om finansiel virksomhed.

Ifølge artikel 55, stk. 2, 4. afsnit, i BRRD, finder bestemmelsen ikke anvendelse på passiver en række forpligtelser, hvis disse indeholder hybride kernekapitalinstrumenter, supplerende kapitalinstrumenter og gældsinstrumenter som omhandlet i artikel 2, stk. 1, nr. 48, nr. ii, hvis disse instrumenter er usikrede passiver.

§ 217, stk. 1, henviser til konkurslovens § 97, som omhandler simple krav, f.eks. almindelige fakturakrav for indkøb af varer og tjenesteydelser. Det er ifølge bemærkningerne til § 275, stk. 1, hensigten, at bestemmelsen alene skal finde anvendelse på sådanne forpligtelser. Hybride kernekapitalinstrumenter og supplerende kapitalinstrumenter er efterstillet simple krav, som er omfattet af konkurslovens § 97, hvorfor de er udelukket fra bestemmelsens anvendelsesområde. For så vidt angår gældsinstrumenter som omhandlet i artikel 2, stk. 1, nr. 48, nr. ii, defineres disse som obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld. Sådanne instrumenter vil, hvis de er omfattet af konkurslovens § 97, definitorisk være usikrede. Indehavere af fordringer med sikkerhed i pant vil således kunne søge fyldestgørelse i pantet ved debitors betalingsmisligholdelse. Dermed har indehaverne ikke i udgangspunktet et krav efter konkurslovens § 97. Den nuværende formulering af § 217, stk. 1, indebærer således, at usikrede gældsinstrumenter vil kunne undtages fra kravet om kontraktmæssig anerkendelse af bail-in.

Det foreslås derfor i *§ 217, stk. 1,* efter »konkurslovens § 97«: at indsætte », med undtagelse af usikrede obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld«.

Det foreslåede vil indskrænke anvendelsesområdet for § 217, stk. 1, til forpligtelser omfattet af konkurslovens § 97, som ikke er usikrede obligationer og andre former for omsættelig gæld og instrumenter, der skaber eller anerkender en gæld.

Den foreslåede bestemmelse har til formål at bringe undtagelsen i § 275, stk. 1, i overensstemmelse med artikel 55, stk. 2, 4. afsnit i BRRD.

Til nr. 10 (§ 219, stk. 2, nr. 12, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 219, stk. 2, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter fastlægger Finanstilsynets forpligtelse til at påse overholdelsen af en række europæiske retsakter. Det indebærer, at Finanstilsynet kan give påtaler, påbud, m.v. for overtrædelse af de oplistede retsakter.

Det foreslås i *§ 219, stk. 2,* at indsætte *nr. 12,* hvorefter Finanstilsynet påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf.

Det foreslås i *§ 291, stk. 2,* at indsætte *nr. 13,* hvorefter Finanstilsynet påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.

De foreslåede ændringer vil medføre, at Finanstilsynet bliver udpeget som kompetent myndighed efter DORA-forordningen og MiCA til at føre tilsyn med overholdelsen af forordningernes bestemmelser og regler udstedt i medfør af forordningerne.

Finanstilsynet får med de foreslåede nr. 12 og 13 bl.a. også mulighed for at give påbud og påtaler for overtrædelser af forordningen, jf. § 219 og mulighed for at offentliggøre påbud og påtaler til en virksomhed eller en fysisk person, jf. § 279. Se nærmere om Finanstilsynets mulighed for offentliggørelse af reaktioner i medfør af lov om fondsmæglerselskaber og investeringsservice og -aktiviteter i bemærkningerne til §§ 277-286, jf. Folketingstidende 2020-21, tillæg A, L 207 som fremsat, side 590-599.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningerne, jf. § 232 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter.

DORA-forordningen finder bl.a. anvendelse på investeringsselskaber, jf. artikel 2, stk. 1, litra e.

Efter artikel 46, litra c, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets direktiv (EU) 2019/2034 af 27. november 2019 om tilsyn med investeringsselskaber sikre overholdelsen af DORA-forordningen for investeringsselskaber.

Bestemmelsen supplerer artikel 46, litra c, i DORA-forordningen.

Det foreslåede vil medføre, at Finanstilsynet udpeges i henhold til artikel 93, stk. 1, i MiCA, som den kompetente myndighed, der er ansvarlig for at udføre de i MiCA fastsatte funktioner og opgaver.

Kommissionen er i medfør af MiCA bemyndiget til at udstede reguleringsmæssige tekniske standarder, som Finanstilsynet i medfør af den foreslåede bestemmelse også skal føre tilsyn med.

Til nr. 11 (§ 257, stk. 1, nr. 14, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

I medfør af § 255, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter er Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger, som de får kendskab til gennem tilsynsvirksomheden.

§ 257, stk. 1, er en undtagelse til tavshedspligten i § 255, stk. 1. Bestemmelsen fastsætter i hvilke tilfælde, der ikke er noget til hinder for, at fortrolige oplysninger videregives til en række institutioner, myndigheder og organer mv. i et andet EU/EØS-land mv.

I medfør af § 257, stk. 1, har Finanstilsynet ikke mulighed for at videregive oplysninger til Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 257, stk. 1,* at indsætte *nr. 14,* hvorefter Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større IKT-relateret hændelse fra et fondsmæglerselskab, jf. artikel 19, stk. 1, 1. pkt., i DORA-

forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 12 (§ 259, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 259, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter nævner de virksomheder, der kan anses som part i forhold til Finanstilsynet i sager, hvor Finanstilsynet har truffet eller vil træffe afgørelse over for den pågældende i medfør af bl.a. lov om fondsmæglerselskaber og investeringsservice og -aktiviteter og andre relevante forordninger.

Det foreslås at ændre *§ 259, stk. 1,* således, at der indgår en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023

om markeder for kryptoaktiver og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at virksomheder, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af DORA-forordningen eller regler udstedt i medfør heraf, også vil være at anse som parter i afgørelsessagen.

Til nr. 13 (§ 266, stk. 1, nr. 5, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 266, stk. 1, fastsætter, hvilke bestemmelser der kan straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås at indsætte nyt *§ 266, stk. 1, nr. 5,* hvorefter artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, artikel 74, artikel 75, stk. 3-6 og 9, artikel 76, stk. 3, 4 og 9-15, artikel 77, artikel 78, artikel 79, artikel 80, stk. 1-3, artikel 81, stk. 1-14, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver kan straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslåede vil medføre, at overtrædelse af de oplistede artikler i MiCA, straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Artikel 65, stk. 4, i MiCA omhandler oplysningskrav ved grænseoverskridende levering af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA. Den strafbare handling består i, at et fondsmæglerselskab påbegynder leveringen af kryptoaktivtjenester i en anden medlemsstat end Danmark inden 15 kalenderdage efter at have indgivet de oplysninger, der er omhandlet i artikel 65, stk. 1, eller inden at have modtaget den i artikel 65, stk. 2, omtalte meddelelse fra Finanstilsynet.

Artikel 66, stk. 1-5, i MiCA omhandler udbydere af kryptoaktivtjenesters forpligtelse til at handle ærligt, redeligt og professionelt i kundernes bedste interesse. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk.

3, i MiCA. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab giver sine kunder vildledende oplysninger.

Artikel 68, stk. 4-9, i MiCA omhandler kravene til ledelsesordninger og indretningen af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af artikel 68, stk. 4, 5 og 7-9, er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA. Ansvarssubjektet for overtrædelse af artikel 68, stk. 6, er ledelsesorganet hos fondsmæglerselskabet. Den strafbare handling består eksempelvis i, at fondsmæglerselskabet ikke har vedtaget procedure, som er tilstrækkelige til at sikre overholdelsen af MiCA. Det strafbare forhold kan endvidere bestå i, at ledelsesorganer hos fondsmæglerskabet ikke regelmæssigt vurderer og evaluerer effektiviteten af den politik og de ordninger og procedurer, der er indført for at opfylde forpligtelserne i artikel 66-83 i MiCA, eller træffer passende foranstaltninger til at afhjælpe eventuelle mangler.

Artikel 69 i MiCA omhandler krav til meddelelse af Finanstilsynet om eventuelle ændringer i ledelsesorganet i udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA. Den strafbare handling består eksempelvis i, at fondsmæglerselskabet ikke giver Finanstilsynet alle oplysninger, som er nødvendige for Finanstilsynets vurdering af overholdelsen af artikel 68 i MiCA, inden nye medlemmerne af ledelsesorganet tiltræder deres stilling.

Artikel 71, stk. 1-4, i MiCA fastsætter krav til udbydere af kryptoaktivtjenesters klagebehandlingsprocedurer. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA. Den strafbare handling består eksempelvis i, at fondsmæglerselskaber kræver betaling af gebyr eller anden afgift i forbindelse med behandling af klager fra deres kunder.

Artikel 72, stk. 2-4, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA. Den strafbare handling består eksempelvis i, at fondsmæglerselskaber ikke oplyser deres kunder og potentielle kunder, om de skridt udbyderen har taget for at begrænse interessekonflikter.

Artikel 73, stk. 2 og 3, i MiCA regulerer udbydere af kryptoaktivtjenesters outsourcing af tjenester eller aktiviteter til tredjeparter. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA. Den strafbare handling

består eksempelvis i, at fondsmæglerselskaber ikke træffer alle rimelige foranstaltninger for at undgå yderligere operationel risiko, eller at fondsmæglerselskaber ikke sikrer, at betingelserne i artikel 73, stk. 1, litra a-g, til enhver tid er opfyldt.

Artikel 74, i MiCA omhandler velordnet afvikling af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester efter artikel 60, stk. 3, i MiCA, som udfører de i artikel 75-79 i MiCA beskrevne aktiviteter. Den strafbare handling består eksempelvis i, at den i artikel 74 nævnte plan for velordnet afvikling ikke godtgør, at fondsmæglerselskabet har evnen til at gennemføre en velordnet afvikling uden at påføre sine kunder unødig økonomisk skade.

Artikel 75, stk. 3-6 og 9, i MiCA fastsætter forpligtelser for udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at fondsmæglerselskabets politik for deponering, som anført i artikel 75, stk. 3, ikke minimerer risikoen for tab af kunders kryptoaktiver som følge af svig, cybertrusler eller forsømmelighed.

Artikel 76, stk. 3, 4 og 9-15, i MiCA fastsætter en række krav til drift af handelsplatforme for kryptoaktiver, herunder krav til indholdet af handelsplatformens driftsregler, krav om offentliggørelse af handelsoplysninger, krav vedrørende afvikling af kryptoaktivtransaktioner, mv. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der driver en handelsplatform for kryptoaktiver. Den strafbare handling består eksempelvis i, at fondsmæglerselskaber, der driver en handelsplatform for kryptoaktiver, ikke offentliggør pris, volumen og tidspunkt for de transaktioner, der udføres i forbindelse med kryptoaktiver handlet på deres handelsplatforme.

Artikel 77 i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der veksler mellem kryptoaktiver og midler eller andre kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der veksler mellem kryptoaktiver og midler eller andre kryptoaktiver. Den strafbare handling består eksempelvis i, at fondsmæglerselskabet ikke udfører kundernes ordrer til de viste priser på det tidspunkt, hvor ordren vedrørende veksling var endelig.

Artikel 78 i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der udfører ordrer vedrørende kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udfører ordrer vedrørende kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at fondsmæglerselskabet ikke har udarbejdet og gennemført en politik for ordreudførelse, der sikrer at fondsmæglerselskabet er i stand til at opnå det bedst mulige resultat i forbindelse med kundeordrer.

Artikel 79 i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der placerer kryptoaktiver, om at underrette udbydere af kryptoaktiver, personer, der anmoder om optagelse til handel af kryptoaktiver, eller enhver tredjepart, der handler på dennes vegne om de oplysninger, som fremgår af artikel 79, stk. 1, litra a-d. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der placerer kryptoaktiver. Placering af kryptoaktiver er defineret i artikel 3, stk. 1, nr. 21, i MiCA. Den strafbare handling består eksempelvis i, at fondsmæglerselskaber, der placerer kryptoaktiver, ikke underretter en udbyder af kryptoaktiver om oplysningerne i artikel 79, stk. 1, litra a-d, inden der indgås kontrakt om placering af kryptoaktiver.

Artikel 80, stk. 1-3, i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der modtager og formidler ordrer vedrørende kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der modtager og formidler ordrer vedrørende kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab, der modtager og formidler ordrer, ikke indfører procedurer og ordninger, der sikrer hurtig og korrekt formidling af kunders ordrer til udførelse på en handelsplatform for kryptoaktiver.

Artikel 81, stk. 1-14, i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der yder rådgivning om kryptoaktiver og udbyder af kryptoaktivtjenester, som yder porteføljepleje af kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der yder rådgivning om kryptoaktiver og udbyder porteføljepleje af kryptoaktiver. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab, der yder rådgivning om kryptoaktiver eller porteføljepleje af kryptoaktiver, undlader at advare sine kunder eller potentielle kunder om de forhold, som er oplistet i artikel 81, stk. 9, litra a-f.

Den foreslåede bestemmelse supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Til nr. 14 (§ 266, stk. 2, nr. 4 og 5, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 266, stk. 2, fastsætter, hvilke bestemmelser der kan straffes med bøde eller fængsel indtil fire måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås at indsætte nyt *§ 266, stk. 2, nr. 4*, hvorefter Artikel 59, stk. 1, artikel 60, stk. 3, artikel 70, stk. 1-4, artikel 72, stk. 1, artikel 75, stk. 1, 2 og 7, artikel 76, stk. 1, 2 og 5-8, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver kan straffes med bøde eller fængsel indtil fire måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslåede vil medføre, at overtrædelse af de oplistede artikler i MiCA, straffes med bøde eller fængsel indtil fire måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024.

Artikel 59, stk. 1, i MiCA omhandler tilladelseskrav til at udbyde kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester uden den nødvendige tilladelse. Den strafbare handling består i at et fondsmæglerselskab udbyder kryptoaktivtjenester uden at have tilladelse til at levere kryptoaktivtjenester efter artikel 60 i MiCA.

Artikel 60, stk. 3, i MiCA fastsætter krav om underretning af Finanstilsynet, førend fondsmæglerselskaber kan levere kryptoaktivtjenester. Ansvarssubjektet for overtrædelsen af bestemmelserne er et fondsmæglerselskab. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab påbegynder levering af en kryptoaktivtjeneste, uden at have underrettet Finanstilsynet med de oplysninger, der er anført i artikel 60, stk. 7, mindst 40 arbejdsdage inden fondsmæglerselskabet leverer disse tjenester første gang.

Artikel 70, stk. 1-4, i MiCA omhandler krav vedrørende opbevaring af kundernes kryptoaktiver og midler. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab opbevarer kryptoaktiver på vegne af deres kunder, uden at træffe passende foranstaltninger til at forhindre, at kundernes kryptoaktiver anvendes til handel for deres egen regning.

Artikel 72, stk. 1, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder kryptoaktivtjenester. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab ikke opretholder og anvender effektive politikker til at identificere mellem dem selv og personerne opregnet i artikel 72, stk. 1, litra a-e.

Artikel 75, stk. 1, 2 og 7, i MiCA omhandler specifikke forpligtigelser for udbydere af kryptoaktivtjenester, som leverer deponering og administration af kryptoaktiver på vegne af kunder. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der udbyder levering af deponering og administration af kryptoaktiver på vegne af kunder. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab, der leverer deponering og administration af kryptoaktiver på vegne af kunder, ikke holder sine kunders kryptoaktiver adskilt fra sine egne kryptoaktiver.

Artikel 76, stk. 1, 2 og 5-8, i MiCA fastsætter specifikke krav til udbydere af kryptoaktivtjenester, der driver en handelsplatform for kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelsen er et fondsmæglerselskab, der driver en handelsplatform for kryptoaktiver. Den strafbare handling består eksempelvis i, at et fondsmæglerselskab, der driver handelsplatforme for kryptoaktiver, handler for egen regning på den handelsplatform for kryptoaktiver, som den driver.

Bestemmelsen supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Det foreslås at indsætte *§ 266, stk. 2, nr. 5,* i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, hvorefter overtrædelser af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-4, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1 og 2, stk. 3, 1. og 2. pkt., stk. 4, 6 og 7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26, stk. 1, stk. 2, stk. 3, stk. 5, stk. 6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) straffes med bøde.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for

overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der fondsmæglerselskaber, jf. artikel 2, stk. 1, litra e, jf. artikel 2, stk. 2, i DORA-forordningen,

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne

kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er en finansiel enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i en finansiel enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at den finansielle enhed indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten,
integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er en finansiel enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at en finansiel enhed skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er et fondsmæglerselskab. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er et fondsmæglerselskab

Den strafbare handling kan eksempelvis bestå i, at den en finansiel enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet i en finansiel enhed. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den en finansiel enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler en finansiel enheds forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er en finansiel enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at en finansiel enhed skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er en finansiel enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er en finansiel enhed. En strafbar overtrædelse kan eksempelvis bestå i, at en finansiel enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at den finansielle enhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. Den finansielle enhed skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er en finansiel enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at den finansielle enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at en finansiel enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er en finansiel enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er en finansiel enhed. En strafbar overtrædelse består eksempelvis i, at den finansielle enhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -

procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre den finansielle enhed.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal den finansielle enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig

forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at den finansielle enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal en finansiel enhedet gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at den finansielle enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer den finansielle enhed infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og

efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er en finansiel enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at fondsmæglerselskaber skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den en finansiel enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er en finansiel enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at den finansielle enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er en finansiel enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at den finansielle enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er en finansiel enhed. Den strafbare handling består i at den finansielle enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer

for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal den finansielle enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for fondsmæglerselskaber, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at den finansielle enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er en finansiel enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at er fondsmæglerselskab som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og

informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og

funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er en finansiel enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er en finansiel enhed. Den strafbare handling består i, at den finansielle enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når den finansielle enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er en finansiel enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrren finansiel enhedets kerneaktivitet. Er der eksempelvis tale om et pengeinstitut, kan en kerneaktivitet være muligheden for at udstede lån til kunder. En gennemgang og en analyse af en it-relateret hændelse har til formål at mindske risikoen for, at en lignende hændelse opstår igen.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til

Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at den finansielle enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, hvad den finansielle enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle nehed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig

cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at den finansielle enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at den finansielle enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i at den finansielle enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at den finansielle enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at den finansielle enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at den finansielle enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også

bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at den finansielle enhed sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1 er en finansiel enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal den finansielle enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at den finansielle enhed indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er en finansiel enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som

til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at den finansielle enhed skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f), samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er en finansiel enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal den finansielle enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er en finansiel enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er en finansiel enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at den finansielle enhed definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1, bestå i, at den finansielle enhed ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at fondsmæglerselskaber er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. Den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende

procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at den finansielle enhed klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er en finansiel enhed. Den strafbare består i, at den finansielle enhed ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at den finansielle enhed klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er en finansiel enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter den finansielle enhed, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er en finansiel enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er en finansiel enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at den finansielle enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.

I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er en finansiel enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad

omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som det berørte fondsmæglerselskab udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er en finansiel enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er en finansiel enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal den finansielle enhed sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1, omhandlede test ved at kombinere en risikobaseret tilgang

med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er en finansiel enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien

skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enhed samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både fondsmæglerselskaber på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme

tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består i, at den finansielle enhed har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke

er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i den finansielle enheds programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem den finansielle enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at

migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhedet. Den strafbare handling består eksempelvis i, at den finansielle enhed ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til nr. 15 (§ 275, stk. 1, nr. 8 og 9, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 275, stk. 1, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter, indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet eller Erhvervsstyrelsen retter sig til. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet eller Erhvervsstyrelsen i henhold til lov om fondsmæglerselskaber og investeringsservice og -aktiviteter og en række EU-retsakter på det finansielle område.

Det foreslås i *§ 275, stk. 1, nr. 8,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.

Det foreslås i *§ 275, stk. 1, nr. 9,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at afgørelser truffet af Finanstilsynet i medfør af MiCA og regler udstedt i medfør heraf samt DORA-forordningen og regler udstedt i medfør heraf kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, som afgørelsen retter sig til.

Den foreslåede nr. 8 er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter fondsmæglerselskaber skal efterleve en række krav i forordningen, hvis de udbyder kryptoaktivtjenester.

Til nr. 16 (§ 276, nr. 9 og 10, i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter)

Den gældende § 276 i lov om fondsmæglerselskaber og investeringsservice og -aktiviteter er en generel bemyndigelsesbestemmelse, der giver erhvervsministeren bemyndigelse til at fastsætte regler, som er nødvendige

for at anvende eller gennemføre de afgørelser eller retsakter, som vedtages af Kommissionen i medfør af en række direktiver og forordninger.

Artikel 139 i MiCA tillægger Europa-Kommissionen beføjelser til at udstede en række delegerede retsakter.

Det foreslås i *§ 276, stk. 1, nr. 9,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslås i *§ 276, stk. 1, nr. 10,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at erhvervsministeren bemyndiges til at fastsætte regulering på de områder, hvor det som følge af delegerede retsakter, udstedt i medfør af DORA-forordningen eller MiCA, måtte være nødvendigt.

Til § 5

Til nr. 1 (fodnoten til lov om forvaltere af alternative investeringsfonde m.v.)

Det foreslås i *fodnoten* til lov om forvaltere af alternative investeringsfonde m.v. at indsætte, at der med denne lov foretages en gennemførelse af dele af Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022 om ændring af direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 for så vidt angår digital operationel modstandsdygtighed i den finansielle sektor, idet lovforslaget implementerer de dele af direktivet i lov om forvaltere af alternative investeringsfonde m.v., der omfatter forvaltere af alternative investeringsfonde. Det drejer sig om artikel 3 i direktivet, der fastsætter ændringer til Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde.

Direktivet er et følgedirektiv til DORA-forordningen. Med nærværende lovforslag bliver Finanstilsynet også udpeget som kompetent myndighed efter forordningen til at føre tilsyn med forvaltere af alternative investeringsfondes overholdelsen af forordningen. Der henvises til lovforslagets § 5, nr. 4.

Til nr. 2 (§ 8, stk. 6, i lov om forvaltere af alternative investeringsfonde m.v.)

Den gældende § 8, stk. 1, i lov om forvaltere af alternative investeringsfonde m.v. fastslår hvilke aktiviteter, en forvalter med tilladelse til at forvalte alternative investeringsfonde, og som ikke er selvforvaltende, må udføre. Det følger af bestemmelsen, at forvaltere, som ikke er selvforvaltende, ikke må udføre andre aktiviteter end dem, der er omhandlet i bilag 1, nr. 1 og 2, jf. dog stk. 2 og 3. Afgrænsningen i bestemmelsen indebærer, at en forvalter af alternative investeringsfonde efter gældende ret ikke må udføre investeringstjenester eller accessoriske tjenesteydelser med kryptoaktiver.

Det foreslås at indsætte § 8, *stk. 6*, hvorefter en forvalter af alternative investeringsfonde kan levere tjenester med kryptoaktiver som angivet i artikel 60, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, svarende til de tjenester, som det specifikt er meddelt tilladelse til i henhold til denne lov, hvis forvalteren giver Finanstilsynet meddelelse mindst 40 arbejdsdage, inden disse tjenester leveres første gang. Meddelelsen skal ledsages af de oplysninger, der er anført i artikel 60, stk. 7, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver.

Det foreslåede vil medføre, at en forvalter af alternative investeringsfonde fremadrettet må udbyde aktiviteter som angivet i artikel 60, stk. 5, i MiCA, hvis forvalteren lever op til betingelserne i artikel 60, stk. 7, i MiCA.

Den foreslåede bestemmelse er ny og er en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024. I artikel 60, stk. 5, i MiCA, bestemmes det, at en forvalter af alternative investeringsfonde skal kunne udføre disse aktiviteter, såfremt betingelserne angivet i bestemmelsen er opfyldt.

En forvalter af alternative investeringsfonde er ikke forpligtet til at ansøge om tilladelse til at udbyde kryptoaktivtjenester, jf. artikel 59, stk. 1, litra b, i MiCA.

Den foreslåede bestemmelse fastlægger, at Finanstilsynet er kompetent myndighed til at vurdere en underretning efter artikel 60, stk. 8, i MiCA.

En forvalter af alternative investeringsfonde må ikke begynde at levere kryptoaktivtjenester, så længe meddelelsen er ufuldstændig.

Retten til at levere kryptoaktivtjenester ophæves ved inddragelsen af den tilladelse, der gav en forvalter af alternative investeringsfonde mulighed for at levere kryptoaktivtjenester uden at skulle indhente en tilladelse i henhold til artikel 59, jf. artikel 60, stk. 11, i MiCA.

Bestemmelsen supplerer artikel 60, stk. 5, i MiCA.

Til nr. 3 (§ 27, stk. 2, nr. 6, i lov om forvaltere af alternative investeringsfonde m.v.)

Det fremgår af § 27, stk. 2, nr. 6, at en forvalter, under hensyntagen til karakteren af de forvaltede alternative investeringsfonde, skal have effektive former for virksomhedsstyring, herunder betryggende kontrol- og sikringsforanstaltninger på it-området. Bestemmelsen gennemfører dele af artikel 18, stk. 1, i Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde.

Det foreslås at ændre *§ 27, stk. 2, nr. 6,* således, at en forvalter af alternative investeringsfonde skal have betryggende kontrol- og sikringsforanstaltninger på it-området, også hvad angår net- og informationssystemer, der oprettes og styres i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede bestemmelse vil medføre, at en forvalter af alternative investeringsfonde også skal have betryggende kontrol- og sikringsforanstaltninger hvad angår net- og informationssystemer, der oprettes og styres i overensstemmelse med DORA-forordningen.

DORA-forordningen fastsætter ensartede krav til sikkerheden i de net- og informationssystemer, der understøtter finansielle enheders forretningsprocesser.

Ved net- og informationssystem forstås enhver it-infrastruktur, herunder teleinfrastruktur, it-aktiver, teknologier og enheder, der anvendes til lagring, behandling, overførsel eller anden brug af digitale data samt de digitale data, der indgår i ovenstående.

Den foreslåede ændring gennemfører artikel 3, nr. 1, i Europa-Parlamentets og Rådets direktiv 2022/2556/EU af 14. december 2022, der ændrer i artikel 18, stk. 1, i Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde.

Overtrædelse af § 27, stk. 2, nr. 6, kan straffes med bøde eller fængsel indtil 4 måneder, medmindre højere straf er forskyldt efter anden lovgivning, jf. lovforslagets § 190, stk. 1, i lov om forvaltere af alternative investeringsfonde m.v. Ansvarssubjektet i forhold til overtrædelse af lovforslagets § 27, stk. 2, er en forvalter af alternative investeringsfonde.

Det betyder, at hvis en forvalter ikke opfylder de i nr. 1-7 oplistede krav, herunder betryggende kontrol- og sikringsforanstaltninger på it-området, jf. nr. 6, vil forvalteren kunne straffes med bøde eller fængsel.

Med den foreslåede ændring vil en forvalter også kunne straffes med bøde eller fængsel, hvis forvalteren ikke har betryggende kontrol- og sikringsforanstaltninger hvad angår net- og informationssystemer, der oprettes og styres i overensstemmelse med DORA-forordningen. Der henvises i øvrigt til lovforslagets § 4, nr. 9, og bemærkningerne hertil.

Til nr. 4 (§ 155, stk. 1, 6. pkt., i lov om forvaltere af alternative investeringsfonde m.v.)

Den gældende § 155, stk. 1, i lov om forvaltere af alternative investeringsfonde m.v. fastlægger blandt andet Finanstilsynets forpligtelse til at påse overholdelsen af en række europæiske retsakter. Det indebærer, at Finanstilsynet kan give påtaler, påbud, m.v. for overtrædelse af de oplistede retsakter.

Det foreslås i *§ 155, stk. 1, 6. pkt.*, at Finanstilsynet desuden påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver og regler udstedt i medfør heraf og Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.

Det foreslåede vil medføre, at Finanstilsynet udpeges i henhold til artikel 93, stk. 1, i MiCA, som den kompetente myndighed, der er ansvarlig for at udføre de i MiCA fastsatte funktioner og opgaver.

Kommissionen er i medfør af artikel 139 i MiCA bemyndiget til at udstede delegerede retsakter, som Finanstilsynet i medfør af den foreslåede bestemmelse også vil skulle føre tilsyn med.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter en række aktører skal efterleve kravene i forordningen.

Den foreslåede ændring vil ligeledes medføre, at Finanstilsynet bliver udpeget som kompetent myndighed til at påse overholdelsen af DORA-forordningen.

DORA-forordningen finder bl.a. anvendelse på forvaltere af alternative investeringsfonde, jf. artikel 2, stk. 1, litra k. Forordningen finder dog ikke anvendelse på forvaltere af alternative investeringsfonde, der har registreret hjemsted i Danmark, som ikke er omfattet af forpligtelsen til at søge om tilladelse som forvalter af alternative investeringsfonde, jf. § 6, stk. 1, og som ikke har valgt frivilligt at søge en sådan tilladelse til at forvalte alternative investeringsfonde (registrerede forvaltere af alternative investeringsfonde), jf. § 1, stk. 4, i lov om alternative investeringsfonde m.v., jf. artikel 2, stk. 3, litra a, i DORA-forordningen.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningen, jf. § 161 i lov om forvaltere af alternative investeringsfonde m.v.

Finanstilsynet får med bestemmelsen bl.a. også mulighed for at give påbud og påtaler for overtrædelser af forordningerne, jf. § 155.

Efter artikel 46, litra i, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde, sikre overholdelsen af DORA-forordningen for forvaltere af alternative investeringsfonde.

Bestemmelsen supplerer artikel 46, litra i, i DORA-forordningen.

Til nr. 5 (§ 170, stk. 7, nr. 29, i lov om forvaltere af alternative investeringsfonde m.v.)

I medfør af § 170, stk. 1, i lov om forvaltere af alternative investeringsfonde er Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger, som de får kendskab til gennem tilsynsvirksomheden.

§ 170, stk. 7, er en undtagelse til tavshedspligten i § 170, stk. 1. Bestemmelsen fastsætter til hvem og i hvilke tilfælde, Finanstilsynet kan videregive fortrolige oplysninger, uanset § 170, stk. 1.

I medfør af § 170, stk. 7, har Finanstilsynet ikke mulighed for at videregive oplysninger til Center for Cybersikkerhed, Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 170, stk. 7,* at indsætte *nr. 29,* hvorefter Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til Center for Cybersikkerhed, SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større it-relateret hændelse fra en forvalter af alternative investeringsfonde, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. de centrale kontaktpunkter eller CSIRT'er, der er udpeget eller oprettet i overensstemmelse med NIS 2-direktivet, dvs. Center for Cybersikkerhed. Bestemmelsen nævner også SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle

sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 6 (§ 171, stk. 1, 9-11. pkt., i lov om forvaltere af alternative investeringsfonde m.v.)

§ 171, stk. 1, 1. pkt., i lov om forvaltere af alternative investeringsfonde fastsætter regler om offentliggørelse af reaktioner, som Finanstilsynets bestyrelse har truffet beslutning om, eller som Finanstilsynet har givet efter delegation fra Finanstilsynets bestyrelse. Bestemmelsen regulerer derimod ikke det tilfælde, hvor det alene er Finanstilsynet, der har truffet en afgørelse om at give en reaktion til en virksomhed omfattet af loven, uden at der er tale om en delegation fra Finanstilsynets bestyrelse.

I medfør af § 171, stk. 1, 1. pkt., skal en virksomhed, der har modtaget en reaktion, som Finanstilsynets bestyrelse har truffet beslutning om, eller som Finanstilsynet har givet efter delegation fra Finanstilsynets bestyrelse, offentliggøre oplysningerne herom på sin eventuelle hjemmeside på et sted, hvor de naturligt hører hjemme. Finanstilsynet skal også offentliggøre reaktionen på Finanstilsynets hjemmeside i medfør af § 171, stk. 1, 6. pkt.

Det foreslås i *§ 171, stk. 1, 9. pkt.*, at reaktioner givet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor skal offentliggøres på Finanstilsynets hjemmeside med angivelse af forvalterens navn, jf. dog stk. 4

Med den foreslåede ændring vil Finanstilsynet skulle offentliggøre reaktioner, der er givet af Finanstilsynet til en virksomhed for en overtrædelse af DORA-forordningen, uden at dette er sket efter en delegation fra Finanstilsynets bestyrelse. Ved reaktioner forstås f.eks. påbud eller påtaler. Reaktionen skal offentliggøres på Finanstilsynets hjemmeside. Derimod er virksomheden ikke selv forpligtet til at offentliggøre reaktionen. Virksomheden vil kun være forpligtet til at offentliggøre reaktionen, hvis bestyrelsen, eller Finanstilsynet efter delegation fra bestyrelsen, har truffet beslutning herom, i henhold til DORA-forordningen, jf. § 171, stk. 1, 1. pkt.

Det foreslås i *§ 171, stk. 1, 10.* og *11. pkt.*, at hvis en reaktion givet i henhold til 1. pkt. eller 8. pkt. indbringes for Erhvervsankenævnet eller domstolene, skal det fremgå af Finanstilsynets offentliggørelse. Status og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Med bestemmelsen skal det både fremgå af Finanstilsynets offentliggørelse, hvis en reaktion givet af Finanstilsynets bestyrelse, af Finanstilsynet efter delegation fra bestyrelsen, eller af Finanstilsynet i henhold til DORA-forordningen indbringes for Erhvervsankenævnet eller domstolene.

Offentliggørelsen skal ske i naturlig sammenhæng med den offentliggørelse, som Finanstilsynet tidligere har foretaget.

I medfør af 10. pkt. skal Finanstilsynet desuden tilføje oplysninger om status og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse til Finanstilsynets offentliggørelse. Status kan eksempelvis være, at parten efterfølgende trækker sin klage tilbage, eller at sagen afvises, hvorimod oplysninger om status quo ikke skal offentliggøres. Status for forløbet under sagens behandling i Erhvervsankenævnet skal heller ikke offentliggøres. Det omfatter eksempelvis anmodning om processkrifter m.v.

Afgørelser truffet af Finanstilsynet, bl.a. i henhold til loven eller regler udstedt i medfør heraf, kan indbringes for Erhvervsankenævnet af den, som afgørelsen retter sig mod, jf. § 189 i loven. Desuden foreslås det i § 5, nr. 7, i nærværende lovforslag, at afgørelser truffet af Finanstilsynet i henhold til DORA-forordningen også kan indbringes for Erhvervsankenævnet.

Indbringes en afgørelse for Erhvervsankenævnet, vil Finanstilsynet blive orienteret herom af Erhvervsankenævnet. Finanstilsynet vil herefter – i de tilfælde hvor den indbragte afgørelse er offentliggjort i medfør af § 171, stk. 1 – offentliggøre oplysninger om afgørelsens indbringelse. Finanstilsynets offentliggørelse heraf skal som udgangspunkt ske inden for 1 til 2 hverdage.

Finanstilsynets offentliggørelse skal ske på Finanstilsynets hjemmeside dér, hvor Finanstilsynet tidligere har offentliggjort reaktionen i henhold til DORA-forordningen efter § 171, stk. 1, 6. pkt., eller efter forslaget til nyt stk. 1, 8. pkt. Oplysningen om, at sagen er indbragt for Erhvervsankenævnet, skal fremgå tydeligt.

Finanstilsynet skal desuden offentliggøre det endelige udfald af sagen. Det indebærer ikke, at Finanstilsynet skal offentliggøre Erhvervsankenævnets kendelser i sin helhed. Disse offentliggøres af Erhvervsankenævnet.

Den foreslåede ændring gennemfører også artikel 54, stk. 1, i DORA-forordningen, hvormed de kompetente myndigheder uden unødigt ophold på deres officielle websteder skal offentliggøre enhver afgørelse om at pålægge en administrativ sanktion, som ikke kan påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen. En administrativ sanktion kan bl.a. kan være et påbud eller en påtale.

Det fremgår dog videre af artikel 54, stk. 5, i DORA-forordningen, at hvis den kompetente myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

Artikel 54, stk. 1 og 5, svarer derfor til kravet om offentliggørelse af reaktioner i henhold til DORA-forordningen og den efterfølgende offentliggørelse af indbringelse af en reaktion til enten Erhvervsankenævnet eller domstolene i henhold til forslaget til § 171, stk. 1, 8.-10. pkt.

For nærmere om § 171 og offentliggørelse henvises der i det hele til de specielle bemærkningerne til § 171, tidligere § 170, jf. Folketingstidende 2012-2013, tillæg A, L 175 som fremsat, side 186-189.

Den foreslåede bestemmelse er ny og foreslås som en konsekvens af, at MiCA finder anvendelse fra den 30. december 2024, hvorefter Finanstilsynet påser efterlevelsen af kravene i forordningen.

Til nr. 7 (§ 189 i lov om forvaltere af alternative investeringsfonde m.v.)

Den gældende § 189, stk. 1, i lov om forvaltere af alternative investeringsfonde m.v. indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet retter sig mod. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet i medfør af lov om forvaltere af alternative investeringsfonde og en række EU-retsakter på det finansielle område.

Det foreslås i *§ 189* at ændre »tjenesteydelser eller« til: »tjenesteydelser,« og efter » bæredygtige investeringer « indsættes:», Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver eller Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede vil medføre, at afgørelser truffet af Finanstilsynet i medfør af DORA-forordningen eller MiCA og regler udstedt i medfør af disse forordninger kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den, som afgørelsen retter sig til.

Til nr. 8 (§ 190, stk. 1, i lov om forvaltere af alternative investeringsfonde m.v.)

Den gældende § 190, stk. 1, i lov om forvaltere af alternative investeringsfonde m.v. fastsætter, at overtrædelser af lovens bestemmelser og en række EU-retsakter kan straffes med bøde eller fængsel indtil fire måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås i *§ 190, stk. 1,* efter »om europæiske sociale iværksætterfonde« at indsætte »og artikel 59, stk. 1, artikel 60, stk. 5, artikel 70, stk. 1-4, artikel 72, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver«.

Det foreslåede vil medføre, at overtrædelse af artikel 59, stk. 1, artikel 60, stk. 5, artikel 70, stk. 1-4, artikel 72, stk. 1, i MiCA straffes med bøde eller fængsel indtil fire måneder, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Artikel 59, stk. 1, i MiCA omhandler tilladelseskrav til at udbyde kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelsen er enhver fysisk eller juridisk person, der udbyder kryptoaktivtjenester uden den nødvendige tilladelse. Den strafbare handling består i at udbyde kryptoaktivtjenester uden enten at være meddelt tilladelse efter artikel 63 eller uden at have tilladelse til at levere kryptoaktivtjenester efter artikel 60 i MiCA.

Artikel 60, stk. 5, i MiCA fastsætter krav om underretning af Finanstilsynet, førend forvaltere af alternative investeringsfonde kan levere kryptoaktivtjenester svarende til forvaltning af porteføljer af investeringstjenester og accessoriske tjenesteydelser, som det specifikt er meddelt tilladelse til. Ansvarssubjektet for overtrædelsen af bestemmelserne er forvaltere af alternative investeringsfonde. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde påbegynder levering af en kryptoaktivtjeneste, uden at have underrettet Finanstilsynet med de oplysninger, der er anført i artikel 60, stk. 7, mindst 40 arbejdsdage inden forvalteren leverer disse tjenester første gang.

Artikel 70, stk. 1-4, i MiCA omhandler krav vedrørende opbevaring af kunders kryptoaktiver og midler. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at forvaltere af alternative investeringsfonde, der opbevarer kryptoaktiver på vegne af deres kunder, ikke træffer passende

foranstaltninger til at forhindre, at kundernes kryptoaktiver anvendes til handel for deres egen regning.

Artikel 72, stk. 1, i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde ikke opretholder og anvender effektive politikker til at identificere mellem dem selv og personerne opregnet i artikel 72, stk. 1, litra a-e.

Bestemmelsen supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

Til nr. 9 (§ 190, stk. 2, i lov om forvaltere af alternative investeringsfonde m.v.)

Den gældende § 190, stk. 2, fastsætter, at overtrædelser af lovens bestemmelser og en række EU-retsakter kan straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

Det foreslås i *§ 190, stk. 2,* efter »om pengemarkedsforeninger« at indsætte »samt artikel 64, stk. 8, artikel 65, stk. 4, artikel 66, stk. 1-5, artikel 68, stk. 4-9, artikel 69, artikel 71, stk. 1-4, artikel 72, stk. 2-4, artikel 73, stk. 2 og 3, og artikel 81, stk. 1-14, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver, og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26, stk. 1-6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor«.

Det foreslåede vil medføre, at overtrædelse af de oplistede artikler straffes med bøde, medmindre højere straf er forskyldt efter den øvrige lovgivning.

I det følgende redegøres for de nævnte artikler i MiCA.

Artikel 64, stk. 8, i MiCA regulerer udbydere af kryptoaktivtjenesters forpligtigelse til at sikre overførelse af deres kunders kryptoaktiver og midler i tilfælde af, at udbyderens tilladelse bliver inddraget. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af

alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde ikke har passende procedurer for, hvorledes kryptoaktiver som opbevares på vegne af forvalterens kunder, vil blive overført til en anden udbyder af kryptoaktivtjenester, i tilfælde af inddragelse af forvalterens tilladelse.

Artikel 65, stk. 4, i MiCA omhandler oplysningskrav ved grænseoverskridende levering af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består i, at en forvalter af alternative investeringsfonde påbegynder leveringen af kryptoaktivtjenester i en anden medlemsstat end Danmark inden 15 kalenderdage efter at have indgivet de oplysninger, der er omhandlet i artikel 65, stk. 1, eller inden at have modtaget den i artikel 65, stk. 2, omtalte meddelelse fra Finanstilsynet.

Artikel 66, stk. 1-5, i MiCA omhandler udbydere af kryptoaktivtjenesters forpligtelse til at handle ærligt, redeligt og professionelt i kundernes bedste interesse. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at forvalter af alternative investeringsfonde giver sine kunder vildledende oplysninger.

Artikel 68, stk. 4-9, i MiCA omhandler kravene til ledelsesordninger og indretningen af udbydere af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af artikel 68, stk. 4, 5 og 7-9 er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Ansvarssubjektet for overtrædelse af artikel 68, stk. 6, er ledelsesorganet hos en forvalter af alternative investeringsfonde. Den strafbare handling består eksempelvis i, at forvalteren ikke har vedtaget procedurer, som er tilstrækkelige til at sikre overholdelsen af MiCA. Det strafbare forhold kan endvidere bestå i, at ledelsesorganer hos en forvalter af alternative investeringsfonde ikke regelmæssigt vurderer og evaluerer effektiviteten af den politik og de ordninger og procedurer, der er indført for at opfylde forpligtelserne i artikel 66-83 i MiCA, herunder ikke træffer passende foranstaltninger til at afhjælpe eventuelle mangler i den henseende.

Artikel 69 i MiCA indebærer krav om at meddele Finanstilsynet eventuelle ændringer i ledelsesorganet hos en udbyder af kryptoaktivtjenester. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel

60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde ikke giver Finanstilsynet alle oplysninger, som er nødvendige for Finanstilsynets vurdering af overholdelsen af artikel 68 i MiCA, inden nye medlemmer af ledelsesorganet tiltræder deres stilling.

Artikel 71, stk. 1-4, i MiCA fastsætter krav til udbydere af kryptoaktivtjenesters klagebehandlingsprocedurer. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde kræver betaling af gebyr eller anden afgift i forbindelse med behandling af klager fra sine kunder.

Artikel 72, stk. 2-4 i MiCA fastsætter krav om effektive politikker og procedurer til identificering, forebyggelse, håndtering og oplysning om interessekonflikter. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde ikke oplyser sine kunder og potentielle kunder om de skridt, forvalteren har taget for at begrænse interessekonflikter.

Artikel 73, stk. 2 og 3, i MiCA regulerer udbydere af kryptoaktivtjenesters outsourcing af tjenester eller aktiviteter til tredjeparter. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der udbyder kryptoaktivtjenester efter artikel 60, stk. 5, i MiCA. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde ikke træffer alle rimelige foranstaltninger for at undgå yderligere operationel risiko, eller at en forvalter af alternative investeringsfonde ikke sikrer, at betingelserne i artikel 73, stk. 1, litra a-g, til enhver tid er opfyldt.

Artikel 81, stk. 1-14, i MiCA fastsætter en række krav til udbydere af kryptoaktivtjenester, der yder rådgivning om kryptoaktiver og udbyder af kryptoaktivtjenester, som yder porteføljepleje af kryptoaktiver. Ansvarssubjektet for overtrædelse af bestemmelserne er en forvalter af alternative investeringsfonde, der yder porteføljepleje af kryptoaktiver. Den strafbare handling består eksempelvis i, at en forvalter af alternative investeringsfonde, der yder porteføljepleje af kryptoaktiver, undlader at advare sine kunder eller potentielle kunder om de forhold, som er oplistet i artikel 81, stk. 9, litra a-f.

Bestemmelsen supplerer artikel 111, stk. 1, 2. afsnit, i MiCA.

I det følgende redegøres for de nævnte artikler i DORA-forordningen.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der forvaltere af alternative investeringsfonde, jf. artikel 2, stk. 1, litra k, jf. artikel 2, stk. 2, i DORA-forordningen.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring.

En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også

bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan

kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-

indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare

procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende

ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den

hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk.

1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår

af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket

betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant,

inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-

risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og

sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere

cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed

gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og

forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder

og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 6

Til nr. 1 (§ 3, stk. 1, nr. 28-29, i lov om firmapensionskasser)

Den gældende bestemmelse i § 3 definerer en række begreber anvendt i lov om firmapensionskasser. Variable løndele og kønsneutrale lønpolitikker er ikke defineret heri.

Variable løndele defineres i den gældende § 5, stk. 1, i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser (aflønningsbekendtgørelsen) med senere ændringer som aflønningsordninger, hvor den endelige aflønning ikke er kendt på forhånd, herunder bonusordninger, resultatkontrakter, engangsvederlag og andre lignende ordninger, der ikke er en del af den faste løndel.

Det foreslås i *§ 3, stk. 1, nr. 28,* at der ved variable løndele forstås aflønningsordninger, hvor den endelige aflønning ikke er kendt på forhånd, herunder bonusordninger, resultatkontrakter, engangsvederlag og andre lignende ordninger, der ikke er en del af den faste løndel.

Den foreslåede bestemmelse viderefører med redaktionelle ændringer aflønningsbekendtgørelsens § 5, stk. 1. Det foreslåede tilsigter ikke materielle ændringer.

Der er ikke i lovteksten tale om en udtømmende opremsning af variable løndele.

Direkte resultatafhængige eller performanceafhængige programmer som f.eks. bonusordninger, resultatlønskontrakter og andre aflønningsordninger, der afhænger af, at den ansatte lever op til på forhånd fastsatte mål og kriterier, udgør variabel løn.

Fastholdelsesbonusser udgør ligeledes variabel løn, herunder både fastholdelsesbonusser, der udelukkende er bundet op på den ansattes forbliven i en vis periode, og fastholdelsesbonusser, der ligeledes er bundet op på resultatkrav. I forhold til nyansættelsesgodtgørelse (sign-on bonus) og fratrædelsesgodtgørelse reguleres dette i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser med senere ændringer.

Endvidere udgør andre ad-hoc beløb, engangsvederlag og diskretionære beløb, som ikke nødvendigvis er direkte resultatafhængige, ligeledes variabel løn. Dette kan både være engangsvederlag på baggrund af f.eks. en bonuspulje i firmapensionskassen, men det kan også være beløb, der tildeles som efterfølgende belønning på baggrund af f.eks. et stort arbejdspres, mange arbejdstimer, gode resultater, færdiggørelse af projekter,

omstruktureringer m.v. Sådanne ad-hoc beløb, engangsvederlag og diskretionære beløb udgør også variabel løn, idet den ansatte ikke på forhånd ved, om et sådant vederlag modtages. Aflønningen er således ikke en del af den faste løn og derfor ikke kendt på forhånd.

Aftaletidspunktet er ikke afgørende for, om der er tale om variable løndele. Der kan således være tale om variable løndele, både hvis muligheden for opnåelse af bonus/vederlag er aftalt forudgående, og hvis virksomheden efterfølgende tildeler bonus/vederlag på engangsbasis.

For ansatte, som er omfattet af en aftale om overarbejdstidsbetaling, f.eks. timelønnede ansatte, anses overarbejdstidsbetaling for fast løn, forudsat at der på forhånd er aftalt faste rammer for honorering, herunder i forhold til timeregnskab, timesats, afregningsinterval m.v. Tilsvarende vil på forhånd aftalte faste tillæg til lønnen som udgangspunkt udgøre en del af den faste løndel.

For så vidt angår dividende eller afkast, der tilkommer en ejer af en firmapensionskasse, er der ikke tale om variabel løn i lovens forstand, idet afkast fra eksempelvis en aktie ikke kan anses for at være en løn, der betales af firmapensionskassen på grundlag af en kontrakt om vederlag for det arbejde, den pågældende har udført for firmapensionskassen. Omvendt vil det som udgangspunkt anses for at være variabel løn, såfremt en firmapensionskasse beslutter sig for diskretionært at foretage overskudsdeling til de ansatte, uanset om dette ikke er aftalt på forhånd med de ansatte.

Det foreslås i *§ 3, stk. 1, nr. 29,* at der ved begrebet kønsneutral aflønningspolitik forstås en aflønningspolitik, der er baseret på lige løn for samme arbejde eller arbejde af samme værdi uanset den ansattes køn.

Med en kønsneutral lønpolitik menes en politik, som behandler alle køn på samme måde. Det vil sige, at lønpolitikken sikrer, at ansatte modtager lige løn for arbejde af samme art eller arbejde af samme værdi uanset vedkommendes køn og sikrer implementering af virksomhedsværdier, der fremmer ligebehandling af alle køn. Udover at sikre lige løn for samme arbejde skal lønpolitikken ligeledes sikre lige muligheder for ansatte, uanset vedkommendes køn, da dette er en forudsætning for kønsneutral løn.

Princippet om lige løn for samme arbejde eller arbejde af samme værdi uanset vedkommendes køn er nedfældet i artikel 157 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Dette princip skal anvendes på en konsekvent måde af firmapensionskasserne. Ifølge artikel 157 i TEUF

inkluderer lige løn for samme arbejde eller arbejde af samme værdi den almindelige grundløn, mindsteløn eller løn og ethvert andet vederlag, hvad enten det er i kontanter eller naturalier, som medarbejdere modtager direkte eller indirekte for vedkommendes ansættelse af arbejdsgiveren. TEUF opfordrer til yderligere foranstaltninger for at sikre lige muligheder og ligebehandling af alle køn i spørgsmål om beskæftigelse og erhverv.

Der henvises til bemærkningerne til forslagets § 43 e, stk. 2.

Til nr. 2 (§§ 43 e-43 h, i lov om firmapensionskasser)

§ 43 e

Den gældende § 8 i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser (aflønningsbekendtgørelsen), fastlægger, at en firmapensionskasse skal vedtage en skriftlig lønpolitik. Overtrædelser af bestemmelsen straffes med bøde, jf. § 29, stk. 1, i aflønningsbekendtgørelsen.

Det foreslås i *§ 43 e, stk. 1*, at en firmapensionskasse skal vedtage en skriftlig lønpolitik, der er i overensstemmelse med og fremmer en sund og effektiv risikostyring.

Det foreslåede viderefører med enkelte redaktionelle ændringer i § 8 i aflønningsbekendtgørelsen. Den foreslåede bestemmelse medfører ingen materielle ændringer.

Den foreslåede bestemmelse viderefører implementeringen af artikel 23, stk. 1, og stk. 3, litra d, i Europa-Parlamentets og Rådets direktiv 2016/2341/EU af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'er) aktiviteter og tilsynet hermed. Det følger heraf, at IORP'erne skal udforme og anvende en forsvarlig aflønningspolitik for alle de personer, der reelt leder IORP'en, varetager nøglefunktioner og andre kategorier af personale, hvis professionelle aktiviteter har væsentlig indflydelse på IORP'ens risikoprofil, på en måde der står i rimeligt forhold til deres størrelse og interne organisation samt størrelsen, arten, omfanget og kompleksiteten af dens aktiviteter. Aflønningspolitikken skal være forenelig med en sund og effektiv risikostyring og må ikke tilskynde til risikotagning, som er uforenelig med IORP'ens risikoprofiler og regler.

En lønpolitik udgør en ramme for firmapensionskassens aflønning af sine ansatte. Lønpolitikken skal være tilpasset virksomhedens forhold og understøtte virksomhedens risikostyring.

Lønpolitikken skal indføres, gennemføres og opretholdes i overensstemmelse med firmapensionskassens forretnings- og risikostyringsstrategi, risikoprofil, mål og risikostyringspraksis samt deres langsigtede interesser og resultater som helhed, ligesom den skal omfatte tiltag til at forhindre interessekonflikter. En lønpolitik bør derfor beskrive, hvilke overordnede mål virksomheden ønsker at opnå med sin aflønningsstruktur.

En lønpolitik skal finde anvendelse på firmapensionskassen som helhed og indeholde specifikke ordninger, som tager højde for opgaver og resultater for medlemmer af bestyrelsen og direktionen samt andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil.

Firmapensionskassens bestyrelse fastlægger de generelle principper for lønpolitikken, som skal omfatte alle ansatte i virksomheden, navnlig aflønning af direktionen, andre væsentlige risikotagere og andre personer, der handler på virksomhedens vegne. En lønpolitik bør endvidere fastlægge rammerne for personer, som handler på virksomhedens vegne, eksempelvis tilknyttede agenter, således at betaling af disse personer ikke tilskynder til uforholdsmæssig risikotagning eller uhensigtsmæssigt salg af produkter. Hvor det er relevant, bør en lønpolitik endvidere tage højde for personsammenfald mellem virksomhedens hovedaktionærer og ansatte samt adressere potentielle interessekonflikter i denne henseende. En lønpolitik skal ligeledes sikre, at der ikke opstår væsentlige interessekonflikter for ansatte i kontrolfunktioner.

Firmapensionskassen skal sikre, at der er en klar, gennemsigtig og effektiv ledelse med hensyn til aflønning, herunder tilsyn med lønpolitikken.

Lønpolitikken skal formidles til alle ansatte i firmapensionskassen.

En lønpolitik skal tage afsæt i virksomhedens størrelse, organisation samt omfanget og kompleksiteten af virksomhedens aktiviteter. Ved vurderingen af virksomhedens størrelse kan der bl.a. lægges vægt på værdien af virksomhedens aktiver og passiver, værdien af virksomhedens risikovægtede aktiver, summen af store engagementer, kapitalgrundlaget samt antallet af ansatte. Ved vurdering af virksomhedens organisation kan der bl.a. lægges vægt på virksomhedens organisering af passende risikostyringsfunktioner. Ved vurdering af arten samt omfanget og kompleksiteten af virksomhedens aktiviteter kan der bl.a. lægges vægt på kompleksiteten og karakteren af virksomhedens forretningsmodel, produkter og kontrakter samt underliggende aktiver og passiver.

En lønpolitik skal være i overensstemmelse med virksomhedens forretningsmodel og risikoprofil, værdier, langsigtede interesser, organisatoriske struktur samt iagttage forbruger og investorbeskyttelseshensyn, herunder tage hensyn til de langsigtede virkninger af trufne investeringsbeslutninger. En lønpolitik må ikke tilskynde til overdreven risikotagning, men skal derimod fremme ansvarlig forretningsadfærd og tilskynde til risikobevidsthed og forsigtig risikotagning.

En lønpolitik skal indeholde de overordnede mål for virksomhedens, forretningsenhedernes og ansattes resultater og de overordnede metoder for måling af resultaterne samt de overordnede resultatkriterier. Virksomhedens lønpolitik bør skelne mellem de forskellige forretningsenheder, ledelsesfunktioner samt kontrolfunktioner for så vidt angår variabel aflønning og de overordnede resultatkriterier.

En lønpolitik skal sikre, at der ved beslutninger om tildeling af variabel løn tages højde for de risici, som er forbundet med de resultatkrav, der kan udløse en variabel løn. Resultatkravene skal afspejle både de ansattes, forretningsenhedernes og virksomhedens samlede resultater.

En lønpolitik skal afspejle, om der er forskel på muligheden for at optjene variabel løn mellem de forskellige forretningsenheder, herunder hvilke risici der er forbundet hermed i de forskellige forretningsenheder, samt hvordan dette afspejles i muligheden for variabel løn. Det skal således være muligt at udlede af virksomhedens lønpolitik, om og hvordan virksomheden anvender variabel løn, herunder hvilke overordnede kriterier der gælder for, at en ansat kan få tildelt variabel løn. Virksomheden kan have fastsat kriterier som eksempelvis omkostningsudviklingen i virksomheden, kundetilfredshed og virksomhedens resultat før skat.

En firmapensionskasse skal have en lønpolitik uanset, om virksomheden alene anvender fast løn og således ikke anvender variabel aflønning. Anvender virksomheden alene variabel løn i ekstraordinære tilfælde, eksempelvis i tilfælde af at ansatte har ydet en ekstraordinær indsats, skal det fremgå af lønpolitikken, at virksomheden anvender variabel løn, herunder hvilke former for variabel løn virksomheden anvender i sådanne tilfælde samt kriterierne for tildeling af løndelen.

Da der gælder særlige begrænsninger for brugen af variabel løn til bestyrelse, direktion og andre væsentlige risikotagere, er det naturligt, at en lønpolitik særligt fokuserer på aflønningen af denne personkreds, uanset at den gælder for alle ansatte. Virksomhedens lønpolitik bør angive, hvilke former for variabel løn, eksempelvis resultatkontrakter,

nyansættelsesgodtgørelser, fastholdelsesbonusser m.v., der kan tildeles, herunder tage stilling til de begrænsninger for brugen af variabel løn, som følger af det foreslåede § 43 h.

En lønpolitik skal eksempelvis fastlægge loftet for variabel løn for bestyrelsen, direktionen samt virksomhedens andre væsentlige risikotagere, hvis virksomheden anvender variabel løn. Loftets størrelse kan variere for bestyrelsen, direktionen og andre væsentlige risikotagere, så længe disse er fastsat indenfor rammerne af det foreslåede § 43 h, stk. 1, nr. 1-3. Bestyrelsen kan med generalforsamlingens godkendelse eksempelvis fastsætte et loft, som er lavere end det, der følger af det foreslåede § 43 h, stk. 1, nr. 1-3.

Såfremt virksomheden tildeler variabel løn til bestyrelsen, direktionen eller andre væsentlige risikotagere, skal lønpolitikken sikre en passende balance mellem den faste og den variable løndel. Den passende balance kan variere afhængigt af modtagerens funktion og virksomhedens forhold i øvrigt. Anvender virksomheden instrumenter som variabel løn, bør en lønpolitik oplyse, hvilke former for instrumenter en virksomhed kan tildele, eksempelvis efterstillet gæld, aktier i modervirksomheden m.m. Såfremt en virksomhed anvender eller gerne vil have mulighed for at anvende nyansættelsesgodtgørelser, som pr. definition er variabel løn, bør den maksimale størrelse heraf fremgå af lønpolitikken.

Hvis det er relevant, bør lønpolitikken endvidere indeholde virksomhedens krav til udskydelse af variable løndele samt begrundelse for, hvordan udskydelsesperioden er tilpasset virksomhedens risikoprofil. Lønpolitikken bør ligeledes, hvis relevant, indeholde en beskrivelse af, hvordan virksomheden forholder sig til kravene om forudgående og efterfølgende risikojustering af tildeling og udbetaling af variabel løn. I praksis medfører en effektiv lønpolitik, at variable løndele kan nedjusteres som følge af forudgående eller efterfølgende risikojusteringer. Eksempelvis kan det fremgå af en lønpolitik, at variable løndele nedjusteres på udbetalingstidspunktet som følge af, at virksomhedens økonomiske situation er væsentligt forringet siden tildelingstidspunktet. En lønpolitik bør således anføre, hvordan variable løndele kan justeres i forhold til ændringer i resultater for de enkelte ansatte, afdelingerne samt virksomheden. Endvidere kan det eksempelvis fremgå af lønpolitikken, at variable løndele kan nedjusteres eller kræves tilbagebetalt som følge af, at modtageren har været i ond tro.

En lønpolitik skal bidrage til opnåelse og opretholdelse af et sundt kapitalgrundlag og tage højde for eventuelle restriktioner for udlodninger.

En lønpolitik bør således tage højde for, at udbetaling af variabel løn ikke svækker virksomhedens mulighed for at styrke sit kapitalgrundlag.

En lønpolitik bør angive fremgangsmåden for udpegning af væsentlige risikotagere.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelse af § 43 e, stk. 1, straffes med bøde. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Overtrædelser kan eksempelvis bestå i, at en firmapensionskasse helt undlader at udarbejde en skriftlig lønpolitik eller har en lønpolitik, som åbenlyst er i strid med aflønningsreglerne.

Det foreslås i *§ 43 e, stk. 2*, at firmapensionskassens lønpolitik skal være kønsneutral.

Ved en kønsneutral lønpolitik forstås en lønpolitik baseret på lige løn for samme arbejde eller arbejde af samme værdi uanset den ansattes køn.

Firmapensionskassens bestyrelse skal således vedtage og opretholde en lønpolitik, der sikrer, at ansatte modtager lige løn for arbejde af samme art eller arbejde af samme værdi uanset vedkommendes køn, og sikrer implementering af virksomhedsværdier, der fremmer ligebehandling af alle køn. Udover at sikre lige løn for samme arbejde skal lønpolitikken ligeledes sikre lige muligheder for ansatte, uanset vedkommendes køn, da dette er en forudsætning for kønsneutral løn. Firmapensionskassens kønsneutrale lønpolitik skal finde anvendelse for alle firmapensionskassens ansatte, inklusive firmapensionskassens væsentlige risikotagere.

Lønpolitikken og alle tilknyttede ansættelsesvilkår, der har indflydelse på lønnen pr. måleenhed eller tidsrate, bør være kønsneutral. Dette inkluderer, men er ikke begrænset til løn, herunder tildelings- og udbetalingsbetingelser, rekrutteringspolitikker, karriereudviklings- og successionsplaner, adgang til uddannelse og muligheden for at søge om interne stillinger. Enhver form for kønsdiskrimination eller andre former for forskelsbehandling skal ikke tolereres. Dette omfatter eksempelvis forskelsbehandling som følge af forældreorlov.

Princippet om lige løn til mænd og kvinder for samme arbejde eller arbejde af samme værdi er nedfældet i artikel 157 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Dette princip skal anvendes på en konsekvent måde af institutterne. Ifølge artikel 157 i TEUF inkluderer lige løn for samme arbejde eller arbejde af samme værdi den almindelige grundløn, mindsteløn eller løn og ethvert andet vederlag, hvad enten det er

i kontanter eller naturalier, som medarbejdere modtager direkte eller indirekte for vedkommendes ansættelse af arbejdsgiveren. TEUF opfordrer til yderligere foranstaltninger for at sikre lige muligheder og ligebehandling af ethvert køn i spørgsmål om beskæftigelse og erhverv.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelser af § 43 e, stk. 2, straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af bestemmelsen er firmapensionskassen. Overtrædelser består eksempelvis i, at virksomhedens lønpolitik ikke er kønsneutral eller ikke sikrer lige muligheder for alle køn.

§ 43 f

Den gældende § 14 i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasse med senere ændringer (aflønningsbekendtgørelsen), fastsætter regler om godkendelse af lønpolitikken, om at bestyrelsesformanden skal redegøre for virksomhedens aflønning af bestyrelse og direktion samt om offentliggørelsen af oplysninger om aflønningen af ledelsen i virksomheden. Overtrædelser af bestemmelsen straffes med bøde, jf. § 29 i aflønningsbekendtgørelsen.

Det foreslås i *§ 43 f, stk. 1, 1. pkt.,* at firmapensionskassens øverste organ skal godkende firmapensionskassens lønpolitik, jf. § 43 e, herunder retningslinjer for tildeling af variabel løn og retningslinjer for fratrædelsesgodtgørelser, ved enhver væsentlig ændring og mindst hvert fjerde år.

Kravet om det øverste organs godkendelse af lønpolitikken (»say on pay«) er gennemført i overensstemmelse med den politiske aftale af 31. august 2010 mellem den daværende regering (Venstre og Det Konservative Folkeparti), Socialdemokraterne, Dansk Folkeparti, Socialistisk Folkeparti, Radikale Venstre og Liberal Alliance om forsvarlig lønpolitik i den finansielle sektor. Det følger af aftalen, at der skal være forsvarlige aflønningspolitikker i den finansielle sektor, som også sikrer kapitalejernes indflydelse på virksomhedens lønpolitik. Firmapensionskassens lønpolitik skal således godkendes af det øverste organ, hvilket typisk er generalforsamlingen, uanset om firmapensionskassen benytter variabel aflønning eller ej, idet en beslutning om ikke at benytte variabel aflønning ligeledes udgør en lønpolitik, som medlemmerne af det øverste organ skal tage stilling til.

Lønpolitikken skal godkendes som et separat punkt på dagsordenen. En lønpolitik kan eksempelvis ikke godkendes som en del af formandens beretning.

Hvis det øverste organ ikke godkender lønpolitikken, skal bestyrelsen udarbejde en ny lønpolitik, der tager højde for det øverste organs bemærkninger, og som igen skal forelægges til godkendelse for det øverste organ.

Det følger af det foreslåede, at firmapensionskassens øverste organ skal godkende virksomhedens lønpolitik ved enhver væsentlig ændring og mindst hvert fjerde år.

En væsentlig ændring, som vil forudsætte en ny godkendelse, kan f.eks. være en justering af rammerne for fordelingen mellem fast og variabel løn eller introduktion af nye komponenter i lønpolitikken. Helt formelle ændringer i lønpolitikken, herunder tilpasning af formalia og lign., anses ikke for at udgøre en væsentlig ændring.

Enhver ændring af lønforholdene for medlemmer af direktionen og bestyrelsen anses for at udgøre en væsentlig ændring.

Firmapensionskassens øverste organ skal som minimum godkende firmapensionskassens lønpolitik hvert fjerde år, også hvis der ikke foretages ændringer.

Som hidtil vil de ændrede dele af lønpolitikken først kunne benyttes for aftaler om variabel løn for direktionen og bestyrelsen, når den reviderede lønpolitik er godkendt af firmapensionskassens øverste organ. Det vil være i modstrid med det nævnte »say on-pay-princip«, hvis ændrede dele af lønpolitikken kan benyttes for direktionen og bestyrelsen, før virksomhedens øverste organ har taget stilling til den reviderede lønpolitik.

For væsentlige risikotagere kan ændrede dele af en revideret lønpolitik som hidtil benyttes, når den reviderede lønpolitik er godkendt af bestyrelsen. Den reviderede lønpolitik godkendes så af firmapensionskassens øverste organ ved førstkommende lejlighed. Lønpolitikken skal altid være i overensstemmelse med og fremme en sund og effektiv risikostyring, jf. den foreslåede § 43 e.

Lønpolitikken skal ikke berøre ansættelsesforhold, der er omfattet af kollektive overenskomster, medmindre der er tale om bonusordninger m.v. for overenskomstansatte, som ikke er fastsat i overenskomsten, hvilket

betyder, at virksomhedens øverste organ ikke vil skulle godkende lønforhold, der reguleres af det overenskomstdækkede område.

Det foreslås i *43 f, stk. 1, 2. pkt.,* at firmapensionskassens lønpolitik hurtigst muligt efter godkendelsen skal offentliggøres på virksomhedens hjemmeside.

Det betyder, at lønpolitikken skal offentliggøres på virksomhedens hjemmeside umiddelbart efter godkendelsen uden unødigt ophold.

Det foreslås i *§ 43 f, stk. 1, 3. pkt.,* at lønpolitikken skal forblive offentligt tilgængelig på hjemmesiden, så længe den er gældende.

Den foreslåede bestemmelse indebærer, at virksomheden ikke må fjerne en allerede offentliggjort lønpolitik fra sin hjemmeside, så længe den er gældende.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelse af § 43 f, stk. 1, straffes med bøde. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Overtrædelser kan eksempelvis bestå i, at firmapensionskassen undlader at offentliggøre sin lønpolitik, eller at firmapensionskassen undlader at forelægge en ny lønpolitik, der medfører væsentlige ændringer i aflønningen i den pågældende virksomhed, for det øverste organ.

Det foreslås i *§ 43 f, stk. 2, 1. pkt.,* at formanden for bestyrelsen i sin beretning for firmapensionskassens øverste organ skal redegøre for aflønningen af firmapensionskassens bestyrelse og direktion.

Den foreslåede bestemmelse indeholder en pligt for formanden for bestyrelsen i firmapensionskassen til at redegøre for aflønningen af firmapensionskassens bestyrelse og direktion. Redegørelsen skal indgå som et led i formandens beretning for virksomhedens øverste organ.

Formålet med kravet er, at generalforsamlingen i firmapensionskassen skal forholde sig til bestyrelsens og direktionens aflønning.

Det foreslås i *§ 43 f, stk. 2, 2. pkt.,* at redegørelsen skal indeholde oplysninger om aflønningen i det foregående regnskabsår og om den forventede aflønning i det indeværende samt det kommende regnskabsår.

Det foreslås i *§ 43 f, stk. 2, 3. pkt.,* at formanden for bestyrelsen skal forklare og begrunde lønpolitikkens indhold og dens efterlevelse i sin beretning for virksomhedens øverste organ.

Formandens beretning skal navnlig adressere de overordnede komponenter i virksomhedens lønpolitik og uddybe hensigten hermed. Derudover skal bestyrelsesformanden forklare lønpolitikkens efterlevelse, herunder tilfælde hvor lønpolitikken eventuelt ikke efterleves.

Hvis det øverste organ skal godkende forslag til revideret lønpolitik, jf. det foreslåede § 43 b, stk. 1, kan formanden for bestyrelsen begrænse forklaringen af og begrundelsen for lønpolitikkens indhold og dens efterlevelse til ændringerne af lønpolitikken og formålet med disse ændringer.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelser af § 43 f, stk. 2, straffes med bøde. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Den strafbare handling kan eksempelvis bestå i, at formanden for bestyrelsen ikke forklarer lønpolitikkens indhold og dens efterlevelse i sin beretning for virksomhedens øverste organ.

Det foreslås i *§ 43 f, stk. 3,* at firmapensionskassens øverste organ skal godkende aflønningen af virksomhedens bestyrelse for det igangværende regnskabsår.

Det foreslåede indebærer, at virksomhedens øverste organ skal godkende aflønningen af firmapensionskassens bestyrelse for det igangværende regnskabsår særskilt. Der gælder allerede krav om, at bestyrelsesformanden i sin beretning redegør for aflønningen af firmapensionskassens bestyrelse og direktion. I naturlig forlængelse heraf foreslås krav om, at firmapensionskassens øverste ledelsesorgan godkender bestyrelsens aflønning.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelser af § 43 f, stk. 3, straffes med bøde. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Den strafbare handling kan eksempelvis bestå i, at firmapensionskassens øverste organ ikke får forelagt indstillingen om aflønningen af bestyrelsen for det igangværende regnskabsår, hvorefter firmapensionskassen vil kunne straffes herfor.

Det foreslås i *§ 43 f, stk. 4,* at bestyrelsen i en firmapensionskasse årligt skal udarbejde og offentliggøre en vederlagsrapport.

Det foreslåede indebærer, at bestyrelsen skal udarbejde en klar og forståelig vederlagsrapport, som giver et overblik over den samlede aflønning af

ledelsesmedlemmerne i virksomheden i medfør af lønpolitikken, jf. stk. 1. Den samlede aflønning skal forstås som summen af fast og variabel løn, herunder eventuelle godtgørelser og lignende, som hvert medlem af bestyrelsen eller direktionen har optjent.

Alle goder uanset form betragtes i relation til vederlagsrapporten som aflønning, der således også gælder typer af goder, der ikke er nævnt direkte i virksomhedens lønpolitik.

Udover de oplysnings- og offentliggørelseskrav, der stilles i det foreslåede stk. 5-6, stilles der ikke formkrav til, hvordan firmapensionskassen udformer vederlagsrapporten.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelse af § 43 f, stk. 4, straffes med bøde. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Den strafbare handling kan eksempelvis bestå i, at en virksomhed omfattet af bestemmelsen helt undlader at udarbejde en vederlagsrapport.

Det foreslås i *§ 43 f, stk. 5,* at vederlagsrapporten skal indeholde oplysninger nævnt i stk. 5, nr. 1 og 2.

Oplysningerne har til formål at bibringe medlemmerne og øvrige interessenter et bedre grundlag for at vurdere, om der er forbindelse mellem løn og resultater for hvert enkelt ledelsesmedlem.

I medfør af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, kan overtrædelser af det foreslåede § 43 f, stk. 5, straffes med bøde. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Den strafbare handling kan eksempelvis bestå i, at firmapensionskassens vederlagsrapport helt eller delvist ikke indeholder oplysningerne nævnt i stk. 5, nr. 1 og 2.

Det foreslås i *§ 43 f, stk. 5, nr. 1,* at vederlagsrapporten skal indeholde oplysninger om det samlede vederlag, som hvert medlem af bestyrelsen og direktionen har optjent fra firmapensionskassen og andre virksomheder inden for samme koncern i de seneste tre år, herunder oplysninger om fastholdelses- og fratrædelsesordningers væsentligste indhold.

Vederlagsrapporten skal give et samlet overblik over den aflønning, som de enkelte ledelsesmedlemmer, herunder nye og tidligere, har optjent fra firmapensionskassen og andre virksomheder indenfor samme koncern i de seneste tre år. Vederlagsrapporten skal angive de pågældende

ledelsesmedlemmer med navn og skal således oplyse vederlaget fordelt på individniveau.

Ved optjente beløb forstås både faste og variable løndele, som er udbetalt, såvel som løndele, der endnu ikke er kommet til udbetaling.

Der skal ikke kun rapporteres om ledelsesmedlemmer, der har fungeret i et helt regnskabsår eller samtlige af de tre seneste år, men om alle eksisterende, nye og tidligere ledelsesmedlemmer, der har optjent vederlag, som er udbetalt eller endnu ikke er kommet til udbetaling i den pågældende treårige periode. For tidligere ledelsesmedlemmer oplyses også eksempelvis om eventuelle fratrædelsesgodtgørelser, der er blevet udbetalt i perioden efter fratrædelsen.

Vederlagsrapporten må ikke indeholde de særlige kategorier af personoplysninger, som er omhandlet i artikel 9, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen).

Det foreslås i *§ 43 f, stk. 5, nr. 2,* at vederlagsrapporten skal indeholde en redegørelse for sammenhængen mellem ledelsens aflønning og virksomhedens strategi og relevante mål herfor.

Det foreslåede indebærer, at virksomheden i vederlagsrapporten skal beskrive sammenhængen mellem den faktiske aflønning af ledelsen, virksomhedens lønpolitik og de bagvedliggende mål, som aflønningspolitikken understøtter.

Det foreslås i *§ 43 f, stk. 6, 1. pkt.,* at hurtigst muligt efter generalforsamlingens afholdelse skal vederlagsrapporten offentliggøres på firmapensionskassens hjemmeside.

Det betyder, at vederlagsrapporten skal offentliggøres på firmapensionskassens hjemmeside umiddelbart efter generalforsamlingens afholdelse uden unødigt ophold.

Det foreslås i *§ 43 f, stk. 6, 2. pkt.,* at vederlagsrapporten skal forblive offentligt tilgængelig på hjemmesiden i en periode på 10 år.

Offentliggørelse af vederlagsrapporten er nødvendig for, at medlemmerne og øvrige interessenter bedre kan vurdere, hvordan virksomheden gennemfører sin lønpolitik i praksis, herunder aflønningen af de enkelte

ledelsesmedlemmer, og i hvilken udstrækning denne aflønning er afpasset virksomhedens strategi og mål.

Det foreslås i *§ 43 f, stk. 6, 3. pkt.,* at vederlagsrapporten kan være tilgængelig i en længere periode, forudsat at den ikke længere indeholder personoplysninger.

Det foreslåede indebærer, at firmapensionskassens øverste organ kan vælge at lade vederlagsrapporten være tilgængelig i en længere periode end 10 år, forudsat at vederlagsrapporten ikke indeholder personoplysninger.

Det vil i praksis betyde, at der skal laves en version af vederlagsrapporten, hvor det ikke længere fremgår, hvilke ledelsesmedlemmer – nuværende eller tidligere - der har modtaget hvilke vederlag. Dette vil som minimum betyde, at navnene på alle ledelsesmedlemmer skal fjernes fra rapporten.

Overtrædelser af det foreslåede stk. 6 vil kunne straffes med bøde efter det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3. Ansvarssubjektet i forhold til overtrædelser af bestemmelsen er firmapensionskassen. Den strafbare handling kan eksempelvis bestå i, at en firmapensionskasse undlader at offentliggøre vederlagsrapporten, eller at firmapensionskassens vederlagsrapport er offentliggjort i kortere tid end 10 år.

§ 43 g

Det følger af § 19 i bekendtgørelse nr. 16 af 4. januar 2010 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdvirksomheder og firmapensionskasser (aflønningsbekendtgørelsen), at firmapensionskassen, i tilfælde af outsourcing af firmapensionskassens aktiviteter til leverandører efter § 40 i lov om firmapensionskasser, skal sikre, at lønpolitikken overholdes af den virksomhed, som firmapensionskassen har outsourcet aktiviteterne til. Det indebærer, at firmapensionskassen skal sikre, at lønpolitikken skal overholdes for så vidt angår aflønning af ledelsen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, i det omfang aflønningen relaterer sig til arbejde, som er outsourcet fra firmapensionskassen. Det indebærer også, at det skal fremgå af de kontraktuelle forpligtelser mellem firmapensionskassen og virksomheden, som firmapensionskassen har outsourcet til, at lønpolitikken skal overholdes.

Den foreslåede § 43 g viderefører § 19 i aflønningsbekendtgørelsen.

Det følger af det foreslåede *stk. 1, 1. pkt.,* at en firmapensionskasse ved outsourcing af aktiviteter til en leverandør skal sikre, at aflønning af ledelsen

og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, hos leverandøren sker inden for rammerne af firmapensionskassens lønpolitik.

Den foreslåede bestemmelse gennemfører artikel 31, stk. 2 og stk. 3, litra a, i Europa-Parlamentets og Rådets direktiv 2016/2341/EU af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'er) aktiviteter og tilsynet hermed. Det følger heraf, at IORP'erne skal bevare det fulde ansvar for, at forpligtelserne i medfør af dette direktiv opfyldes, når de outsourcer nøglefunktioner eller andre aktiviteter. Outsourcing af nøglefunktioner eller andre aktiviteter må ikke foregå på en måde, der kan føre til forringelse af kvaliteten af ledelsessystemet i den pågældende IORP.

Den foreslåede bestemmelse medfører, at en firmapensionskasse som hidtil skal sikre, at firmapensionskassens lønpolitik overholdes af den leverandør, som firmapensionskassen har outsourcet firmapensionskassens aktiviteter til, herunder outsourcing af nøglefunktioner og ledelse, i det omfang aflønningen relaterer sig til arbejde, som er outsourcet fra firmapensionskassen.

Firmapensionskassen er således ikke forpligtet til at sikre, at den generelle aflønning hos leverandøren, som firmapensionskassen har outsourcet blandt andet nøglefunktioner og ledelse til, efterlever firmapensionskassens lønpolitik. Firmapensionskassens forpligtelse til at sikre, at lønpolitikken overholdes af leverandøren, er begrænset til de tilfælde, hvor firmapensionskassen har outsourcet aktiviteter, der vedrører firmapensionskassens ledelse eller ansatte, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil.

Det er hensigten med bestemmelsen at sikre, at aflønningsreglerne ikke kan omgås ved outsourcing af opgaverne.

Det følger af det foreslåede *§ 43 g, stk. 1, 2. pkt.,* at det skal fremgå af aftalen mellem firmapensionskassen og leverandøren, at firmapensionskassens lønpolitik skal overholdes.

Den foreslåede bestemmelse gennemfører artikel 31, stk. 5, i Europa-Parlamentets og Rådets direktiv 2016/2341/EU af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'er) aktiviteter og tilsynet hermed. Herefter skal IORP'er, der outsourcer nøglefunktioner, ledelse af disse IORP'er eller andre aktiviteter, der er omfattet af dette direktiv, indgå skriftlig aftale med tjenesteyderen. En sådan aftale skal have retsvirkning og skal klart beskrive IORP'ens og tjenesteyderens rettigheder og forpligtelser.

Firmapensionskassen er således forpligtet til at sikre, at det fremgår af aftalen med leverandøren, der outsources aktiviteter til, at firmapensionskassens lønpolitik overholdes i de tilfælde, hvor leverandøren varetager funktioner, hvis ansvarshavende almindeligvis ville være omfattet af firmapensionskassens lønpolitik.

Det følger af det foreslåede *§ 43 g, stk. 2,* at stk. 1 ikke finder anvendelse i det omfang leverandøren allerede er underlagt regler om aflønning i den finansielle regulering.

§ 43 h

Den gældende § 18 i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasse (aflønningsbekendtgørelsen), med senere ændringer, indeholder regler om begrænsninger af brugen af variable løndele for medlemmer af bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil i firmapensionskasser. Overtrædelse af bestemmelsen straffes med bøde, jf. § 29, stk. 1, i aflønningsbekendtgørelsen.

Det foreslås i *§ 43 h, stk. 1, nr. 1,* at firmapensionskasser ved aflønning af bestyrelsen og direktionen skal sikre, at de variable løndele til et medlem af bestyrelsen eller direktionen på tidspunktet for beregningen af den variable løndel højst må udgøre 50 pct. af henholdsvis honoraret eller den faste grundløn inklusive pension.

Bestemmelsen udgør en offentligretlig regulering af firmapensionskassernes pligter, som har indflydelse på den pågældende virksomheds mulighed for at indgå aftaler om variabel løn med medlemmer af bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil.

Firmapensionskassen kan vælge, at den variable løndel skal variere i forhold til bestyrelsen og direktionen. Den variable løndel kan dog ikke overstige den i forslaget fastsatte procentsats.

Loftet på 50 pct. for et medlem af bestyrelsen eller direktionen skal opgøres på beregningstidspunktet, dvs. ved tildeling af en variabel løndel og inden udskydelse af en del af den variable løndel. Overholdelsen af grænsen for variabel løn skal ses i forhold til det indkomstår, hvor den variable løn optjenes.

Der skal være en passende balance mellem variable og faste løndele, så den faste løndel er så tilstrækkelig høj, at det er muligt at føre en fleksibel bonuspolitik, og for at sikre, at ledelsens privatøkonomi ikke skal være afhængig af, at de opnår deres bonus.

Det foreslås i *§ 43 h, stk. 1, nr. 2,* at de variable løndele til firmapensionskassens andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil (væsentlige risikotagere), på beregningstidspunktet højst må udgøre 100 pct. af den faste grundløn, inklusive pension.

Loftet gælder for hver enkelt person.

Loftet på 100 pct. for firmapensionskassens væsentlige risikotagere skal opgøres på beregningstidspunktet, dvs. ved tildeling af en variabel løndel og inden udskydelse af en del af den variable løndel. Overholdelsen af grænsen for variabel løn skal ses i forhold til det indkomstår, hvor den variable løn optjenes. Dette svarer til fremgangsmåden ved opgørelse af loftet på 50 pct. for bestyrelse og direktion, jf. det foreslåede stk. 1, nr. 1.

Der skal være en passende balance mellem variable og faste løndele, så den faste løndel er tilstrækkelig høj til at muliggøre en fleksibel bonuspolitik, og for at sikre, at den ansattes privatøkonomi ikke skal være afhængig af, at de opnår bonus.

Det foreslås i *§ 43 h, stk. 1, nr. 3,* at firmapensionskassens øverste organ kan beslutte, at de variable løndele til firmapensionskassens andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, kan udgøre op til 200 pct. af den faste grundløn inklusive pension, hvis betingelserne i litra a-e er opfyldt. Kravene i de foreslåede litra a-e er kumulative. De skal således alle være opfyldt.

Beslutningen om benyttelse af et højere maksimalt loft kan enten vedrøre alle firmapensionskassens væsentlige risikotagere eller vedrøre en del af disse ansatte, eksempelvis væsentlige risikotagere i en bestemt afdeling. Det øverste organ kan således beslutte, at der skal gælde forskellige maksimale lofter for forskellige grupper af væsentlige risikotagere.

Loftet på 200 pct. for væsentlige risikotagere skal opgøres på beregningstidspunktet, dvs. ved tildeling af en variabel løndel og inden udskydelse af en del af den variable løndel. Overholdelsen af grænsen for variabel løn skal ses i forhold til det indkomstår, hvor den variable løn optjenes. Dette svarer til fremgangsmåden ved opgørelse af loftet på 50 og 100 pct., jf. det foreslåede § 43 h, stk. 1, nr. 1 og 2.

Der skal være en passende balance mellem variable og faste løndele, således at den faste løndel er så tilstrækkelig høj, at det er muligt at føre en fleksibel bonuspolitik, og for at sikre, at den ansattes privatøkonomi ikke skal være afhængig af, at de opnår deres bonus.

Det foreslås i *§ 43 h, stk. 1, nr. 3, litra a*, at firmapensionskassen senest ved indkaldelse til det øverste organs forsamling skal orientere det øverste organ om, at der ønskes stillingtagen til benyttelse af et højere maksimalt loft.

Firmapensionskassens øverste organ er generalforsamlingen. Firmapensionskassen kan benytte de kommunikationsmidler, som firmapensionskassen normalt benytter ved indkaldelse til generalforsamling m.v.

Det foreslås i *§ 43 h, stk. 1, nr. 3, litra b*, at det øverste organ skal træffe beslutning om benyttelse af et højere maksimalt loft på baggrund af en detaljeret anbefaling fra firmapensionskassen, der begrunder indstillingen herom, herunder antallet af berørte ansatte, disses arbejdsområder, det nye foreslåede maksimale loft og den forventede indvirkning på firmapensionskassens mulighed for at bevare et sundt kapitalgrundlag. Medlemmerne af det øverste organ skal modtage anbefalingen senest samtidig med indkaldelsen til det øverste organs forsamling.

Det vil være bestyrelsen, der på firmapensionskassens vegne fremsætter forslaget på generalforsamlingen, og det vil derfor også være bestyrelsen, der er ansvarlig for udarbejdelsen af den detaljerede anbefaling til medlemmerne.

Den detaljerede anbefaling skal gøre medlemmerne i stand til at træffe beslutningen om et højere maksimal loft på et oplyst grundlag, hvor bestyrelsen begrunder sin indstilling til det øverste organ. Væsentlige oplysninger, som eksempelvis hvor mange ansatte, der vil blive berørt af et højere loft samt deres arbejdsområder, skal fremgå af anbefalingen, så medlemmerne bl.a. kan udlede, om det foreslåede højere loft vil gælde for alle firmapensionskassens væsentlige risikotagere eller kun for nogle kategorier af disse, eksempelvis kun for de væsentlige risikotagere i nogle afdelinger i firmapensionskassen.

Desuden skal en vurdering af indvirkningen på firmapensionskassens kapitalgrundlag indgå i anbefalingen, så medlemmerne har mulighed for at inddrage en eventuel indvirkning på værdien af deres ejerandele i beslutningen.

Medlemmerne skal modtage anbefalingen senest samtidig med indkaldelsen til det øverste organs forsamling. Firmapensionskassen kan benytte de kommunikationsmidler, som firmapensionskassen normalt benytter ved indkaldelse til generalforsamling m.v.

Hvis firmapensionskassen ikke senest ved indkaldelsen til det øverste organs forsamling har orienteret det øverste organ om, at der ønskes stillingtagen til benyttelse af et højere maksimalt loft, kan beslutningen på det øverste organs forsamling efter omstændighederne være ugyldig. Det samme gælder, hvis firmapensionskassens bestyrelse ikke senest ved indkaldelsen til det øverste organs forsamling har sendt det øverste organ en detaljeret anbefaling om benyttelse af et højere maksimalt loft.

Det foreslås i *§ 43 h, stk. 1, nr. 3, litra c,* at firmapensionskassen senest samtidig med fremsendelse af anbefalingen til medlemmerne af det øverste organ, jf. det foreslåede litra b, skal informere Finanstilsynet om anbefalingen til medlemmerne, herunder det foreslåede højere maksimale loft og begrundelsen for indstillingen. Firmapensionskassen skal på anmodning fra Finanstilsynet godtgøre, at det foreslåede højere maksimale loft ikke er i strid med firmapensionskassens forpligtelser efter denne lov, herunder særligt kapitalgrundlagskravene.

Finanstilsynet vil i sådanne tilfælde lægge vægt på bestyrelsens drøftelse af forholdene, ligesom Finanstilsynet vil lægge vægt på firmapensionskassens kapitalforhold, herunder firmapensionskassens kapitalgrundlagskrav, solvens og likviditet. Hvis Finanstilsynet vurderer, at der er nærliggende risiko for, at firmapensionskassen som følge af et højere maksimalt loft og en senere udbetaling af en sådan variabel løn ikke vil overholde kapitalgrundlagskravenet eller solvenskravet, kan Finanstilsynet påbyde firmapensionskassen ikke at hæve loftet eller ikke at udbetale den variable løn på udbetalingstidspunktet i overensstemmelse med det foreslåede stk. 1, nr. 6.

Det foreslås i *§ 43 h, stk. 1, nr. 3, litra d, 1.* og *2. pkt.,* at beslutningen om benyttelse af et højere maksimalt loft tiltrædes af firmapensionskassens øverste organ med mindst 66 pct. af de afgivne stemmer, forudsat at mindst 50 pct. af de stemmeberettigede medlemmer er repræsenteret på generalforsamlingen. Hvis mindre end 50 pct. af de stemmeberettigede medlemmer er repræsenteret på generalforsamlingen, skal beslutningen tiltrædes af mindst 75 pct. af de afgivne stemmer.

Majoritetskravet er skærpet i forhold til almindelige beslutninger på generalforsamlingen, som typisk kan tages ved simpelt flertal, jf. eksempelvis § 26 i lov om firmapensionskasser.

Eventuelle stemmeretsbegrænsninger og stemmelofter skal respekteres efter bestemmelsen.

Det foreslås i *§ 43 h, stk. 1, nr. 3, litra d, 3. pkt.,* at en ansat, som er medlem af firmapensionskassen, ikke må deltage i afstemningen herom på det øverste organs forsamling, hvis den ansatte har en væsentlig interesse i beslutningen, der kan være stridende mod firmapensionskassens interesse.

Bestemmelsen følger princippet i § 86 i selskabsloven vedrørende kapitalejeres inhabilitet. Bestemmelsen skal sikre, at medlemmer ikke er med til at tage beslutninger, som de selv har en væsentlig interesse i.

Bestemmelsen er en undtagelse til den generelle regel om, at medlemmer som udgangspunkt frit kan udøve deres indflydelse på firmapensionskassens generalforsamlinger med henblik på at fremme egne interesser. I visse sammenhænge kan interessekonflikten dog være så åbenbar og væsentlig, at medlemmet anses for inhabil.

Et medlem vil kunne være omfattet af inhabilitetsbestemmelsen, hvis beslutningen om benyttelse af et højere maksimalt loft vedrører vedkommende selv, dvs. hvis vedkommende er udpeget som en af firmapensionskassens væsentlige risikotagere, og et eventuelt højere loft f.eks. vil gælde for alle væsentlige risikotagere.

Hvis generalforsamlingen kun skal tage stilling til, om der kan benyttes et højere maksimalt loft for visse ansatte, eksempelvis ansatte i en specifik afdeling, og den pågældende arbejder i en anden afdeling, vil beslutningen ikke vedrøre den ansatte.

Der kan dog forekomme andre situationer, hvor den ansatte er inhabil, uden at beslutningen vedrører vedkommende selv. Hvis beslutningen om forhøjelse af loftet for variabel løn eksempelvis vedrører et nærtstående familiemedlem til et medlem, må medlemmet anses for at være inhabil i forhold hertil.

Hvis beslutningen vedrører en ansat, som også er medlem, må bestyrelsen foretage en vurdering af, om den ansatte har en så åbenbar og væsentlig interesse i beslutningen, at det kan være i strid med firmapensionskassens interesse. Bestyrelsen må således foretage en konkret vurdering af, om beslutningen vedrører generelle medarbejderrelaterede spørgsmål vedrørende en større gruppe af ansatte, som ikke vil føre til inhabilitet, eller om beslutningen særligt angår den enkelte ansatte eller det enkelte medlem eller en mindre gruppe af ansatte eller medlemmer, som kan føre til

inhabilitet. Det vil være afgørende, om beslutningen om benyttelse af et højere maksimalt loft er af så åbenbar og væsentlig betydning for den pågældende, at det må betragtes som tvivlsomt, om den pågældende vil kunne agere uden at lade sig påvirke af sin særlige egeninteresse. Dette kan f.eks. være tilfældet, hvis den pågældende er den eneste væsentlige risikotager i firmapensionskassen, eller hvis den pågældende er den eneste, der vil blive omfattet af et højere maksimalt loft. Bestyrelsens vurdering skal fremgå af bestyrelsens anbefaling til det øverste organ.

Hvis bestyrelsen vurderer, at en beslutning særligt angår den enkelte ansatte eller det enkelte medlem, eller en mindre gruppe af ansatte eller medlemmer, som kan føre til inhabilitet, er det bestyrelsens ansvar at sikre, at dirigenten, inden generalforsamlingen finder sted, får instruktion om, hvilke enkelte ansatte eller medlemmer, der efter bestyrelsens opfattelse vil være afskåret fra at deltage i afstemningen om forhøjelse af loft for variabel løn. Dette ændrer ikke på, at det ifølge selskabslovgivningens regler er det enkelte medlem, der selv har ansvaret for at vurdere, om vedkommende er inhabil.

En overtrædelse af det foreslåede nr. 3, litra d, kan efter omstændighederne medføre, at det øverste organs beslutning om et højere maksimalt loft må anses som ugyldig.

Det foreslås i *§ 43 h, stk. 1, nr. 3, litra e,* at firmapensionskassen senest 8 dage efter det øverste organs forsamling skal informere Finanstilsynet om det øverste organs beslutning, herunder om størrelsen på et eventuelt besluttet højere maksimalt loft.

Firmapensionskassen skal informere Finanstilsynet, både hvis det øverste organ beslutter at benytte et højere maksimalt loft for enten alle eller en del af firmapensionskassens væsentlige risikotagere, og hvis det øverste organ beslutter ikke at følge indstillingen ved ikke at vedtage forslaget med den krævede majoritet, jf. det foreslåede litra d ovenfor.

Det følger af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, at overtrædelse af § 43 h, stk. 1, kan straffes med bøde. Overtrædelser kan eksempelvis bestå i, at en firmapensionskasse tildeler sin bestyrelse og direktion over 50 pct. af dennes faste løn eller honorar i variabel aflønning eller undlader at informere Finanstilsynet om firmapensionskassens vedtagelse af et højere maksimalt loft for variabel aflønning til væsentlige risikotagere. En overtrædelse af de foreslåede nr. 3, litra c-e, kan i øvrigt efter omstændighederne medføre, at det øverste organs beslutning om et højere maksimalt loft må anses som ugyldig.

Det foreslås i *§ 43 h, stk. 1, nr. 4*, at mindst 50 pct. af en variabel løndel til bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, på tidspunktet for beregningen af den variable løn skal bestå af en balance af finansielle instrumenter. Balancen af finansielle instrumenter kan udgøres af efterstillet gæld i firmapensionskassen eller andre instrumenter, som i passende grad afspejler firmapensionskassens kreditværdighed som en firmapensionskasse, hvis aktivitet formodes at fortsætte. Instrumenterne kan udstedes i firmapensionskassen eller dennes modervirksomhed, der ejer firmapensionskassen fuldt ud.

Mindst 50 pct. af den variable løn vil skulle bestå af en balance af de nævnte typer af instrumenter. Ved vurderingen af om der foreligger en balance mellem de nævnte typer af instrumenter, må der tages hensyn til, hvilke typer af instrumenter det er muligt at benytte ud fra firmapensionskassens juridiske struktur og størrelse, samt hvad der afspejler firmapensionskassens kreditværdighed, ligesom der må tages hensyn til, at det kan være hensigtsmæssigt at benytte flere forskellige typer af instrumenter for på bedste vis at sikre en langsigtet interesse, herunder set ud fra en proportionalitetsbetragtning i forhold til bl.a. størrelsen af den variable løndel. Efter Finanstilsynets praksis kan en balance af instrumenter bestå af et enkelt finansielt produkt, hvis firmapensionskassen kan give en passende begrundelse herfor.

Kravet om, at mindst 50 pct. af den variable løn skal bestå af finansielle instrumenter, skal ses i forhold til tidspunktet for beregningen af den variable løndel (beregningstidspunktet), jf. bemærkningerne til det foreslåede stk. 1, nr. 5, hvor der angives et eksempel på samspillet mellem reglerne i det foreslåede stk. 1, nr. 4 og nr. 5. Ved beregningstidspunktet forstås det tidspunkt, hvor opgørelsen af den variable løn foretages i henhold til kriterier, der ligger til grund for beregningen af den variable løns størrelse i henhold til aftalen mellem firmapensionskassen og den pågældende modtager (direktør, væsentlig risikotager mv.).

Ved fordelingen af den beregnede variable løndel på henholdsvis kontanter og finansielle instrumenter skal værdiansættelsen af de pågældende instrumenter ske efter anerkendte værdiansættelsesprincipper, som eksempelvis Black-Scholes modellen. Det foreslåede stk. 1, nr. 4, skal ses i sammenhæng med det foreslåede stk. 3, hvorefter firmapensionskassen skal sikre sig, at finansielle instrumenter, der overdrages til personer omfattet af stk. 1 som en del af den variable løn i medfør af det foreslåede stk. 1, nr. 4, ikke må afhændes af disse personer i en passende periode. Forslaget er udtryk for, at man vil sikre, at bestyrelsen og direktionen samt firmapensionskassens andre væsentlige risikotagere har samme økonomiske

incitamenter som en langsigtet investor. Modtager direktøren i en firmapensionskasse en variabel løn, hvoraf halvdelen består af eksempelvis aktier i firmapensionskassens modervirksomhed, må det antages, at direktørens interesse i, at aktiekursen i firmapensionskassen stiger, øges. Tilsvarende må det antages, at interessen heri udstrækkes over en længere periode, hvis det ikke er muligt for direktøren at afhænde aktierne i en af firmapensionskassen fastsat passende periode. I det tilfælde, hvor aflønningen sker i aktier, har direktøren ligeledes i samme periode en interesse i, at aktien ikke falder.

Det foreslås i *§ 43 h, stk. 1, nr. 5, 1. pkt.,* at firmapensionskassens udbetaling af mindst 40 pct., eller ved større beløb mindst 60 pct., af en variabel løndel skal ske over en periode på mindst fire år med påbegyndelse 1 år efter beregningstidspunktet, dog for bestyrelsen og direktionen mindst fem år.

Den foreslåede bestemmelse indebærer, at firmapensionskassen skal sikre, at udbetaling af mindst 40 pct. af den variable løn skal udskydes over en periode på mindst fire år med påbegyndelse 1 år efter beregningstidspunktet. For bestyrelsen og direktionen skal perioden dog mindst være fem år, med en ligelig fordeling over årene eller med en voksende andel i slutningen af udskydelsesperioden. Ved større variable løndele foreslås det, at mindst 60 pct. af den variable løn skal udskydes på samme måde.

Der er som udgangspunkt tale om større variable løndele, hvis den samlede variable løn før skat overstiger 750.000 kr. om året. For variable løndele, der ikke overstiger 750.000 kr. om året, må firmapensionskassen foretage en vurdering af, om de variable løndele konkret må anses for "større beløb". Ved vurderingen kan der lægges vægt på sammenhængen med den pågældendes løn og risikoprofil i øvrigt.

Bestemmelsen i det foreslåede stk. 1, nr. 5, skal forstås således, at udbetalingen af den udskudte del af den variable løn først kan påbegyndes et år efter, at den variable løn er beregnet (beregningstidspunktet). Det betyder, at den del af den beregnede variable løn, der ikke udskydes, kan udbetales i umiddelbar forlængelse af beregningen. Ved "beregningstidspunktet" forstås det tidspunkt, hvor opgørelsen af den variable løn, der sker i henhold til de kriterier, der ligger til grund for beregningen af den variable løns størrelse i henhold til aftalen mellem virksomheden og den pågældende modtager (direktør, væsentlig risikotager m.v.), foretages.

Endvidere forudsættes det i bestemmelsen, at den udskudte del af den variable løn udbetales i intervaller med et års mellemrum, da der skal være et passende tidsrum imellem udbetalingerne til at vurdere, om

forudsætningerne har ændret sig, således at den udskudte del af den variable løn ikke skal udbetales helt eller delvist.

Formålet med bestemmelsen er at sikre, at en variabel løn, der baserer sig på kortsigtede resultater, eksempelvis resultater opnået på baggrund af en investering i indtjeningsåret, bliver justeret for de risici, der viser sig ved den pågældende investering i årene efter. Da tidshorisonten for firmapensionskassens realisering af fortjenester og tab som følge af forskellige typer af aktiviteter varierer, skal der være en tilsvarende mulighed for udskydelse af udbetalingen af en del af den relaterede variable løn til den pågældende medarbejder, der har været involveret i aktiviteterne. Ved at udskyde udbetalingen af som minimum 40-60 pct. af den beregnede variable løndel, sikres det, at firmapensionskassen får mulighed for at justere for de langsigtede virkninger, som en given investering medfører.

Da bestemmelsens formål er at begrænse muligheden for at opnå en variabel løn på baggrund af en kortsigtet indsats eller investering, der på længere sigt viser sig at være tabsgivende for firmapensionskassen, skal bestemmelsen endvidere ses i sammenhæng med det foreslåede stk. 4. Firmapensionskassen skal i henhold til det forslåede stk. 4, sikre, at udbetaling af den udskudte del af den variable løn til medlemmer af bestyrelsen, direktionen og firmapensionskassens andre væsentlige risikotagere er betinget af, at de kriterier, der har dannet grundlag for beregningen af den variable løn, fortsat er opfyldt, herunder at firmapensionskassens økonomiske situation ikke er væsentligt forringet i forhold til tidspunktet for beregningen af den variable løndel.

Den periode, der ligger til grund for beregningen, må gerne strække sig over mere end et år, jf. bemærkningerne til det foreslåede stk. 4.

Det foreslås i *§ 43 h, stk. 1, nr. 5, 2. pkt.,* at udbetalingen skal ske med en ligelig fordeling over årene eller med en voksende andel i slutningen af perioden.

Den foreslåede bestemmelse indebærer, at den del af den variable løn, der skal udskydes, skal udskydes med en ligelig fordeling, eller med en voksende andel i slutningen af perioden, over mindst fire år for virksomhedens væsentlige risikotagere og for bestyrelsen og direktionen over mindst fem år. Det er muligt for firmapensionskassen at aftale en længere periode med den pågældende modtager, hvis firmapensionskassen eksempelvis vurderer, at de risici, der er knyttet til denne modtagers aktiviteter, har en længere tidshorisont end fire år. Det er dog ikke muligt at aftale en kortere periode end fire år. For bestyrelsen og direktionen kan der ikke aftales en kortere periode end fem år. Bestemmelsen skal endvidere forstås således, at det er muligt for firmapensionskassen at aftale med

modtageren, at der udskydes mere end en fjerdedel om året, således at der eksempelvis i det sidste år udbetales tre fjerdedele. Det er således alene et mindstekrav, at fordelingen skal være ligelig over årene.

Bestemmelsen om udskydelse gælder også for den del af den variable løn, der består af finansielle instrumenter, der afspejler firmapensionskassens kreditværdighed, jf. forslaget til stk. 1, nr. 4.

I det følgende gennemgås et eksempel på samspillet mellem forslaget til stk. 1, nr. 4 og 5. Eksemplet tager udgangspunkt i, at der i forlængelse af år 0, dvs. beregningsåret, udbetales en fast grundløn inklusive pension på 2 mio. kr. til en direktør i en firmapensionskasse. Direktørens variable løndel udgør samme år 750 t.kr. efter aftale mellem direktøren og firmapensionskassen.

Som følge af forslaget til § 43 h, stk. 1, nr. 1, må den variable løndel i dette eksempel maksimalt udgøre 1 mio. kr. Den beregnede variable løn på 750 t.kr. overholder derfor grænsen.

Ifølge forslaget til § 43 h, stk. 1, nr. 4, skal mindst 50 pct. af den variable løndel – dvs. 375 t.kr. – bestå af eksempelvis efterstillet gæld. Det følger endvidere af § 43 h, stk. 3, at når disse gældsbreve er overdraget til direktøren, må direktøren ikke indfri disse i en passende periode, der fastsættes af firmapensionskassen.

Der tages i eksemplet udgangspunkt i, at der for direktøren er tale om en større variabel løndel, hvorfor 60 pct. af den variable løndel skal udskydes over en periode på mindst fem år med en ligelig fordeling over årene, jf. forslaget til § 43 h, stk. 1, nr. 5. Der skal således udskydes mindst 450 t.kr., som fordeles ligeligt over en periode på mindst fem år – dvs. 90 t.kr. pr år. Den del af den beregnede variable løn (300 t.kr.), der ikke skal udskydes i medfør af stk. 1, nr. 5, kan udbetales i forlængelse af beregningen.

Kravet om, at mindst halvdelen af den variable løn skal bestå af finansielle instrumenter, der afspejler firmapensionskassens kreditværdighed, gælder både den del af den beregnede variable løn, der udskydes og den del, der udbetales i forlængelse af beregningen. Firmapensionskassen kan altså ikke nøjes med at udskyde den kontante del af den variable løn. Den variable løndel, der udskydes, skal således bestå ligeligt af kontanter og finansielle instrumenter på beregningstidspunktet.

Lovforslagets krav kan opfyldes ved udbetaling af den variable løn med følgende fordeling:

Skema 1

Løndel, der udbetales	År 0 (beregningsåret)	År 1	År 2	År 3	År 4	År 5	I alt
Kontant	150 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	375 t.kr.
Efterstillet gæld	150 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	375 t.kr.
I alt	300 t.kr.	90 t.kr.	90 t.kr.	90 t.kr.	90 t.kr.	90 t.kr.	750 t.kr.

Skema 1 viser, at der i forlængelse af det år, hvor den variable løn beregnes (beregningsåret), udbetales 150 t.kr kontant og overdrages efterstillet gæld til en værdi af 150 t.kr. til direktøren, svarende til 40 pct. af den samlede variable løn på 750 t.kr. Skemaet viser også, at udbetalingen af den efterstillede gæld skal udbetales over en periode på fem år med en ligelig fordeling over årene eller alternativt med en voksende andel i slutningen af perioden.

Både den del af aktierne, som overdrages til direktøren i forlængelse af beregningsåret og den del af aktierne, der først overdrages til direktøren i år et-fem, skal underlægges en passende tilbageholdelsesperiode, hvor disse ikke kan afhændes af direktøren, jf. det foreslåede § 43 h, stk. 3. Det er firmapensionskassen, der vurderer, hvad der skal forstås ved en passende periode i overensstemmelse med det foreslåede § 43 h, stk. 3.

I eksemplet i skema 2 anvendes aktier og aktieoptioner i modervirksomheden som instrumenter. I eksemplet er der tale om en direktør, alene 12,5 pct. af den faste grundløn, inklusive pension, vil derfor kunne bestå af aktieoptioner eller tilsvarende instrumenter, jf. det foreslåede § 43 h, stk. 2. Det betyder, at værdien af aktieoptionerne i eksemplet maksimalt kan udgøre 250 t.kr. svarende til en tredjedel af direktørens variable løn og 12,5 pct. af den faste grundløn inklusive pension. Som ved aktier skal der ved aktieoptioner, der skal udskydes, tages udgangspunkt i værdien på beregningstidspunktet (efter opgørelsen af beregningen i år 0). Der skal på dette tidspunkt foretages en beregning af, hvor mange aktieoptioner i firmapensionskassen direktøren ville få overdraget for et beløb maksimalt svarende til 250 t.kr. Firmapensionskassen i eksemplet vælger dog, at aktieoptionerne alene skal udgøre halvdelen af de tildelte aktiers værdi, og overdrager således aktieoptioner svarende til en værdi af 75 t.kr. i forlængelse af beregningsåret. Værdiansættelsen af aktieoptionerne skal ske efter anerkendte værdiansættelsesprincipper, såsom Black-Scholes modellen. Den resterende del af aktieoptionerne, hvis værdi udgør 112,5 t.kr., overdrages ligeligt med 22,5 t.kr. over de fem følgende år, og det er

direktøren, som bærer risikoen for, at disses aktieoptionernes værdi ændres i udskydelsesperioden.

Lovforslagets krav kan opfyldes ved udbetaling af den variable løn med følgende fordeling:

Skema 2							
Løndel	År 0 (beregningsåret)	År 1	År 2	År 3	År 4	År 5	I alt
Kontant	150 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	45 t.kr.	375 t.kr.
Aktier m.v.	75 t.kr.	22,5 t.kr.	22,5 t.kr.	22,5 t.kr.	22,5 t.kr.	22,5 t.kr.	187,5 t.kr.
Aktieoptioner	75 t.kr.	22,5 t.kr.	22,5 t.kr.	22,5 t.kr.	22,5 t.kr.	22,5 t.kr.	187,5 t.kr.
I alt	300 t.kr.	90 t.kr.	90 t.kr.	90 t.kr.	90 t.kr.	90 t.kr.	750 t.kr.

I forhold til den efterfølgende tilbageholdelsesperiode gælder den tilsvarende bestemmelse i det foreslåede § 43 h, stk. 3, hvorefter firmapensionskassen skal fastsætte en passende periode, hvori direktøren ikke kan udnytte eller afhænde de aktieoptioner, der er overdraget til direktøren. Eksempelvis vil de aktieoptioner, direktøren modtager efter udløbet af år 1, ikke kunne udnyttes eller afhændes før tilbageholdelsesperioden, som er fastsat af firmapensionskassen, er udløbet.

Kravet om udskydelse af en del af den variable løn i stk. 1, nr. 5, betyder, at den faktiske variable løn, som direktøren får rådighed over et givent indkomstår, både består af den del af den variable løn, som er udbetalt i året, samt den del af den udskudte variable løn fra tidligere indkomstår, som udbetales i det pågældende år. Det vil sige, at den samlede udbetalte variable løn, der relaterer sig til et givent indkomstår, kan overstige 50 pct. af den faste løn inklusive pension i dette indkomstår, uden at dette vil være i strid med grænsen på 50 pct. i § 43 h, stk. 1, nr. 1.

Kravet om udskydelse i det foreslåede stk. 1, nr. 5, rejser spørgsmål i forhold til, hvornår modtageren skal beskattes. Det skatteretlige udgangspunkt er, at en indtægt beskattes, når modtageren har erhvervet endelig ret til indtægten (retserhvervelsestidspunktet). Forslaget om udskydelse af en del af den variable løn skal ses i sammenhæng med kravet i det foreslåede stk. 4 om, at firmapensionskassen i aftalen med modtageren skal sikre sig, at udbetalingen af den udskudte del af den variable løn er betinget af, at de

kriterier, der har dannet grundlag for beregningen af den variable løn, fortsat er opfyldt ved udbetalingen af den udskudte del samt betinget af, at firmapensionskassens økonomiske situation ikke er væsentligt forringet i forhold til tidspunktet for beregningen af den variable løndel.

Efter stk. 4, er det således et krav, at firmapensionskassen knytter betingelser til aftalen om den udskudte variable løn, der har en sådan karakter, at der hersker reel usikkerhed om, hvorvidt aftalen bliver gennemført – eksempelvis opfyldelsen af økonomiske mål. En aftale med modtageren, der indeholder en sådan reel usikkerhed omkring aftalens gennemførelse, og hvor betingelserne for udbetalingen af den udskudte del ikke er betingelser, som modtageren selv har kontrol over, vil udskyde den skattemæssige retserhvervelse, indtil betingelserne er opfyldt. Modtageren vil i sådanne tilfælde ikke skulle beskattes af den udskudte del af den variable løn, før den er endeligt retserhvervet. Det beror på en konkret vurdering i forhold til den enkelte lønaftale, om betingelserne er af en sådan karakter, at der foreligger en reel usikkerhed om, hvorvidt disse opfyldes.

I forhold til beregning af feriegodtgørelse af den udskudte variable løndel, fremgår det af ferieloven, at dette alene sker i forhold til indkomstskattepligtige beløb.

Det foreslås i *§ 43 h, stk. 1, nr. 6,* at firmapensionskassen skal sikre, at firmapensionskassen kan undlade at udbetale en variabel løndel helt eller delvis, hvis firmapensionskassen på tidspunktet for udbetaling af den variable løn ikke overholder solvenskapitalkravet i § 54, eller Finanstilsynet vurderer, at der er nærliggende risiko herfor.

Det følger af forslaget sammenholdt med den foreslåede generelle hjemmel i lovens § 97 til at udstede påbud mv. ved overtrædelser af loven, at Finanstilsynet kan påbyde firmapensionskassen at benytte det foreslåede stk. 1, nr. 6, hvis solvenskapitalkravet ikke er opfyldt, eller hvis Finanstilsynet vurderer, at der er nærliggende risiko herfor. Det vil eksempelvis kunne være tilfældet, hvis en firmapensionskasse med en lav solvens står overfor at skulle udbetale større summer i variabel løn. Finanstilsynet vil i disse tilfælde kunne påbyde firmapensionskassen at reducere sin udbetaling af den variable løn, eksempelvis til en nærmere angivet procentdel af firmapensionskassens indtjening. Bestemmelsen er, i modsætning til det foreslåede stk. 1, nr. 7, ikke til hinder for, at de personer, der på baggrund af bestemmelsen har fået reduceret deres variable løn helt eller delvist, får udbetalt den resterende del af den variable løn på et senere tidspunkt, hvis der ikke længere er nærliggende risiko for, at firmapensionskassen herved ikke overholder solvenskapitalkravet.

Det foreslås i *§ 43 h, stk. 1, nr. 7,* at firmapensionskassen skal sikre, at firmapensionskassen ikke udbetaler variabel løn til medlemmer af bestyrelsen og direktionen, hvis Finanstilsynet i medfør af § 83 kræver, at virksomheden udarbejder en plan for genoprettelse af firmapensionskassens økonomiske stilling.

Forslaget betyder, at firmapensionskassen skal aftale med bestyrelsen og direktionen, at disses ret til variabel løn bortfalder, hvis Finanstilsynet, i den periode hvor aftalen løber, stiller krav efter § 83 i lov om firmapensionskasser. Retten til den variable løn vil således ikke genopstå, hvis firmapensionskassen opfylder minimumsbasiskapitalen indenfor den frist, Finanstilsynet har fastsat.

Det følger af det foreslåede § 117, stk. 2, at overtrædelse af § 43 h, stk. 1, kan straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af det foreslåede § 43 h, stk. 1, er firmapensionskassen. Firmapensionskassen vil eksempelvis kunne straffes med bøde, hvis firmapensionskassen ikke overholder forpligtelserne i nr. 1-7. Dette vil eksempelvis være tilfældet, hvis virksomheden ikke sikrer, at udbetalingsbegrænsningerne for variabel løn overholdes. Firmapensionskassen kan således straffes med bøde, hvis en direktørs variable løndel overstiger 50 pct. af vedkommendes faste løn inklusive pension, eller hvis ikke 50 pct. af direktørens variable løndel er givet i instrumenter på tidspunktet for beregningen.

Det foreslås i *§ 43 h, stk. 2,* at aktieoptioner eller lignende instrumenter for bestyrelsen og direktionen i firmapensionskassen højst må udgøre 12,5 pct. af henholdsvis honoraret og den faste grundløn inklusive pension på tidspunktet for beregningen heraf.

Aktieoptionerne kan gives i firmapensionskassens modervirksomhed.

Grænsen på 12,5 pct. skal ses i forhold til aktieoptionernes værdi på tidspunktet for beregningen af den variable løn (beregningstidspunktet). Den faktiske værdi af aktieoptionerne på udnyttelsestidspunktet kan være væsentligt større eller væsentligt mindre. Bestemmelsen betyder, at i de tilfælde, hvor firmapensionskassen alene ønsker at tildele variabel løn i form af aktieoptioner, kan bestyrelsen og direktionen alene modtage op til 12,5 pct. i variabel løn. Den foreslåede begrænsning af brugen af aktieoptioner til bestyrelsen og direktionen udelukker ikke firmapensionskassen fra, udover at tildele aktieoptioner, samtidig at tildele anden form for variabel løn til disse personer, når blot grænsen på 50 pct. i stk. 1, nr. 1, overholdes.

Ved lignende instrumenter i det foreslåede stk. 2, skal forstås, instrumenter, der i lighed med aktieoptioner kan have en struktur, der kan medføre overdreven risikotagning.

Det følger af det foreslåede § 117, stk. 2, at overtrædelse af § 43 h, stk. 2, kan straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af det foreslåede § 43 h, stk. 2, er firmapensionskassen. Firmapensionskassen vil kunne straffes med bøde, hvis et medlem af bestyrelsen eller direktionen modtager aktieoptioner eller lignende instrumenter, der udgør mere en 12,5 pct. af henholdsvis honoraret eller den faste løn inklusive pension på tidspunktet for beregningen.

Det foreslås i *§ 43 h, stk. 3*, at firmapensionskassen skal sikre sig, at efterstillet gæld og instrumenter m.v., der overdrages til bestyrelsen, direktionen eller andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil som en del af den variable løn efter det foreslåede stk. 1, nr. 4, ikke må afhændes af disse personer i en passende periode.

Bestemmelsen understøtter forslaget i stk. 1, nr. 4, om, at mindst halvdelen af den variable løn skal udbetales i efterstillet gæld og andre instrumenter med det formål at sikre, at bestyrelsen, direktionen og de øvrige ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil (væsentlige risikotagere), har samme økonomiske incitamenter som en langsigtet investor.

Forpligtelsen til ikke at afhænde gældsbreve m.v. i en passende periode, som er nærmere fastsat af firmapensionskassen, skal reguleres i aftalen mellem modtageren og firmapensionskassen.

Firmapensionskassen skal i forhold til det enkelte bestyrelsesmedlem, direktionsmedlem, ansatte eller grupper af ansatte, vurdere, hvad der må anses for en passende periode. Det hensyn, der skal varetages ved en sådan passende tilbageholdelsesperiode, er, at firmapensionskassens mere langsigtede interesser på denne måde tilgodeses. Se bemærkningerne til stk. 1, nr. 5, hvor der gennemgås et eksempel på samspillet mellem kravene i stk. 1, nr. 4 og 5.

Det følger af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, at overtrædelse af § 43 h, stk. 3, kan straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af det foreslåede § 43 h, stk. 3, er firmapensionskassen. Overtrædelser kan eksempelvis bestå i, at firmapensionskassen ikke har sikret, at den del af den variable løn, som er givet i instrumenter, har været tilbageholdt i en passende periode.

Det foreslås i *§ 43 h, stk. 4*, at en firmapensionskasse skal sikre, at udbetaling af den efter stk. 1, nr. 5, udskudte variable løndel til bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil, er betinget af, at de kriterier, der har dannet

grundlag for beregningen af den variable løndel, fortsat er opfyldt på udbetalingstidspunktet betinget af, at den pågældende ikke har deltaget i eller været ansvarlig for en adfærd, der har resulteret i betydelige tab for virksomheden, eller ikke har efterlevet passende krav til hæderlighed samt betinget af, at virksomhedens økonomiske situation ikke er væsentligt forringet i forhold til tidspunktet for beregningen af den variable løndel.

Den foreslåede bestemmelse indebærer, at firmapensionskassens udbetaling af den efter stk. 1, nr. 5, udskudte variable løndel betinges af opfyldelsen af tre kriterier.

For det første skal firmapensionskassen sikre, at udbetalingen er betinget af, at de kriterier, der har dannet grundlag for beregningen af den variable løndel, fortsat er opfyldt på udbetalingstidspunktet. Det indebærer, at den udskudte del af den variable løn alene udbetales eller overdrages, hvis dette er holdbart set i forhold til firmapensionskassens økonomiske situation som helhed, samt hvis det kan begrundes i de resultater, som forretningsafdelingen og den modtagende medarbejder har leveret. Den variable løn skal, under hensyn til aftale- og ansættelsesretlige principper, kunne reduceres væsentligt, hvis firmapensionskassen leverer et væsentligt underskud.

For det andet skal firmapensionskassen sikre, at udbetalingen betinges af, at den pågældende ikke har deltaget i eller været ansvarlig for en adfærd, der har resulteret i betydelige tab for firmapensionskassen, eller ikke har efterlevet passende krav til hæderlighed. Det indebærer, at det indgår som en betingelse i vurderingen af, om den udskudte variable løndel skal udbetales, om den pågældende har deltaget i eller været ansvarlig for en adfærd, der har resulteret i betydelige tab for firmapensionskassen, eller ikke har efterlevet kravene til egnethed og hæderlighed.

Betingelsen har den betydning, at selv i en situation, hvor firmapensionskassen har haft et bonusudløsende resultat, og både den pågældende og dennes afdeling har opfyldt sine øvrige resultatlønsforpligtelser (performet), kan den pågældende miste retten til op til 100 pct. af den udskudte variable løndel, hvis betingelsen ikke er opfyldt.

I forhold til, at den pågældende ikke må have deltaget i eller været ansvarlig for en adfærd, der har resulteret i betydelige tab for firmapensionskassen set i forhold til størrelsen af firmapensionskassens kapitalgrundlag, kan dette eksempelvis være tab som følge af retssager med baggrund i den pågældendes adfærd. Det kan også være tab, firmapensionskassen har lidt, f.eks. som følge af uansvarlige investeringer og långivning eller mangelfuld rådgivning af kunder eller lignende.

Derudover skal det indgå i vurderingen, om vedkommende har efterlevet kravene til egnethed og hæderlighed, jf. § 42, stk. 1.

Ved indtræden i hvervet eller stillingen gælder der for medlemmer af bestyrelsen og direktionen krav om godkendelse efter reglerne om egnethed og hæderlighed i § 42, stk. 1, ligesom der må foretages en fornyet vurdering, hvis forholdene efterfølgende ændres. Både for personer, der er omfattet af egnetheds- og hæderlighedskravene, og for andre ansatte, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil, vil vurderingen i høj grad svare til den vurdering, som foretages efter § 42, stk. 1, uden at der dog er tale om en egentlig egnetheds- og hæderlighedsvurdering.

Det må således vurderes, om den pågældende har udvist eller udviser en adfærd, hvor der er grund til at antage, at vedkommende ikke har varetaget eller vil varetage stillingen på en forsvarlig måde.

I det omfang væsentlige risikotagere udfører opgaver, der er fastlagt i den finansielle regulering, vil varetagelsen af opgaverne tillige indgå i en vurdering af de pågældendes adfærd. Vurderingen skal foretages på udbetalingstidspunktet efter udskydelsesperiodens udløb.

For det tredje, skal firmapensionskassen sikre, at udbetalingen betinges af, at firmapensionskassens økonomiske situation ikke er væsentligt forringet i forhold til tidspunktet for beregningen af den variable løndel (backtesting).

Reduktion eller bortfald af den variable løndel skal ske, hvis blot en af betingelserne om udløsning af tab eller manglende opfyldelse af kravene til egnethed og hæderlighed, eller en af de allerede gældende betingelser vedrørende opfyldelsen af kriterier, der har dannet grundlag for beregning af den variable løndel, eller vedrørende firmapensionskassens økonomiske situation, er opfyldt.

Som nævnt i bemærkningerne til det foreslåede til stk. 1, nr. 5, er det skatteretlige udgangspunkt, at en indtægt beskattes, når modtageren har erhvervet endelig ret til indtægten (retserhvervelsestidspunktet). Forslaget til stk. 4 skal derfor ses i sammenhæng med stk. 1, nr. 5.

Det følger af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, at overtrædelse af § 43 h, stk. 4, kan straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af det foreslåede § 43 h, stk. 4, er firmapensionskassen. Den strafbare handling består eksempelvis i, at firmapensionskassen i forbindelse med udbetalingen af den udskudte variable løndel ikke foretager en vurdering af, om de kriterier, der dannede grundlag for beregningen af den variable løn, fortsat er opfyldt på

udbetalingstidspunktet. Firmapensionskassen vil eksempelvis kunne straffes med bøde, hvis firmapensionskassen ikke har reduceret den udskudte variable løndel i forbindelse med udbetalingen heraf, hvis firmapensionskassens økonomiske situation er væsentligt forringet på udbetalingstidspunktet set i forhold til beregningstidspunktet.

Det foreslås i *§ 43 h, stk. 5,* at firmapensionskassen skal sikre sig, at bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, som modtager variabel løn, skal tilbagebetale den variable løn helt eller delvis, hvis den variable løn er udbetalt på grundlag af oplysninger om resultater, som kan dokumenteres at være fejlagtige, og hvis modtageren er i ond tro (clawback).

Det følger af den foreslåede bestemmelse, at hel eller delvis tilbagebetaling af allerede udbetalt variabel løn skal ske i de tilfælde, hvor den variable løn er udbetalt på grundlag af oplysninger om resultater, som kan dokumenteres at være fejlagtige, og modtageren er i ond tro herom.

Krav om tilbagebetaling skal stilles under hensyn til almindelige aftale- og ansættelsesretlige principper, herunder retsgrundsætningen om condictio indebiti. Det betyder, at det er en afgørende forudsætning for, om firmapensionskassen kan kræve tilbagebetaling af allerede udbetalt variabel løn, at modtageren har været i ond tro – eksempelvis i det tilfælde, hvor modtageren af den variable løn bevidst har været med til at afgive fejlagtige oplysninger om resultater, der ligger til grund for beregningen af modtagerens variable løn.

Det følger af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, at overtrædelse af § 43 h, stk. 5, kan straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af det foreslåede § 43 h, stk. 5, er firmapensionskassen. Den strafbare handling kan eksempelvis bestå i, at en direktør har fået udbetalt variabel løn på grundlag af oplysninger om resultater, som kan dokumenteres at være fejlagtige, og direktøren har været i ond tro herom, og firmapensionskassen ikke har krævet en sådan variabel løn tilbagebetalt.

Det foreslås i *§ 43 h, stk. 6, 1. pkt.,* at firmapensionskassen skal sikre, at hvis bestyrelsen, direktionen og andre ansatte, hvis aktiviteter har væsentlig indflydelse på firmapensionskassens risikoprofil, tildeles en pensionsydelse, som udgør variabel løn, jf. § 3, stk. 1, nr. 28, skal firmapensionskassen, hvis modtageren forlader firmapensionskassen inden pensionstidspunktet, beholde denne pensionsydelse i form af instrumenter som nævnt i stk. 1, nr. 4, i fem år.

Den foreslåede bestemmelse finder anvendelse i tilfælde, hvor et medlem af bestyrelsen eller direktionen eller en ansat, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil, modtager pension efter en ydelsesbaseret ordning, og hvor denne pension helt eller delvist kan sidestilles med variable løn. Der er således ikke tale om pensionsbidragsordninger.

Det følger af bestemmelsen, at firmapensionskassen skal sikre, at hvis medlemmer af bestyrelsen og direktionen eller andre væsentlige risikotagere, tildeles en pensionsydelse, som helt eller delvist kan sidestilles med variabel løn, skal firmapensionskassen, hvis modtageren forlader firmapensionskassen inden pensionstidspunktet, beholde denne del af pensionsydelsen i fem år i form af instrumenter som nævnt i forslaget til stk. 1, nr. 4 (instrumentkravet).

Formålet med denne udskudte betaling er den samme som i forslaget til stk. 1, nr. 5, om udskydelse af en del af den variable løn (udskydelseskravet).

Det foreslås i *§ 43 h, stk. 6, 2. pkt.*, at stk. 4 og 5 finder anvendelse på de i 1. pkt. nævnte tilfælde.

Den foreslåede bestemmelse indebærer, at kravene om backtesting og clawback i forslagets stk. 4 og 5 finder anvendelse for en pensionsydelse som helt eller delvist kan sidestilles med variabel løn og som tilbageholdes af firmapensionskassen i form af instrumenter i fem år, i de tilfælde hvor modtageren har forladt firmapensionskassen inden pensionstidspunktet. Det medfører, at firmapensionskassen skal sikre, at kriterierne, der dannede grundlag for beregningen af den variable pensionsydelse, fortsat er opfyldt på udbetalingstidspunktet.

Udbetalingen af pensionsydelsen vil endvidere være betinget af, at modtageren har efterlevet kravene til hæderlighed, ikke har deltaget i eller været ansvarlig for en adfærd, der har resulteret i betydelige tab for firmapensionskassen, og at firmapensionskassens økonomiske situation ikke er væsentligt forringet i forhold til beregningstidspunktet af pensionsydelsen. Firmapensionskassen skal i øvrigt sikre sig, at modtageren af en variabel pensionsydelse skal tilbagebetale denne helt eller delvist, hvis pensionsydelsen er udbetalt på grundlag af oplysninger om resultater, som kan dokumenteres at være fejlagtige, og hvis modtageren er i ond tro herom.

Det foreslås i *§ 43 h, stk. 6, 3. pkt.*, at hvis modtageren er medlem af bestyrelsen eller ansat i firmapensionskassen ved pensionsalderen, skal firmapensionskassen udbetale den variable del af pensionsydelsen til modtageren i form af de i stk. 1, nr. 4, nævnte instrumenter uden mulighed for afhændelse eller udnyttelse i en periode på fem år.

Bestemmelsen varetager samme hensyn som den foreslåede bestemmelses stk. 3, og der henvises derfor hertil.

Det foreslås i *§ 43 h, stk. 6, 4. pkt.*, at stk. 5 finder tilsvarende anvendelse på de i 3. pkt. nævnte tilfælde.

Efter det foreslåede vil kravet om clawback i det foreslåede stk. 5 finde anvendelse på en variabel pensionsydelse som tilbageholdes i form af instrumenter i fem år, hvor modtageren fortsat er medlem af bestyrelsen eller ansat i firmapensionskassen ved pensionsalderen. Det medfører, at firmapensionskassen skal sikre, at modtageren af en variabel pensionsydelse skal tilbagebetale denne helt eller delvist, hvis pensionsydelsen er udbetalt på grundlag af oplysninger om resultater, som kan dokumenteres af være fejlagtige, og hvis modtageren er i ond tro herom.

Det følger af det foreslåede § 117, stk. 2, jf. lovforslagets § 6, nr. 3, at overtrædelse af § 43 h, stk. 6, kan straffes med bøde. Ansvarssubjektet i forhold til overtrædelse af det foreslåede § 43 h, stk. 6, er firmapensionskassen. Den strafbare handling består i, at en firmapensionskasse eksempelvis ikke sikrer sig, at en skønsmæssig pensionsydelse tilbageholdes i form af finansielle instrumenter i fem år, i de tilfælde, hvor en direktør forlader firmapensionskassen inden pensionstidspunktet. Firmapensionskassen vil endvidere kunne straffes med bøde, hvis ikke firmapensionskassen sikrer, at udbetalingen af en skønsmæssig pensionsydelse reduceres, hvis de kriterier, der dannede grundlag for beregningen af den skønsmæssige pensionsydelse ikke længere er opfyldt på udbetalingstidspunktet. Dette kan bl.a. skyldes, at modtageren ikke har efterlevet kravene om egnethed og hæderlighed i den gældende § 42, stk. 1, i lov om firmapensionskasser.

Det foreslås i *§ 43 h, stk. 7,* at for personer i ansættelsesforhold, der er omfattet af en kollektiv overenskomst, finder stk. 1-6 kun anvendelse på aftaler om variable løndele, hvis aftalerne om variabel løn ikke er fastsat i overenskomsten.

De foreslåede regler om aflønning har ikke til hensigt at berøre de rettigheder, som arbejdsmarkedets parter har i forbindelse med overenskomstforhandlinger. Aflønningsreglerne berører heller ikke de rettigheder, der følger af national aftale- og ansættelsesret, ligesom det ikke berører arbejdsmarkedets ret til at indgå og håndhæve kollektive overenskomster i overensstemmelse med nationale love og sædvaner.

Til nr. 3 (§ 97, stk. 1, 2. pkt., i lov om firmapensionskasser)

Det fremgår af § 97, stk. 1, 1. pkt., i lov om firmapensionskasser, at Finanstilsynet påser overholdelsen af denne lov og regler fastsat i medfør af loven. Det fremgår videre af § 97, stk. 1, 2. pkt., at Finanstilsynet påser overholdelsen af de i bestemmelsen nævnte forordninger og regler udstedt i medfør heraf.

Det foreslås i *§ 97, stk. 1, 2. pkt.*, at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring vil medføre, at Finanstilsynet bliver udpeget som kompetent myndighed efter DORA-forordningen til at føre tilsyn med overholdelsen af forordningen.

Forordningen finder bl.a. anvendelse på arbejdsmarkedsrelaterede pensionskasser, jf. artikel 2, stk. 1, litra p.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningen, jf. § 102 i lov om firmapensionskasser.

Finanstilsynet får med bestemmelsen bl.a. også mulighed for at give påbud og påtaler for overtrædelser af forordningen, jf. § 97.

Efter artikel 46, litra m, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'ers) sikre overholdelsen af DORA-forordningen for arbejdsmarkedsrelaterede pensionskasser.

Bestemmelsen supplerer artikel 46, litra m, i DORA-forordningen.

Til nr. 4 (§ 103, stk. 6, nr. 30, i lov om firmapensionskasser)

I medfør af § 103, stk. 1, i lov om firmapensionskasser er Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger som de bl.a. får kendskab til gennem tilsynsvirksomheden.

§ 103, stk. 6, i lov om firmapensionskasser er en undtagelse til tavshedspligten i stk. 1. Bestemmelsen fastsætter til hvem og i hvilke tilfælde Finanstilsynet kan videregive fortrolige oplysninger, uanset § 103, stk. 1.

I medfør af § 103, stk. 6, har Finanstilsynet ikke mulighed for at videregive oplysninger til Center for Cybersikkerhed, Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 103, stk. 6, nr. 30,* at Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til Center for Cybersikkerhed, SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større it-relateret hændelse fra en firmapensionskasse, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. de centrale kontaktpunkter eller CSIRT'er, der er udpeget eller oprettet i overensstemmelse med NIS 2-direktivet, dvs. Center for Cybersikkerhed. Bestemmelsen nævner også SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle

tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 5 (§ 104, stk. 1, og § 112, stk. 1, i lov om firmapensionskasser)

§ 104, stk. 1, i lov om firmapensionskasser nævner de virksomheder, der kan anses som part i forhold til Finanstilsynet i sager, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af bl.a. lov om firmapensionskasser.

§ 112, stk. 1, indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet retter sig til. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet i medfør af lov om firmapensionskasser og de i bestemmelsen nævnte forordninger.

Det foreslås i *§ 104, stk. 1,* og *§ 112, stk. 1,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at virksomheder, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af DORA-forordningen eller regler udstedt i medfør heraf, også vil være at anse som parter i afgørelsessagen, og at afgørelser truffet af Finanstilsynet i medfør af DORA-forordningen og regler udstedt i medfør heraf kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, som afgørelsen retter sig til.

Til nr. 6-8 (§ 105, stk. 1, 4.-6. pkt., i lov om firmapensionskasser)

Det fremgår af § 105, stk. 1, 1. pkt., i lov om firmapensionskasser, at der skal ske offentliggørelse af reaktioner, som Finanstilsynets bestyrelse har truffet beslutning om, eller som Finanstilsynets har givet efter delegation fra Finanstilsynets bestyrelse. Offentliggørelsen skal ske med angivelse af firmapensionskassens navn. I medfør af stk. 1, 2. pkt., skal offentliggørelsen ske på Finanstilsynets hjemmeside. § 105, stk. 1, regulerer ikke det tilfælde, hvor det alene er Finanstilsynet uden delegation fra bestyrelsen, der har truffet afgørelse om at give en reaktion til en firmapensionskasse.

Det foreslås i *§ 105, stk. 1,* efter 3. pkt., at indsætte et nyt punktum, der bliver 4. pkt., hvoraf fremgår, at reaktioner givet i henhold til DORA-

forordningen skal offentliggøres på Finanstilsynets hjemmeside med angivelse af firmapensionskassens navn, jf. dog stk. 4.

Med den foreslåede ændring vil Finanstilsynet skulle offentliggøre reaktioner, der er givet af Finanstilsynet til en virksomhed for en overtrædelse af DORA-forordningen. Ved reaktioner forstås f.eks. påbud eller påtaler. Reaktionen skal offentliggøres på Finanstilsynets hjemmeside.

I bestemmelsen er der indsat en henvisning til § 105, stk. 4, der vedrører de tilfælde, hvor offentliggørelse ikke kan ske, og at offentliggørelsen ikke må indeholde fortrolige oplysninger, jf. nærmere herom i de specielle bemærkninger til § 105, tidligere § 104, jf. Folketingstidende 2018-2019, tillæg A, L 79 som fremsat, side 196-200.

I medfør af § 105, stk. 1, 4. pkt., der bliver 5. pkt., at indbringes en reaktion, der offentliggøres i henhold til 1. pkt., dvs. en reaktion, som Finanstilsynets bestyrelse har truffet beslutning om, eller som Finanstilsynet har givet en virksomhed efter delegation fra bestyrelsen, for domstolene, skal dette fremgå af Finanstilsynets offentliggørelse, og det efterfølgende resultat af domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Desuden foreslås det i *§ 105, stk. 1, 4. pkt.*, der bliver 5. pkt., at ændre 1. pkt., til 1. eller 4. pkt.

Med den foreslåede bestemmelse vil det også skulle fremgå af Finanstilsynets offentliggørelse af en reaktion givet i henhold til DORA-forordningen, hvis denne indbringes for domstolene, og det efterfølgende resultat af domstolenes afgørelse vil også skulle fremgå af Finanstilsynets hjemmeside. Offentliggørelsen heraf vil skulle ske hurtigst muligt.

Det foreslås videre i *§ 105, stk. 1*, at indsætte et *6. pkt.*, hvoraf det fremgår, at indbringes reaktionen, der er offentliggjort i henhold til 4. pkt., for Erhvervsankenævnet, skal dette fremgå af Finanstilsynets offentliggørelse, og det efterfølgende resultat af Erhvervsankenævnets afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Med den foreslåede bestemmelse vil det skulle fremgå af offentliggørelsen af en reaktion givet i henhold til DORA-forordningen, hvis denne indbringes for Erhvervsankenævnet, ligesom det efterfølgende resultat heraf skal fremgå af offentliggørelsen.

Offentliggørelsen skal ske i naturlig sammenhæng med den offentliggørelse, som Finanstilsynet tidligere har foretaget.

Det foreslås i lovforslagets § 6, nr. 5, at afgørelser truffet af Finanstilsynet i henhold til DORA-forordningen vil kunne indbringes for Erhvervsankenævnet. Indbringes en afgørelse for Erhvervsankenævnet, vil Finanstilsynet blive orienteret herom af Erhvervsankenævnet. Finanstilsynet vil herefter – i de tilfælde hvor den indbragte afgørelse er offentliggjort – offentliggøre oplysninger om afgørelsens indbringelse. Finanstilsynets offentliggørelse heraf skal som udgangspunkt ske inden for 1 til 2 hverdage.

Finanstilsynets offentliggørelse skal ske på Finanstilsynets hjemmeside dér, hvor Finanstilsynet tidligere har offentliggjort reaktionen. Oplysningen om, at sagen er indbragt for Erhvervsankenævnet, skal fremgå tydeligt.

Finanstilsynet skal desuden offentliggøre det endelige udfald af sagen. Det indebærer ikke, at Finanstilsynet skal offentliggøre Erhvervsankenævnets kendelser i deres helhed. Disse offentliggøres af Erhvervsankenævnet.

De foreslåede ændringer i § 105, stk. 1, 4.-6. pkt., gennemfører artikel 54, stk. 1, i DORA-forordningen, hvormed de kompetente myndigheder uden unødigt ophold på deres officielle websteder skal offentliggøre enhver afgørelse om pålæggelse af en administrativ sanktion, som ikke kan påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen. En administrativ sanktion kan bl.a. kan være et påbud eller en påtale.

Det fremgår dog videre af artikel 54, stk. 5, i DORA-forordningen, at hvis den kompetente myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

For nærmere om § 105 og offentliggørelse henvises der i det hele til de specielle bemærkningerne til § 105, tidligere § 104, jf. Folketingstidende 2018-2019, tillæg A, L 79 som fremsat, side 196-200.

Til nr. 9 (§ 117, stk. 2, i lov om firmapensionskasser)

Den gældende bestemmelse i § 117 er en straffebestemmelse. Bestemmelsen indeholder i stk. 2 en opremsning af de bestemmelser, hvis overtrædelse kan straffes med bøde.

I *§ 117, stk. 2,* indsættes efter »§ 42, stk. 2, jf. stk. 1, nr. 3 og 4,«: »§§ 43 e, 43 f, § 43 g, stk. 1, § 43 h, stk. 1-6,«, og efter »§ 111, stk. 3, 5 og 6,« indsættes: »og artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-3, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1-7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26, stk. 1-6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor,«.

Det foreslåede medfører, at overtrædelse af §§ 43 e, 43 f, § 43 g, stk. 1, § 43 h, stk. 1-6, bestemmelser kan straffes med bøde. Bestemmelserne angår forpligtelser for aflønningsområdet.

Det foreslåede er en videreførelse af gældende ret, da pligterne indeholdt i de tilføjede bestemmelser hidtil har været strafbelagt i henhold til § 29, stk. 1, i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser. For en nærmere gennemgang henvises til bemærkningerne til de foreslåede bestemmelser, jf. de foreslåede § 43 e, § 43 f, § 43 g, stk. 1, og § 43 h, stk. 1-6.

Det foreslåede medfører ligeledes, at overtrædelse af en række artikler i DORA-forordningen vil kunne medføre straf. Dette foreslås i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske

forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der firmapensionskasser.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i

artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer,

som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test

af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller

dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-

aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem

regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle

ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder

automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold,

der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a.

skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til

resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente

myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed

om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-

relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-

relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres,

dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse

indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier,

fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de

skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter

kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges,

såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig

ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt

den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise

kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 7

Til nr. 1 (§ 1, stk. 1, nr. 22-26, i hvidvaskloven)

Den gældende § 1, stk. 1, nr. 22-26, i hvidvaskloven fastlægger, at udbydere af veksling mellem virtuel valuta og fiatvaluta, udbydere af virtuelle tegnebøger, udbydere af veksling mellem en eller flere typer af virtuel valuta, udbydere af overførsel af virtuel valuta og udbydere af finansielle tjenester relateret til en udsteders udbud eller salg af virtuel valuta omfattet af hvidvasklovens anvendelsesområde.

De gældende § 1, stk. 1, nr. 22-26, i hvidvaskloven gennemfører dele af FATF's anbefaling nr. 15 om udbydere af tjenester med virtuel valuta.

Hvidvasklovens § 2, nr. 15-17, definerer virtuelle tegnebøger, virtuel valuta og fiatvaluta.

Det foreslås, at *§ 1, stk. 1, nr. 22-26,* ophæves, og at indsætte udbydere af kryptoaktivtjenester som defineret i lov om finansiel virksomhed i stedet.

Udbydere af kryptoaktivtjenester er defineret i det foreslåede § 332 c, nr. 5, i lov om finansiel virksomhed, jf. jf. lovforslagets § 1, nr. 24.

Kryptoaktiv er defineret i det foreslåede § 332 c, nr. 1, jf. lovforslagets § 1, nr. 24.

Den foreslåede bestemmelse vil medføre en formel ændring af hvidvasklovens anvendelsesområde, da loven fremadrettet ikke vil omfatte udbydere af veksling mellem virtuel valuta og fiatvaluta, udbydere af virtuelle tegnebøger, udbydere af veksling mellem en eller flere typer af

virtuel valuta, udbydere af overførsel af virtuel valuta og udbydere af finansielle tjenester relateret til en udsteders udbud eller salg af virtuelle valutaer. Hvidvaskloven vil i stedet omfatte udbydere af kryptoaktivtjenester som defineret i lov om finansiel virksomhed.

Ændringen vil ikke medføre materielle ændringer, da fysiske og juridiske personer omfattet af de hidtil gældende § 1, stk. 1, nr. 22-26, også vil være omfattet af den nye § 1, stk. 1, nr. 22.

Den foreslåede bestemmelse gennemfører artikel 38, nr. 1 og 2, i Europa-Parlamentets og Rådets forordning (EU) 2023/1113 af 31. maj 2023 om oplysninger, der skal medsendes ved pengeoverførsler og ved overførsler af visse kryptoaktiver (den omarbejdede pengeoverførselsforordning), der er en ændring til artikel 2, stk. 1, nr. 3, og artikel 3, nr. 2, i Europa-Parlamentets og Rådets direktiv 2015/849/EU af 20. maj 2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (herefter 4. hvidvaskdirektiv).

Der henvises i øvrigt til pkt. 2.4 lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 2424, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 2 (§ 2, nr. 4, a og b, i hvidvaskloven)

Den gældende § 2 i hvidvaskloven indeholder en række definitioner.

En korrespondentforbindelse er defineret som værende levering af pengeinstitutydelser fra et pengeinstitut (korrespondenten) til et andet pengeinstitut (respondenten), herunder oprettelse af løbende konto eller passivkonto, og øvrige ydelser som likviditetsstyring, international overførsel af midler m.v., samt en forbindelse mellem en virksomhed omfattet af § 1, stk. 1, nr. 1-12 eller 18, (korrespondenten) til en anden virksomhed omfattet af § 1, stk. 1, nr. 1-12 eller 18, (respondenten), hvor der leveres lignende ydelser, herunder forbindelser indgået med henblik på værdipapirtransaktioner eller overførsler af midler. Det følger af den gældende § 2, nr. 4, litra a og b, i hvidvaskloven.
Definitionen af en korrespondentforbindelse, som beskrevet ovenfor, gennemfører artikel 3, stk. 8, litra a, i 4. hvidvaskdirektiv.

Når der etableres korrespondentforbindelse med en respondent, anses der samtidig i hvidvasklovens forstand at være etableret en forretningsforbindelse til respondenten. Korrespondenten er den virksomhed, der leverer ydelser til en anden virksomhed, mens respondenten er den virksomhed, der modtager ydelserne.

Korrespondentforbindelser omfatter videre tilfælde, hvor der indgås forbindelser mellem virksomheder med henblik på værdipapirtransaktioner eller overførsler af midler. Dette forekommer ved udveksling af såkaldte SWIFT-nøgler mellem finansielle virksomheder. Internationale elektroniske pengeoverførsler understøttes af et meddelelsessystem, der udbydes af SWIFT (Society for Worldwide Interbank Financial Telecommunication). For at kunne kommunikere meddelelser om pengeoverførsler ved brug af SWIFT-nøgler er det en forudsætning, at de finansielle virksomheder i teknisk forstand har udvekslet såkaldte SWIFT-nøgler med hinanden. Udveksling af SWIFT-nøgler er i udgangspunktet et centralt skridt i etableringen af en korrespondentbankforbindelse. Det er i SWIFT-systemet muligt at styre, hvilke typer beskeder udveksling af SWIFT-nøgler giver adgang til. Der kan derfor udveksles SWIFT-nøgler, uden at dette automatisk bevirker, at de involverede virksomheder har mulighed for at gennemføre betalingstransaktioner med hinanden. Udveksling af SWIFT-nøgler medfører dermed ikke i sig selv, at der etableres en korrespondentforbindelse. Der er således visse typer af beskeder, f.eks. i relation til trade finance, der ikke giver mulighed for overførsel af midler.

Definitionen af korrespondentforbindelse skal ses i sammenhæng med hvidlovens § 19, der fastsætter skærpede kundekendskabsprocedurer inden etablering af korrespondentforbindelser hjemmehørende i et land uden for EU/EØS.

Uanset den tekniske løsning er det op til det enkelte institut at vurdere, hvornår der skal foretages skærpede kundekendskabsprocedurer i henhold til definitionen af en korrespondentforbindelse, eller om der er risiko for misbrug til hvidvask eller finansiering af terrorisme.

Det foreslås at affatte hvidvasklovens *§ 2, nr. 4, litra a*, således, at en korrespondentforbindelse defineres som levering af pengeinstitutydelser fra et pengeinstitut (korrespondenten) til et andet pengeinstitut (respondenten), herunder, men ikke begrænset til, oprettelse af løbende konto eller en anden passivkonto, samt tilknyttede ydelser som likviditetsstyring, internationale overførsler af midler, checkclearing, gennemstrømningskonti og valutatransaktioner

Den foreslåede ændring af litra a medfører, at det præciseres i bestemmelsens ordlyd, hvilke typer af tilknyttede ydelser som bl.a. hører under pengeinstitutydelser.

Det foreslås videre, at affatte hvidvasklovens *§ 2, nr. 4, litra b*, således, at en korrespondentforbindelse defineres som en forbindelse mellem en virksomhed omfattet af § 1, stk. 1, nr. 1-12, 18 eller 22, (korrespondenten) og en virksomhed omfattet af § 1, stk. 1, nr. 1-12, 18 eller 22, (respondenten), herunder hvor der leveres lignende ydelser fra et korrespondentinstitut til et respondentinstitut, og forbindelser indgået med henblik på værdipapirtransaktioner eller overførsler af midler eller forbindelser indgået med henblik på transaktioner med kryptoaktiver eller overførsler af kryptoaktiver.

Den foreslåede ændring af litra b medfører, at udbydere af kryptoaktivtjenester omfattes af hvidvasklovens definition af korrespondentforbindelse i de tilfælde, hvor der leveres ydelser, der ligner pengeinstitutydelser.

Ligeledes vil den foreslåede litra b medføre, at forbindelser, som indgås med henblik på at gennemføre transaktioner med kryptoaktiver eller overførsler af kryptoaktiver, omfattes af definitionen af ydelser leveret mellem korrespondent og respondent.

Udbydere af kryptoaktivtjenester vil med den foreslåede litra b ved etablering af en korrespondentforbindelse blive underlagt krav om gennemførelse af kundekendskabsprocedurer i henhold til hvidvasklovens § 11 og skærpede kundekendskabsprocedurer i henhold til hvidvasklovens § 19.

Forbindelser, der etableres mellem udbydere af kryptoaktivtjenester og virksomheder og personer, der er etableret i tredjelande, med henblik på at gennemføre overførsler af kryptoaktiver eller levering af lignende kryptoaktivtjenester, er sammenlignelige med korrespondentforbindelser, der etableres af pengeinstitutter med et tredjelands respondentinstitut.

Definitionen af korrespondentforbindelse i forhold til udbydere af kryptoaktivtjenester skal ses i sammenhæng med hvidvasklovens § 19 om krav til skærpede kundekendskabsprocedurer ved etablering af en korrespondentforbindelse hjemmehørende i et land uden for EU/EØS.

Der henvises til bemærkningerne til § 2, nr. 4, og § 19, jf. Folketingstidende 2016-17, tillæg A, L 41 som fremsat, side 101.

I den omarbejdede pengeoverførselsforordning artikel 38 er der tilføjet en ny artikel 19 b til 4. hvidvaskdirektiv, som fastlægger en række krav om gennemførelse af kundekendskabsprocedurer, herunder skærpede kundekendskabsprocedurer, når udbydere af kryptoaktivtjenester etablerer korrespondentforbindelser.

Flere af disse krav følger af hvidvasklovens § 11, om gennemførelse af kundekendskabsprocedurer, og hvidvasklovens § 19, om gennemførelse af skærpede kundekendskabsprocedurer ved etablering af korrespondentforbindelser udenfor EU/EØS.

Artikel 19 b, stk. 1, litra b, fastsætter, at udbydere af kryptoaktivtjenester ved etablering af korrespondentforbindelser udenfor Unionen skal indhente tilstrækkelige oplysninger om respondenten til fuldt ud at forstå, hvori dens virksomhed består, og på grundlag af offentligt tilgængelige oplysninger at bedømme respondentens omdømme og kvaliteten af overvågningen. Kravet til udbydere af kryptoaktivtjenester i artikel 19 b, litra b, er enslydende med ordlyden i artikel 19, stk. 1, litra a.

Artikel 19, stk. 1, litra a, er implementeret i hvidvasklovens § 19, stk. 1, nr. 1, hvorefter korrespondenten inden etablering af en grænseoverskridende korrespondentforbindelse, der involverer gennemførelse af betalinger med et respondentinstitut uden for Den Europæiske Union, som Unionen ikke har indgået aftale med på det finansielle område, skal indhente tilstrækkelige oplysninger om respondenten til at forstå, hvori respondentens virksomhed består, og ud fra offentligt tilgængelige oplysninger bedømme respondentens omdømme og kvaliteten af det tilsyn, der føres med respondenten i det pågældende land.

Artikel 19 b, stk. 1, litra c, fastsætter, at udbydere af kryptoaktivtjenester ved etablering af korrespondentforbindelser udenfor Unionen skal vurdere respondentens kontrol med, at der ikke foregår hvidvask af penge eller finansiering af terrorisme. Kravet til udbydere af kryptoaktivtjenester i artikel 19 b, litra c, er enslydende med ordlyden i artikel 19, stk. 1, litra b. Artikel 19, stk. 1, litra b, er implementeret i hvidvasklovens § 19, stk. 1, nr. 2, hvorefter korrespondenten inden etablering af en grænseoverskridende korrespondentforbindelse, der involverer gennemførelse af betalinger med et respondentinstitut uden for Den Europæiske Union, som Unionen ikke har indgået aftale med på det finansielle område, skal indhente tilstrækkelige oplysninger til at sikre, at respondenten har effektive kontrolprocedurer med henblik på overholdelse af det pågældende lands regler om bekæmpelse af hvidvask og finansiering af terrorisme.

Artikel 19 b, stk. 1, litra d, fastsætter, at udbydere af kryptoaktivtjenester ved etablering af korrespondentforbindelser udenfor Union skal indhente den øverste ledelses godkendelse, inden der etableres nye korrespondent-forbindelser. Kravet til udbydere af kryptoaktivtjenester i artikel 19 b, litra d, er enslydende med ordlyden i artikel 19, stk. 1, litra c. Artikel 19, stk. 1, litra c, er implementeret i hvidvasklovens § 19, stk. 1, nr. 3, hvorefter korrespondenten inden etablering af en grænseoverskridende korrespondentforbindelse, der involverer gennemførelse af betalinger med et respondentinstitut uden for Den Europæiske Union, som Unionen ikke har indgået aftale med på det finansielle område, skal indhente godkendelse til etablering af korrespondentforbindelsen hos den person, der er udpeget i henhold til § 7, stk. 2.

Artikel 19 b, stk. 1, litra e, fastsætter, at udbydere af kryptoaktivtjenester ved etablering af korrespondentforbindelser udenfor Unionen skal dokumentere de respektive ansvarsområder, der påhviler hver part i korrespondentforbindelsen. Kravet til udbydere af kryptoaktivtjenester i artikel 19 b, litra e, er enslydende med ordlyden i artikel 19, stk. 1, litra d. Artikel 19, stk. 1, litra d, er implementeret i hvidvasklovens § 19, stk. 1, nr. 4, hvorefter korrespondenten skal dokumentere korrespondentens henholdsvis respondentens ansvar for opfyldelse af reglerne i denne lov.

Artikel 19 b, stk. 1, litra f, fastsætter, at udbydere af kryptoaktivtjenester ved etablering af korrespondentforbindelser udenfor Unionen i forbindelse med de såkaldte gennemstrømningskryptoaktivkonti skal sikre, at respondenten har identitetskontrolleret de kunder, der har direkte adgang til korrespondentenhedens konti, og løbende har gennemført kundekendskabsprocedurer, samt at den er i stand til at forelægge relevante kundekendskabsoplysninger for korrespondentenheden efter anmodning. Kravet til udbydere af kryptoaktivtjenester i artikel 19 b, litra f, er enslydende med ordlyden i artikel 19, stk. 1, litra e. Artikel 19, stk. 1, litra e, er implementeret i hvidvasklovens § 19, stk. 2, hvorefter korrespondenten skal sikre sig, at respondenten gennemfører kundekendskabsprocedurer, og at respondenten kan udlevere kundekendskabsoplysninger efter anmodning fra korrespondenten, hvis en respondentforbindelses kunde har direkte adgang til at disponere over midler, som indestår på en konto hos korrespondentforbindelsen.

Artikel 19, stk. 1, 2. led, fastsætter, at udbydere af kryptoaktivtjenester skal dokumentere og registrere beslutninger om at afslutte korrespondentforbindelser af årsager, som har tilknytning til politikker vedrørende bekæmpelse af hvidvask af penge og finansiering af terrorisme. Det følger af hvidvasklovens § 14, stk. 5, at såfremt kundekendskabskravene i hvidvasklovens § 11 ikke kan opfyldes, skal en

etableret forretningsforbindelse afbrydes eller afvikles, og der må ikke gennemføres yderligere transaktioner. Det skal samtidig undersøges, om der skal foretages underretning efter hvidvasklovens § 26. Ydermere følger det af hvidvasklovens § 30, stk. 1, nr. 1, at virksomheder og personer omfattet af denne lov skal opbevare oplysninger indhentet i forbindelse med opfyldelse af kravene i hvidvasklovens kapitel 3 om kundekendskabsprocedurer. Da en korrespondentforbindelse i hvidvasklovens forstand anses som en forretningsforbindelse, gælder kravet om notering også ved korrespondentforbindelser.

Artikel 19, stk. 1, 3. led, fastsætter, at udbydere af kryptoaktivtjenester regelmæssigt skal ajourføre kundekendskabsoplysningerne for korrespondentforbindelsen, eller når der opstår nye risici i forbindelse med respondenten. Det følger af hvidvasklovens § 11, stk. 1, nr. 5, 2. pkt., at oplysninger om kunder løbende skal ajourføres. Da en korrespondentforbindelse i hvidvasklovens forstand anses som en forretningsforbindelse, gælder kravet om ajourføring også ved korrespondentforbindelser.

Artikel 19, stk. 2, fastsætter, at udbydere af kryptoaktivtjenester skal tage hensyn til de oplysninger, der er omhandlet i stk. 1, for på et risikofølsomt grundlag at fastlægge de passende foranstaltninger, der skal træffes for at begrænse de risici, der er forbundet med respondentenheden. Det følger af hvidvasklovens § 11, stk. 3, at virksomheder og personer skal gennemføre alle kundekendskabskrav, jf. § 11, stk. 1 og 2. Omfanget af kundekend-skabsproceduren kan gennemføres ud fra en risikovurdering. I vurderingen skal inddrages oplysninger om forretningsforbindelsens formål, omfang, regelmæssighed og varighed. I vurderingen skal som minimum inddrages de faktorer, som fremgår af hvidvasklovens bilag 2 om begrænsede risikofaktorer og bilag 3 om øgede risikofaktorer. Da en korrespondentforbindelse i hvidvasklovens forstand anses som en forretningsforbindelse, gælder kravet om gennemførelse af kundekendskabsprocedurer også ved korrespondentforbindelser.

Den foreslåede bestemmelse gennemfører artikel 38, nr. 2, litra b i den omarbejdede pengeoverførselsforordning, der er en ændring til artikel 3, nr. 8, i 4. hvidvask-direktiv. Ligeledes gennemfører den foreslåede bestemmelse dele af artikel 38, nr. 5, i den omarbejdede pengeoverførselsforordning, som tilføjer en ny artikel 19 b, til 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og

Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 3 (§ 2, nr. 15 og 16, i hvidvaskloven)

Den gældende § 2 i hvidvaskloven indeholder en række definitioner.

Det følger af hvidvasklovens § 2, nr. 15, at en udbyder af virtuelle tegnebøger defineres som en enhed, som leverer tjenester til at beskytte private kryptografiske nøgler på vegne af sine kunder med henblik på at opbevare, lagre og overføre virtuelle valutaer.

Det følger videre af hvidvasklovens § 2, nr. 16, at virtuel valuta defineres som et digitalt udtryk for værdi, som ikke er udstedt eller garanteret af en centralbank eller en offentlig myndighed, ikke nødvendigvis er bundet til en lovligt oprettet valuta og ikke har samme retsstatus som valuta eller penge, men som accepteres af fysiske og juridiske personer som vekslings-middel, som kan overføres, lagres og handles elektronisk.

Det foreslås, at *§ 2, nr. 15* og *16,* ophæves.

Forslaget er en konsekvens af, at hvidvasklovens § 1, stk. 1, nr. 22-26, foreslås ophævet, og at udbydere af kryptoaktivtjenester foreslås indsat som en ny § 1, stk. 1, nr. 22, i medfør af dette lovforslags § 1, nr. 1. Som en konsekvens heraf vil alle typer af udbydere af tjenester med virtuel valuta samles under den foreslåede § 1, stk. 1, nr. 22, i hvidvaskloven.

Der henvises til bemærkningerne til definitionerne af kryptoaktiver og udbydere af kryptoaktivtjenester i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 24.

Den foreslåede bestemmelse gennemfører artikel 38, nr. 2, litra c og d, i den omarbejdede pengeoverførselsforordning, der er en ændring til artikel 3, nr. 18 og 19, i 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 4 (§ 2, nr. 19, i hvidvaskloven)

Den gældende § 2 i hvidvaskloven indeholder en række definitioner.

Det foreslås i *§ 2, nr. 19,* at selvhostet adresse er en distributed ledger-adresse som defineret i Europa-Parlamentets og Rådets forordning 2023/1113/EU af 31. maj 2023 om oplysninger, der skal medsendes ved pengeoverførsler og ved overførsler af visse kryptoaktiver og om ændring af direktiv 2015/849/EU

Selvhostet adresse er defineret i den omarbejdede pengeoverførselsforordning artikel 3, nr. 18, litra a. Ved selvhostet adresse forstås en distributed ledger-adresse, der ikke er knyttet til en udbyder af kryptoaktivtjenester eller en enhed, der ikke er etableret i Unionen, og som leverer tjenester svarende til dem, en udbyder af kryptoaktivtjenester leverer.

Distributed ledger-adresse er defineret i den omarbejdede pengeoverførselsforordning artikel 3, nr. 17. Ved distributed ledger-adresse forstås en alfanumerisk kode, der identificerer en adresse på et netværk, som anvender distributed ledger-teknologi (DLT) eller lignende teknologi, og hvortil der kan sendes eller modtages kryptoaktiver.

Distributed ledger-teknologi (DLT) er defineret i MiCA artikel 3, nr. 1, som en teknologi, der muliggør drift og brug af distributed ledgers.

Distributed ledger er defineret i MiCA artikel 3, nr. 2, som et informationsregister, der registrerer transaktioner, og som deles og synkroniseres mellem et sæt af DLT-netknudepunkter ved hjælp af en konsensusmekanisme.

Konsensusmekanisme er defineret i MiCA artikel 3, nr. 3, som regler og procedurer, hvorved der mellem DLT-knudepunkter opnås enighed om, at en transaktion er valideret.

DLT-knudepunkt er defineret i MiCA artikel 3, nr. 4, som en anordning eller proces, der indgår i et netværk, og som indeholder en fuldstændig eller delvis kopi af registreringer af alle transaktioner i en distributed ledger.

Det foreslåede implementerer artikel 38, nr. 2, litra d, i den omarbejdede pengeoverførselsforordning, der tilføjer et nyt nr. 19, litra a, til artikel 3, i 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 5 (§ 7, stk. 1, 1. pkt., i hvidvaskloven)

Det følger af hvidvasklovens § 7, stk. 1, 1. pkt., at virksomheder og personer omfattet af hvidvaskloven skal identificere og vurdere risikoen for, at virksomheden eller personen kan blive misbrugt til hvidvask eller finansiering af terrorisme.

Det følger af hvidvasklovens § 7, stk. 1, 2. pkt., at risikovurderingen skal foretages med udgangspunkt i virksomhedens eller personens forretningsmodel og omfatte vurderingen af risikofaktorer, der er forbundet med kunder, produkter, tjenesteydelser og transaktioner samt leveringskanaler og lande eller geografiske områder, hvor forretningsaktiviteterne udøves.

Det foreslås i *§ 7, stk. 1, 1. pkt.*, at der efter »personer« indsættes », der er«.

Der er alene tale om en sproglig ændring af lovteksten, som har til formål at give mulighed for i bemærkningerne at angive, at virksomheder og personer, som udbyder kryptoaktivtjenester, også skal identificere og vurdere risikoen for at blive misbrugt til hvidvask eller finansiering af terrorisme i forbindelse med overførsler af kryptoaktiver, der er rettet mod eller stammer fra en selvhostet adresse.

Den foreslåede bestemmelse medfører, at udbydere af kryptoaktivtjenester skal identificere og vurdere den iboende risiko for, at virksomheden eller personen kan blive misbrugt til hvidvask eller finansiering af terrorisme ved overførsler af kryptoaktiver, som er rettet mod og stammer fra selvhostede adresser. Det betyder, at udbydere af kryptoaktivtjenester skal forstå hvor og i hvilket omfang, de kan blive misbrugt til hvidvask eller finansiering af terrorisme ved overførsler til og fra selvhostede adresser.

Der henvises i til bemærkningerne til § 7, stk. 1, jf. Folketingstidende 2016-17, tillæg A, L 41 som fremsat, side 101.

Den foreslåede bestemmelse gennemfører artikel 38, nr. 4, i den omarbejdede pengeoverførselsforordning, der tilføjer artikel 19a til artikel 3, i 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 6 (§ 7, stk. 2, 1. pkt., § 38, stk. 3 og 6, § 47, stk. 1, 1. pkt., og *stk. 3, § 49, stk. 1, 1. pkt., § 51, § 51 a, stk. 1, § 51 b, stk. 1, 1. pkt., §§ 52, 53 og § 54, stk. 1, i hvidvaskloven)*

Det følger af hvidvasklovens § 7, stk. 2, 1. pkt., at den daglige ledelse i virksomheder omfattet af lovens § 1, stk. 1, nr. 1-8, 9, 10, 18 og 22-26, skal udpege en hvidvaskansvarlig, altså en ansat, der har fuldmagt til at træffe beslutninger på vegne af virksomheden i henhold til lovens § 8, stk. 2, § 17, stk. 2, nr. 5, § 18, stk. 3, og § 19, stk. 1, nr. 3.

Det følger af hvidvasklovens § 38, stk. 3, at oplysninger om, at der er givet underretning efter lovens § 26, stk. 1 og 2, eller at dette overvejes, eller at der er eller vil blive iværksat en undersøgelse efter lovens § 25, stk. 1, kan videregives mellem virksomheder i koncerner omfattet af lovens § 1, stk. 1, nr. 1-12, 18 eller 22-26, og andre virksomheder i koncernen, der har hjemsted eller er hjemmehørende i et EU- eller EØS-land.

Det følger af hvidvasklovens § 38, stk. 6, at oplysninger om, at der er givet underretning efter § 26, stk. 1 og 2, eller at dette overvejes, eller at der er eller vil blive iværksat en undersøgelse efter § 25, stk. 1, kan videregives mellem virksomheder i koncerner omfattet af lovens § 1, stk. 1, nr. 1-14, 16, 20 og 22-26.

Det følger af hvidvasklovens § 47, stk. 1, 1. pkt., at Finanstilsynet fører tilsyn med, at virksomheder og personer omfattet af lovens § 1, stk. 1, nr. 1-12, 18 og 22-26, overholder hvidvaskloven, regler udstedt i medfør heraf, Europa-Parlamentets og Rådets forordning 2015/847/EU af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler, og forordninger indeholdende regler om finansielle sanktioner mod lande, personer, grupper, juridiske enheder eller organer.

Det følger af hvidvasklovens § 47, stk. 3, at Finanstilsynet skal samarbejde med de kompetente myndigheder i EU- eller EØS-lande om at medvirke ved tilsynsaktiviteter, kontroller på stedet eller inspektioner her i landet, når det gælder virksomheder og personer omfattet af lovens § 1, stk. 1, der er under tilsyn i et andet EU- eller EØS-land, eller en dansk virksomhed eller person omfattet af § 1, stk. 1, nr. 1-12, og 22-26, der er er underlagt dansk tilsyn, men opererer i andre EU- eller EØS-lande.

Det følger af hvidvasklovens § 49, stk. 1, 1. pkt., at virksomheder og personer som nævnt i lovens § 1, stk. 1, nr. 1-12, 18 og 22-26, samt leverandører og underleverandører til disse skal give Finanstilsynet de oplysninger, der er nødvendige for tilsynets virksomhed.

Det følger af hvidvasklovens § 51, at Finanstilsynet kan påbyde virksomheder og personer, som er nævnt lovens i § 1, stk. 1, nr. 1-12, 18 og 22-26, at foretage de nødvendige foranstaltninger i tilfælde af overtrædelse af hvidvaskloven, regler udstedt i medfør heraf, Europa-Parlamentets og Rådets forordning 2015/847/EU af 20. maj 2015 om oplysninger, der skal medsendes ved pengeoverførsler, og forordninger indeholdende regler om finansielle sanktioner mod lande, personer, grupper, juridiske enheder eller organer.

Det følger af hvidvaskloven § 51 a, stk. 1, at Finanstilsynet kan påbyde en virksomhed omfattet af lovens § 1, stk. 1, nr. 1-8, 9, 10, 18 og 22-26 at afsætte den person, der er udpeget som hvidvaskansvarlig i henhold til lovens § 7, stk. 2, hvis personen ikke har tilstrækkelig godt omdømme eller personens adfærd giver grund til at antage, at personen ikke vil varetage stillingen på forsvarlig måde.

Det følger af hvidvaskloven § 51 b, stk. 1, 1. pkt., at Finanstilsynet kan påbyde en virksomhed eller person omfattet af lovens § 1, stk. 1, nr. 1-8, 9, 10, 18 og 22-26, at virksomheden eller personen midlertidigt ikke må optage nye kundeforhold, når der er konstateret en alvorlig overtrædelse af bestemmelser i denne lov eller regler udstedt i medfør heraf.

Det følger af hvidvasklovens § 52, at Finanstilsynet for virksomheder og personer som omfattet af lovens § 1, stk. 1, nr. 8, og 22-26, kan fastsætte nærmere regler om anmeldelse, registrering og offentliggørelse, herunder om, hvilke oplysninger der skal registreres, og hvilke forhold anmeldere eller andre kan indsende og registrere elektronisk i Finanstilsynets it-system ved at benytte digital eller tilsvarende elektronisk signatur, samt om brugen af dette system.

Det følger af hvidvasklovens § 53, at erhvervsministeren kan fastsætte regler om pligt for virksomheder omfattet af lovens § 1, stk. 1, nr. 1-12, 18 og 22-26, til at offentliggøre oplysninger om Finanstilsynets vurdering af virksomheden.

Det følger af hvidvasklovens § 54, stk. 1, at såfremt en virksomhed eller person omfattet af lovens § 1, stk. 1, nr. -12, 18 og 22-26, har videregivet oplysninger om virksomheden eller personen, og disse er kommet offentligheden til kendskab, kan Finanstilsynet påbyde virksomheden eller personen at offentliggøre berigtigende oplysninger inden for en af Finanstilsynet fastsat frist, hvis oplysningerne efter Finanstilsynets vurdering er misvisende, og hvis Finanstilsynet vurderer, at oplysningerne kan have skadevirkning for virksomhedens eller personens kunder, indskydere, øvrige kreditorer, de finansielle markeder, hvorpå aktierne i

virksomheden eller værdipapirer udstedt af virksomheden handles, eller den finansielle stabilitet generelt.

Det foreslås, at »-26« udgår i *§ 7, stk. 2, 1. pkt., § 38, stk. 3* og *6, § 47, stk. 1, 1. pkt.,* og *stk. 3, § 49, stk. 1, 1. pkt., § 51, § 51 a, stk. 1, § 51 b, stk. 1, 1. pkt., §§ 52, 53* og *§ 54, stk. 1*.

Det foreslåede er en konsekvens af at hvidvasklovens § 1, stk. 1, nr. 22-26, foreslås ophævet, og at udbydere af kryptoaktivtjenester foreslås indsat som en ny § 1, stk. 1, nr. 22, jf. lovforslagets § 7, nr. 1.

De foreslåede ændringer vil ikke ændre hvidvaskloven materielt.

Til nr. 7 (§ 8, stk. 1, 1. pkt., i hvidvaskloven)

Det følger af hvidvasklovens § 8, stk. 1, at virksomheder og personer omfattet af hvidvaskloven skal have tilstrækkelige skriftlige politikker, forretningsgange og kontroller, som skal omfatte risikostyring, kundekendskabs-procedurer, undersøgelses-, noterings- og underretningspligt, opbevaring af oplysninger, screening af medarbejdere og intern kontrol til effektiv forebyggelse, begrænsning og styring af risici for hvidvask og finansiering af terrorisme. Politikker, kontroller og forretningsgange skal udarbejdes med udgangspunkt i risikovurderingen foretaget efter § 7 under hensyntagen til virksomhedens størrelse.

Det foreslås, at der i *§ 8, stk. 1, 1. pkt.,* efter »personer« indsættes », der er«.

Der er alene tale om en sproglig ændring af lovteksten, som har til formål at give mulighed for i bemærkningerne at angive, at udbydere af kryptoaktivtjenester, skal have tilstrækkelige skriftlige politikker, forretningsgange og kontroller til gennemførelse af kundekendskabsprocedurer, hvor der er tale om overførsel af kryptoaktiver, som er rettet mod og stammer fra selvhostede adresser.

Der henvises til bemærkningerne til § 8, stk. 1, jf. Folketingstidende 2016-17, tillæg A, L 41 som fremsat, side 101.

Den foreslåede bestemmelse gennemfører artikel 38, nr. 4, i den omarbejdede pengeoverførselsforordning, der tilføjer artikel 19 a, til artikel 3, i 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og

Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 8 (§ 10, nr. 2, litra c og d, i hvidvaskloven)

Det følger af hvidvasklovens § 10, nr. 2, litra c, at virksomheder og personer omfattet af hvidvaskloven skal gennemføre kundekendskabsprocedurer, når de udfører en enkeltstående transaktion på 500 euro eller derover ved valutaveksling, herunder veksling mellem virtuel valuta og fiatvaluta, hvad enten transaktionen sker på én gang eller som flere transaktioner, der er eller ser ud til at være indbyrdes forbundet.

Herudover følger det af § 10, nr. 2, litra d, at virksomheder og personer omfattet af hvidvaskloven skal gennemføre kundekendskabsprocedurer, når de udfører en enkeltstående transaktion på 1.000 euro eller derover ved veksling mellem en eller flere typer af virtuel valuta, overførsel af virtuel valuta eller udstedelse af virtuel valuta, hvad enten transaktionen sker på én gang eller som flere transaktioner, der er eller ser ud til at være indbyrdes forbundet.

Det foreslås et sted i *§ 10, nr. 2, litra c,* og tre steder i *§ 10, nr. 2, litra d,* at ændre »virtuel valuta« til »kryptoaktiver«.

Ændringen er en konsekvens af, at definitionen af kryptoaktivtjenester i lov om finansiel virksomhed fremadrettet erstatter definition af virtuel valuta i hvidvaskloven.

Den foreslåede ændring medfører ikke en materiel ændring af hvidvaskloven.

Til nr. 9 (§ 17 a i hvidvaskloven)

Det følger af hvidvasklovens § 17, at virksomheder og personer omfattet af hvidvaskloven ud over kravene i §§ 11 og 12, skal gennemføre skærpede kundekendskabsprocedurer, hvor der vurderes at være øget risiko for hvidvask eller finansiering af terrorisme. Virksomheden eller personen skal i vurderingen tage de højrisikofaktorer i betragtning, som fremgår af bilag 3 til loven, og andre højrisikofaktorer, som skønnes at være relevante.

I den omarbejdede pengeoverførselsforordning artikel 38 er der tilføjet en ny artikel 19 a til 4. hvidvaskdirektiv, som fastlægger en række krav til overførsler af kryptoaktiver, der stammer fra eller er rettet mod selvhostede adresser.

Det fremgår af artikel 19 a, stk. 1., 3. pkt., at udbydere af kryptoaktivtjenester i forbindelse med overførsler af kryptoaktiver, der er rettet mod eller stammer fra en selvhostet adresse, skal træffe en eller flere risikobegrænsende foranstaltninger, der står i et rimeligt forhold til de identificerede risici ved sådanne overførsler. De begrænsende foranstaltninger skal omfatte en eller flere af de foranstaltninger, som er opregnet i artikel 19 a, stk. 1, 3. pkt., litra a-d.

Efter artikel 19 a, stk. 1, 3. pkt., litra a, kan en begrænsende foranstaltning omfatte identifikation og kontrol af identiteten af ordregiveren eller ordremodtageren af en overførsel, som stammer fra eller er rettet mod en selvhostet adresse eller en sådan ordregivers eller ordremodtagers reelle ejer, herunder gennem anvendelse af tredjeparter.

Efter artikel 19 a, stk. 1, 3. pkt., litra b, kan en begrænsende foranstaltning omfatte indhentelse af yderligere oplysninger om de overførte kryptoaktivers oprindelse og bestemmelsessted.

Efter artikel 19 a, stk. 1, 3. pkt., litra c, kan en begrænsende foranstaltning omfatte gennemførelse af skærpet overvågning af de pågældende overførsler.

Efter artikel 19 a, stk. 1, 3. pkt., litra d, kan en begrænsende foranstaltning omfatte enhver anden foranstaltning til begrænsning og styring af risikoen for hvidvask og finansiering af terrorisme, samt risikoen for manglende gennemførelse og unddragelse af målrettede finansielle sanktioner og målrettede finansielle sanktioner i forbindelse med finansiering af spredning af masseødelæggelsesvåben.

Det fremgår videre af artikel 19 a, stk. 2, at European Banking Authority (EBA) senest 18 måneder efter, at den omarbejdede pengeoverførselsforordning træder i kraft, udsteder retningslinjer med henblik på at præcisere de nævnte foranstaltninger i artikel 19 a, stk. 1, 3. pkt., under hensyntagen til den seneste teknologi.

Det foreslås i *§ 17 a,* at erhvervsministeren kan fastsætte regler om gennemførelse af risikobegrænsende foranstaltninger ved overførsel af kryptoaktiver, der er rettet mod eller stammer fra en selvhostet adresse.

Det forventes, at EBA vil fastsætte retningslinjer, som vil klarlægge, hvordan de risikobegrænsende foranstaltninger skal gennemføres, herunder, hvordan man kan identificere og kontrollere ordremodtager og –giver, og hvilken dokumentation, der er tilstrækkelig til at fastslå overførte kryptoaktivers oprindelse og bestemmelsessted. Ydermere forventes EBA's

retningslinjer at klarlægge brug af distributed ledger-teknologi, som benyttes ved overførsel af kryptoaktiver til og fra selvhostede adresser.

Den foreslåede bemyndigelse vil kunne benyttes til at fastsætte regler, der er i overensstemmelse med retningslinjer udstedt af EBA i henhold til artikel 19 a, stk. 2, i 4. hvidvaskdirektiv, med de tilpasninger, der er nødvendige henset til den løbende tekniske udvikling på området for kryptoaktiver og -tjenester.

Den foreslåede bestemmelse gennemfører dele af artikel 38, nr. 4 i den omarbejdede pengeoverførselsforordning, som tilføjer en ny artikel 19 a, til 4. hvidvaskdirektiv. Bestemmelsen gennemfører artikel 19 a, stk. 1, 3. pkt.

Det vil videre være muligt at fastsætte bødestraf for grove og gentagne overtrædelser af visse regler i bekendtgørelsen, jf. § 78, stk. 6, i hvidvaskloven.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 10 (§ 19, stk. 2, i hvidvaskloven)

Det følger af hvidvasklovens § 19, at inden etablering af en grænseoverskridende korrespondentforbindelse, der involverer gennemførelse af betalinger med et respondentinstitut, der hører hjemme i et land uden for Den Europæiske Union, som Unionen ikke har indgået aftale med på det finansielle område, skal korrespondenten, ud over kundekendskabsproceduren i medfør af § 11, for det første indhente tilstrækkelige oplysninger om respondenten til at forstå, hvori respondentens virksomhed består og ud fra offentligt tilgængelige oplysninger bedømme respondentens omdømme og kvaliteten af det tilsyn, der føres med respondenten i det pågældende land, jf. stk. 1, nr. 1. Korrespondenten skal for det andet indhente tilstrækkelige oplysninger til at sikre, at respondenten har effektive kontrolprocedurer med henblik på overholdelse af det pågældende lands regler om bekæmpelse af hvidvask og finansiering af terrorisme, jf. stk. 1, nr. 2, og indhente godkendelse til etablering af korrespondentforbindelsen hos den person, der er udpeget i henhold til § 7, stk. 2, jf. stk. 1, nr. 3. For det tredje skal korrespondenten dokumentere korrespondentens henholdsvis respondentens ansvar for opfyldelse af reglerne i hvidvaskloven, jf. stk. 1, nr. 4.

Det følger af hvidvasklovens § 19, stk. 2, at hvis en respondentforbindelses kunde har direkte adgang til at disponere over midler, som indestår på en konto hos korrespondentforbindelsen, skal korrespondenten sikre sig, at respondenten gennemfører kundekendskabsprocedurer, og at respondenten kan udlevere kundekendskabsoplysninger efter anmodning fra korrespondenten.

Det foreslås i *§ 19, stk. 2,* at inden gennemførelse af kryptoaktivtjenester, skal korrespondenten fastslå, om respondenten er godkendt eller registreret i det pågældende land.

Den foreslåede ændring medfører, at udbydere af kryptoaktivtjenester ved oprettelse af korrespondentforbindelser, hvor respondenten er etableret i et land udenfor EU/EØS, skal korrespondenten fastslå om respondenten er registreret eller godkendt i det land, hvor respondenten er etableret.

Registrering eller godkendelse kan f.eks. fastslås ved indhentelse af dokumentation for registrering eller godkendelse hos det pågældende lands tilsynsmyndighed.

Den gældende § 19 i hvidvaskloven er strafbelagt i medfør af § 78, stk. 1, 2. pkt., og stk. 2. Den foreslåede bestemmelse i § 19, stk. 2, vil således også være strafbelagt i medfør af § 78, stk. 1, 2. pkt. og stk. 2.

Ansvarssubjektet er udbydere af kryptoaktivtjenester, jf. det foreslåede § 1, stk. 1, nr. 22, i hvidvaskloven, jf. lovforslagets § 7, nr. 1. Den strafbare handling består f.eks. i, at en udbyder af kryptoaktivtjenester ved etablering af en korrespondentforbindelse, hvor respondenten er etableret i et land udenfor EU/EØS, ikke fastslår om respondenten er registreret eller godkendt i det land, hvor respondenten er etableret.

Den foreslåede bestemmelse gennemfører dele af artikel 38, nr. 5, i den omarbejdede pengeoverførselsforordning, som tilføjer en ny artikel 19 b til 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 11 (§ 33, 1. pkt., i hvidvaskloven)

Det følger af hvidvasklovens § 33, at Finanstilsynet kan fastsætte regler om, at betalingsinstitutter og e-pengeinstitutter, der er registreret i et EU- eller

EØS-land, og som er etableret her i landet på anden måde end ved en filial, har pligt til at udpege en person med ansvar for at sikre, at virksomheden eller personen overholder reglerne i hvidvaskloven. Finanstilsynet kan fastsætte regler om, at personen skal have tilstedeværelse her i landet, og hvilke funktioner den pågældende person skal udføre på vegne af virksomheden.

I henhold til bemærkningerne til § 33, er kravet forholdsmæssigt, hvilket betyder, at regler om udpegning af en person ikke må gå videre end nødvendigt for at nå målene om at sikre overholdelsen af bestemmelserne om bekæmpelse af hvidvask af penge og finansiering af terrorisme samt at lette tilsynet, jf. Folketingstidende 2016-17, tillæg A, L 41 som fremsat, side 137.

Det foreslås i *§ 33, 1. pkt.*, at »udbydere af betalingstjenester og udstedere af elektroniske penge« ændres til »udbydere af betalingstjenester, udstedere af elektroniske penge og udbydere af kryptoaktivtjenester«.

Ændringen vil medføre, at Finanstilsynet kan fastsætte regler om, at udbydere af tjenester med kryptoaktiver, der er registreret i et EU- eller EØS-land, og som er etableret her i landet på anden måde end ved en filial, har pligt til at udpege en person med ansvar for at sikre, at virksomheden eller personen overholder reglerne i hvidvaskloven. Finanstilsynet kan fastsætte regler om, at personen skal have tilstedeværelse her i landet, og hvilke funktioner den pågældende person skal udføre på vegne af virksomheden.

Udpegning af en person, der handler på den udpegede virksomheds vegne, sikrer, at virksomhederne overholder bestemmelserne om bekæmpelse af hvidvask af penge og finansiering af terrorisme. Yderligere sikrer udpegningen, at tilsynet med disse virksomheder lettes ved at sikre, at myndighederne på en effektiv måde kan modtage dokumenter og oplysninger fra en virksomhed.

Den foreslåede ændring gennemfører artikel 38, nr. 7, i den omarbejdede pengeoverførselsforordning, der er en ændring til artikel 45, stk. 9, i 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger, samt lovforslagets § 1, nr. 24, om supplering af Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA) og bemærkningerne hertil.

Til nr. 12 (§ 35, stk. 1, 1. pkt., og § 36, stk. 1, 1. pkt., i hvidvaskloven)

Det følger af hvidvasklovens § 35, stk. 1, 1. pkt., at virksomheder og personer omfattet af lovens § 1, stk. 1, nr. 12-19 og 21-26, for så vidt angår alternative investeringsfonde, skal have en ordning, hvor deres ansatte via en særlig, uafhængig og selvstændig kanal kan indberette overtrædelser eller potentielle overtrædelser af denne lov og regler udstedt i medfør heraf.

Det følger af hvidvasklovens § 36, stk. 1, 1. pkt., at virksomheder og personer omfattet af lovens § 1, stk. 1, nr. 12-19 og 21-26, ikke må udsætte den ansatte eller den tidligere ansatte for ufordelagtig behandling eller ufordelagtige følger som følge af, at den ansatte eller den tidligere ansatte har indberettet virksomhedens eller personens overtrædelse eller potentielle overtrædelse af denne lov og regler udstedt i medfør heraf til en tilsynsmyndighed eller til en ordning i virksomheden.

Det foreslås i *§ 35, stk. 1, 1. pkt.*, og *§ 36, stk. 1, 1. pkt.*, at ændre »og 21-26« til: », 21 og 22«.

Det foreslåede er en konsekvens af, at hvidvasklovens § 1, stk. 1, nr. 22-26, foreslås ophævet, og at udbydere af kryptoaktivtjenester foreslås indsat som en ny § 1, stk. 1, nr. 22, jf. lovforslagets § 7, nr. 1.

Den foreslåede ændring vil ikke ændre hvidvaskloven materielt.

Til nr. 13 (§ 48, stk. 2, i hvidvaskloven)

Det følger af hvidvasklovens § 48, stk. 2, at virksomheder og personer omfattet af hvidvasklovens § 1, stk. 1, nr. 22-26, skal registreres hos Finanstilsynet for at kunne udøve deres aktiviteter.

Det foreslås, at *§ 48, stk. 2*, ophæves.

Den foreslåede ændring medfører, at udbydere af tjenester med virtuel valuta ikke længere er omfattet af registreringskrav efter hvidvaskloven.

MiCA fastsætter en omfattende lovgivningsmæssig ramme for udbydere af kryptoaktivtjenester, der harmoniserer reglerne vedrørende tilladelse til og drift af udbydere af kryptoaktivtjenester i hele EU/EØS. For at undgå overlappende registreringskrav fjernes registreringskrav i forbindelse med de kategorier af udbydere af kryptoaktivtjenester, som vil blive omfattet af en fælles godkendelsesordning i henhold til MiCA.

Den foreslåede ændring gennemfører artikel 38, nr. 8 i den omarbejdede pengeoverførselsforordning, der er en ændring til artikel 47, stk. 1, i 4. hvidvaskdirektiv.

Der henvises i øvrigt til pkt. 2.4 i lovforslagets almindelige bemærkninger.

Til nr. 14 (§ 48, stk. 3, 1. og 2. pkt., og stk. 6 og 7, i hvidvaskloven)

Det følger af hvidvasklovens § 48, stk. 3, 1. pkt., at Finanstilsynet skal undlade at foretage registrering efter stk. 1 og 2, hvis et medlem af virksomhedens øverste eller daglige ledelse eller personen er dømt for et strafbart forhold, der medfører en nærliggende fare for misbrug af stillingen eller hvervet, jf. straffelovens § 78, stk. 2.

Det følger af hvidvasklovens § 48, stk. 3, 2. pkt., at Finanstilsynet skal undlade at foretage registrering efter stk. 1 og 2, hvis et medlem af virksomhedens øverste eller daglige ledelse eller personen ikke har et tilstrækkeligt godt omdømme og ikke kan udvise hæderlighed, integritet og tilstrækkelig uafhængighed ved varetagelsen af hvervet eller stillingen.

Videre følger det af hvidvasklovens § 48, stk. 6, at Finanstilsynet kan inddrage registreringen af en virksomhed eller en anden juridisk person foretaget efter stk. 1 og 2, hvis et medlem af virksomhedens øverste eller daglige ledelse eller personen efterfølgende omfattes af stk. 3, eller hvis virksomheden eller en reel ejer efterfølgende omfattes af stk. 4.

Efter § 48, stk. 7, kan Finanstilsynet inddrage registreringen af en virksomhed eller en person efter stk. 1 og 2, hvis virksomheden eller personen gør sig skyldig i grove eller gentagne overtrædelser af denne lov.

Det foreslås, at »og 2« udgår af *§ 48, stk. 3, 1.* og *2. pkt.*, og *stk. 6* og *7.*

Forslaget er en konsekvens af at hvidvasklovens § 48, stk. 2, foreslås ophævet, jf. lovforslagets § 7, nr. 13, hvorefter også henvisningerne til registreringskravet bør udgå.

De foreslåede ændringer medfører ikke en materiel ændring af hvidvaskloven.

Til nr. 15 (§ 48, stk. 5, i hvidvaskloven)

Det følger af hvidvasklovens § 48, stk. 5, at straffelovens § 78, stk. 3, finder tilsvarende anvendelse ved Finanstilsynets vurdering i henhold til

bestemmelsens stk. 3 og 4, som omhandler Finanstilsynets pligt til at undlade registrering.

Det foreslås i *§ 48, stk. 5,* at ændre »stk. 3 og 4« til »stk. 2 og 3«.

Forslaget er en konsekvens af, at registreringskravet i hvidvasklovens § 48, stk. 2, foreslås ophævet, jf. lovforslagets § 1, nr. 13, hvorefter henvisningerne i bestemmelsen skal ændres.

Den foreslåede ændring medfører ikke en materiel ændring af hvidvaskloven.

Til nr. 16 (§ 48, stk. 6, i hvidvaskloven)

Det følger af hvidvasklovens § 48, stk. 6, at Finanstilsynet kan inddrage registreringen af en virksomhed eller en person efter stk. 1 og 2, hvis virksomheden eller personen gør sig skyldig i grove eller gentagne overtrædelser af denne lov.

Det foreslås i *§ 48, stk. 6,* at ændre »stk. 3« til »stk. 2« og »stk. 4« til »stk. 3«.

Forslaget er en konsekvens af, at registreringskravet i hvidvasklovens § 48, stk. 2, foreslås ophævet, jf. lovforslagets § 1, nr. 13, hvorefter henvisningerne i bestemmelsen skal ændres.

De foreslåede ændringer medfører ikke materielle ændringer af hvidvaskloven.

Til nr. 17 (§ 54, stk. 2, i hvidvaskloven)

Det følger af hvidvasklovens § 54, stk. 2, at såfremt virksomheden eller personen omfattet af lovens § 1, stk. 1, nr. 1-13, 19, 23-27, ikke berigtiger oplysningerne i overensstemmelse med Finanstilsynets påbud og inden for den af Finanstilsynet fastsatte frist, kan Finanstilsynet offentliggøre påbuddet.

Ved ændring af hvidvaskloven i 2022, jf. lov nr. 2382 af 14. december 2021 blev hvidvasklovens § 1, stk. 1, nr. 9, ophævet. Som følge heraf blev hvidvasklovens § 1, stk. 1, nr. 10-27, ændret til nr. 9-26.

Ved en fejl blev henvisningen til nr. 1-13, 19 og 23-27, i § 54, stk. 2, ikke rettet, som følge af ophævelsen af § 1, stk. 1, nr. 9.

Det foreslås i *§ 54, stk. 2*, at ændre »1-13, 19 og 23-27« til »1-12, 18 og 22«.

Forslaget er en konsekvens af ophævelsen af hvidvasklovens § 1, stk. 1, nr. 9, ved lov nr. 2382 af 14. december 202. Det foreslåede sikrer, at henvisninger til numrene i § 54, stk. 2, ændres, så bestemmelsen tager højde for de ryk, der er sket som følge af ophævelsen af § 1, stk. 1, nr. 9.

Derudover foretages en ændring af henvisningen til stk. 1, nr. 23-26, som følge af at hvidvasklovens § 1, stk. 1, nr. 22-26, foreslås ophævet, og at udbydere af kryptoaktivtjenester foreslås indsat som en ny § 1, stk. 1, nr. 22, i dette lovforslags § 1, nr. 1. Det foreslåede medfører, at henvisningen til de ophævede numre udgår.

Til nr. 18 (§ 78, stk. 1, 2. pkt., i hvidvaskloven)

Den gældende bestemmelse i hvidvasklovens § 78 er en strafbestemmelse. Bestemmelsen fastsætter, hvilke overtrædelser af hvidvaskloven og EU-forordninger, der kan straffes.

Det følger af § 78, stk. 1, 2. pkt., at forsætlig eller groft uagtsom overtrædelse af § 48, stk. 1 og 2, straffes med bøde, medmindre højere straf er forskyldt efter straffelovens regler.

Det foreslås i *§ 78, stk. 1, 2. pkt.*, at ændre »§ 48, stk. 1 og 2,« til »§ 48, stk. 1,«.
Forslaget er en konsekvens af, at registreringskravet i hvidvasklovens § 48, stk. 2, foreslås ophævet i medfør af dette lovforslags § 1, nr. 13, hvorefter henvisningen i bestemmelsen skal ændres.

Den foreslåede ændring medfører ikke en materiel ændring af hvidvaskloven.

Til nr. 19 (§ 85, stk. 4, i hvidvaskloven)

Det fremgår af § 85 i hvidvaskloven, at loven ikke gælder for Færøerne og Grønland, men ved kongelig anordning kan sættes helt eller delvist i kraft for Færøerne og Grønland med de ændringer, de færøske og grønlandske forhold tilsiger.

Det følger af § 59, stk. 1, i hvidvaskloven som sat i kraft for Grønland, at virksomheder og personer som nævnt i § 1, stk. 1, nr. 15 og 22, skal give Erhvervsstyrelsen de oplysninger, som er nødvendige for styrelsens virksomhed. Det følger af § 59, stk. 2, i hvidvaskloven som sat i kraft for Grønland, at Erhvervsstyrelsen, hvis formålet tilsiger det, til enhver tid mod

behørig legitimation uden retskendelse, kan få adgang virksomheder og personer omfattet af § 1, stk. 1, nr. 15 og 22, med henblik på indhentelse af oplysninger, herunder ved kontrolbesøg.

Det følger af § 60 i hvidvaskloven som sat i kraft for Grønland, at Erhvervsstyrelsen inden for en af Erhvervsstyrelsen fastsat frist kan påbyde de virksomheder og personer, som er nævnt i § 1, stk. 1, nr. 15 og 22, at foretage de nødvendige foranstaltninger i tilfælde af overtrædelse af bestemmelser i denne lov eller de regler, der er fastsat i medfør heraf.

Det fremgår af § 59, stk. 1 og 2, i hvidvaskloven, jf. lov nr. 651 af 8. juni 2017, som ændret ved lov nr. 553 af 7. maj 2019, at virksomheder og personer som nævnt i § 1, stk. 1, nr. 15-18 og 22, skal give Erhvervsstyrelsen de oplysninger, der er nødvendige for styrelsens virksomhed, og at Erhvervsstyrelsen, hvis formålet tilsiger det, til enhver tid mod behørig legitimation uden retskendelse kan få adgang til virksomheder og personer omfattet af § 1, stk. 1, nr. 15-18 og 22, med henblik på indhentelse af oplysninger, herunder ved kontrolbesøg.

Det fremgår af § 60 i hvidvaskloven, jf. lov nr. 651 af 8. juni 2017, med de ændringer, der følger af lov nr. 553 af 7. maj 2019, at Erhvervsstyrelsen inden for en af Erhvervsstyrelsen fastsat frist kan påbyde de virksomheder og personer, som er nævnt i § 1, stk. 1, nr. 15-18 og 22, at foretage de nødvendige foranstaltninger i tilfælde af overtrædelse af bestemmelser i denne lov, de regler, der er fastsat i medfør heraf, eller Europa-Parlamentets og Rådets forordninger indeholdende regler om finansielle sanktioner mod lande, personer, grupper, juridiske enheder eller organer.

§ 1, stk. 1, nr. 15-18, omfatter revisorer og revisionsvirksomheder godkendt i henhold til revisorloven, jf. nr. 15, ejendomsmæglere og ejendomsmæglervirksomheder, jf. nr. 16, virksomheder og personer, der i øvrigt erhvervsmæssigt leverer samme ydelser som visse advokater, visse ejendomsmæglere og ejendomsmæglervirksomhed samt visse revisorer og revisionsvirksomheder, herunder revisorer, som ikke er godkendt i henhold til revisorloven, skatterådgivere, jf. nr. 17, samt eksterne bogholdere og udbydere af tjenesteydelser til virksomheder, jf. nr. 18. § 1, stk. 1, nr. 22, omfatter virksomheder og personer, der erhvervsmæssigt opbevarer, handler med eller formidler handel med kunstværker, herunder gallerier og auktionshuse, hvor værdien af transaktionen eller af en række indbyrdes forbundne transaktioner udgør 50.000 kr. eller derover.

§ 1, stk. 1, nr. 16 og nr. 18, er ikke sat i kraft for Grønland, men det er § 1, stk. 1, nr. 15, 17 og 22.

Ved en fejl er § 1, stk. 1, nr. 17, imidlertid ikke nævnt i tilsynsbestemmelserne for Erhvervsstyrelsen i §§ 59 og 60 i hvidvaskloven, som sat i kraft for Grønland. Derfor har Erhvervsstyrelsen ikke de tilsynsbeføjelser, der følger af §§ 59 og 60 overfor personer omfattet af § 1, stk. 1, nr. 17.

Det foreslås i § 85 at indsætte et nyt *stk. 4,* hvorefter de dele af §§ 59 og 60, som i medfør af stk. 1 er sat i kraft for Grønland, ved kongelig anordning vil kunne sættes helt eller delvist i kraft på ny for Grønland med de ændringer, som de grønlandske forhold tilsiger.

Det foreslåede stk. 4 vil medføre, at der indsættes en ny anordningshjemmel i § 85, som kan anvendes til på ny at sætte §§ 59 og 60 i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger.

Hvidvaskloven, som sat i kraft for Grønland, er senere ændret ved anordning nr. 2627 af 28. december 2021, som sætter lov nr. 553 af 7. maj 2019 i kraft. De seneste ændringer til den danske hvidvasklov, herunder til § 1, stk. 1, er derimod ikke sat i kraft for Grønland. Når §§ 59 og 60, sættes helt eller delvist i kraft på ny for Grønland, er der således retlige forhold i Grønland, der tilsiger, at de seneste ændringer af §§ 59 og 60, i den danske hvidvasklov ikke skal sættes i kraft for Grønland, da det vil medføre en forkert henvisning til § 1, stk. 1, i hvidvaskloven, som sat i kraft for Grønland.

Retlige forhold i Grønland tilsiger således, at §§ 59 og 60, skal sættes i kraft på ny uden de ændringer til den danske hvidvasklov, der er indført efter ændringerne ved lov nr. 553 af 7. maj 2019.

Formålet med den foreslåede § 85, stk. 4, er således, at den korrekte henvisning til § 1, stk. 1, nr. 17, i §§ 59 og 60, som sat i kraft for Grønland, kan tilføjes. Indsættelse af den korrekte henvisning vil medføre, at Erhvervsstyrelsens beføjelser og reaktionsmuligheder under tilsyn i Grønland kan udvides til også at gælde for virksomheder og personer, der i øvrigt erhvervsmæssigt leverer samme ydelser som de i nr. 14-16 nævnte persongrupper, herunder revisorer, som ikke er godkendt i henhold til revisorloven, skatterådgivere og eksterne bogholdere, jf. hvidvasklovens § 1, stk. 1, nr. 17.

Til § 8

Til nr. 1 (§ 2, stk. 1, i lov om forsikringsvirksomhed)

Det fremgår af § 2, stk. 1, i lov om forsikringsvirksomhed, at § 139 i lov om forsikringsvirksomhed også finder anvendelse for finansielle holdingvirksomheder og forsikringsholdingvirksomheder.

Det følger af bemærkningerne til § 2, stk. 1, i lov om forsikringsvirksomhed, at bestemmelsen er en videreførelse af § 2 i lov om finansiel virksomhed. Det følger også af bemærkningerne til § 2 i lov om forsikringsvirksomhed, at bestemmelsen alene blev videreført med redaktionelle ændringer i forhold til, hvad der var gældende ret på tidspunktet for vedtagelse af lov om forsikringsvirksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 129.

Det følger af bemærkningerne til § 139, at bestemmelsen er en videreførelse af § 108 i lov om finansiel virksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 338.

§ 108 i lov om finansiel virksomhed var ikke omfattet af opregningen i § 2 i lov om finansiel virksomhed på tidspunktet for vedtagelse af lov om forsikringsvirksomhed.

Det følger af bemærkningerne til § 138 i lov om forsikringsvirksomhed, at bestemmelsen viderefører § 75 i lov om finansiel virksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 336.

§ 75 i lov om finansiel virksomhed var omfattet af opregningen i § 2 i lov om finansiel virksomhed på tidspunktet for vedtagelse af lov om forsikringsvirksomhed.

Det foreslås at ændre i *§ 2, stk. 1,* i lov om forsikringsvirksomhed ved at ændre henvisningen til § 139 til § 138 i bestemmelsen.

Formålet med ændringen er at rette op på en tastefejl i lov om forsikringsvirksomhed, der medførte, at § 139 i lov om forsikringsvirksomhed finder anvendelse for finansielle holdingvirksomheder og forsikringsholdingvirksomheder.

Den foreslåede bestemmelse vil medføre, at direktionen i finansielle holdingvirksomheder og forsikringsholdingvirksomheder ikke er forpligtet til at overholde § 139 i lov om forsikringsvirksomhed, men derimod § 138, hvilket var hensigten med det oprindelige lovforslag.

Til nr. 3 (overskriften før § 8 i lov om forsikringsvirksomhed)

Det foreslås at ophæve *overskriften* før § 8.

Det foreslåede skal ses i sammenhæng med den foreslåede regulering af operatører af finansielle digitale infrastrukturer i afsnit IX c i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 24, der vil erstatte reglerne for datacentraler i den finansielle regulering.

Til nr. 3 (§ 8 i lov om forsikringsvirksomhed)
§ 8 i lov om forsikringsvirksomhed fastsætter, hvilke regler i loven, der finder anvendelse på fælles datacentraler.

Det foreslås at ophæve *§ 8*.

Det foreslåede skal ses i sammenhæng med den foreslåede regulering af operatører af finansielle digitale infrastrukturer i afsnit IX c i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 24, der vil erstatte reglerne for datacentraler i den finansielle regulering.

Til nr. 4 (§ 9, stk. 1, nr. 13, i lov om forsikringsvirksomhed)

Det fremgår af § 9, stk. 1, nr. 13, i lov om forsikringsvirksomhed, at Finanstilsynet fastsætter bestemmelser om revisionens gennemførelse i forsikringsselskaber og i forsikringsselskabers dattervirksomheder, herunder om intern revision og om systemrevisionens gennemførelse i fælles datacentraler.

Det foreslås at ophæve *§ 9, stk. 1, nr. 13.*

Det foreslåede skal ses i sammenhæng med den foreslåede regulering af operatører af finansielle digitale infrastrukturer i afsnit IX c i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 24, der vil erstatte reglerne for datacentraler i den finansielle regulering.

Til nr. 5 (§ 107, stk. 2, i lov om forsikringsvirksomhed)

Lov om forsikringsvirksomhed § 107 indeholder regler om et forsikringsselskabs eller en forsikringsholdingvirksomheds bestyrelses kollektive egnethed.

I § 107, stk. 2, i lov om forsikringsvirksomhed fastsættes, at i forsikringsselskaber, der har tilladelse til at udøve livsforsikringsvirksomhed, med en balancesum på over 30 mia. kr. og i forsikringsselskaber, der har tilladelse til at udøve skadesforsikringsvirksomhed, med en balancesum på over 4 mia. kr., skal

mindst et medlem af bestyrelsen have ledelseserfaring fra et forsikringsselskab eller et relevant pengeinstitut eller realkreditinstitut.

Det fremgår af bemærkningerne til § 107, stk. 2, at bestemmelsen blev indsat som et nyt krav med vedtagelse af lov nr. 718 om forsikringsvirksomhed af 13. juni 2023, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 283. Det fremgår også af bemærkningerne, at indholdet i bestemmelsen allerede fremgik af Finanstilsynets vejledning af 4. juli 2012 til evaluering af bestyrelsens viden og erfaring i forsikringsselskaber, der har tilladelse til at udøve livsforsikringsvirksomhed, og til evaluering af bestyrelsens viden og erfaring i skadesforsikringsselskaber, og at bestemmelsen derfor havde til formål at kodificere Finanstilsynets praksis, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 283.

I vejledning af 4. juli 2012 til evaluering af bestyrelsens viden og erfaring i skadesforsikringsselskaber fremgår det, at kravet bør opfyldes i skadesforsikringsselskaber med en bruttopræmieindtægt på over 4 mia. kr.

Det er således en fejl, at der i § 107, stk. 2, angives krav for skadesforsikringsselskaber med en balancesum på over 4 mia. kr. Der burde i stedet angives krav for skadesforsikringsselskaber med en bruttopræmieindtægt på over 4 mia. kr.

Det foreslås, at ændre *§ 107, stk. 2,* således at »balancesum på over 4 mia. kr.« ændres til »bruttopræmieindtægt på over 4 mia. kr.,«.

Til nr. 6 (§ 123, stk. 2, i lov om forsikringsvirksomhed)

§ 123, stk. 1, i lov om forsikringsvirksomhed indeholder et eksponeringsforbud.

§ 123, stk. 2, i lov om forsikringsvirksomhed fastsætter, at eksponeringsforbuddet i stk. 1 ikke finder anvendelse i forbindelse med deltagelse i bestyrelserne i en række angivne virksomheder, herunder i Landbrugets FinansieringsBank A/S.

Landbrugets FinansieringsBank A/S er ophørt i 2017.

Det foreslås at ændre *§ 123, stk. 2,* så henvisningen til »Landbrugets FinansieringsBank A/S« udgår.

Den foreslåede ændring vil medføre, at Landbrugets FinansieringsBank A/S ikke længere vil fremgå af undtagelsesbestemmelsen i § 123, stk. 2, i lov

om forsikringsvirksomhed. Forslaget vil derfor rette op på en fejl i lov om forsikringsvirksomhed.

Til nr. 7 (§ 193, stk. 13, i lov om forsikringsvirksomhed)

Det følger af § 193, stk. 13, i lov om forsikringsvirksomhed, at Finanstilsynet fastsætter bestemmelser om revisionens gennemførelse i forsikringsselskaber og i forsikringsselskabers dattervirksomheder, herunder om intern revision og om systemrevisionens gennemførelse i fælles datacentraler.

Det foreslås, at »om systemrevisionens gennemførelse i fælles datacentraler« udgår fra *§ 193, stk. 13*.

Det foreslåede skal ses i sammenhæng med den foreslåede regulering af operatører af finansielle digitale infrastrukturer i afsnit IX c i lov om finansiel virksomhed, jf. lovforslagets § 1, nr. 24, der vil erstatte reglerne for datacentraler i den finansielle regulering.

Til nr. 8 (§ 196, stk. 6, i lov om forsikringsvirksomhed)

§ 195 i lov om forsikringsvirksomhed fastsætter regler om et forsikringsselskabs overdragelse af hele eller dele af sin bestand til et andet forsikringsselskab.

§ 195, stk. 6, fastsætter, at en række bestemmelser i selskabsloven ikke finder anvendelse ved bestandoverdragelser omfattet af stk. 1, bl.a. § 274, stk. 3, og § 294, stk. 3.

§§ 274 og 294 blev ophævet ved lov nr. 243 af 7. marts 2023.

Det foreslås at ændre *§ 195, stk. 6,* så »§ 274, stk. 3,« og »§ 294, stk. 3,« udgår.

Det foreslåede er en konsekvensændring som følge af ophævelse af §§ 274 og 294 ved lov nr. 243 af 7. marts 2023.

Til nr. 9 (§ 259, stk. 2, i lov om forsikringsvirksomhed)

Det fremgår af § 259, stk. 1, i lov om forsikringsvirksomhed, at Finanstilsynet påser overholdelsen af denne lov og regler fastsat i medfør heraf. Det fremgår videre af § 259, stk. 2, at Finanstilsynet påser overholdelsen af en række EU-retsakter og regler udstedt i medfør heraf.

Det foreslås i *§* 259, *stk. 2, nr. 8,* at Finanstilsynet påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring vil medføre, at Finanstilsynet bliver udpeget som kompetent myndighed efter DORA-forordningen til at føre tilsyn med overholdelsen af forordningen.

Forordningen finder bl.a. anvendelse på forsikrings- og genforsikringsselskaber, jf. artikel 2, stk. 1, litra n.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningen, jf. 269 i lov om forsikringsvirksomhed.

Finanstilsynet får med bestemmelsen bl.a. også mulighed for at give påbud og påtaler for overtrædelser af forordningen, jf. § 259.

Efter artikel 46, litra k, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) sikre overholdelsen af DORA-forordningen for forsikrings- og genforsikringsselskaber.

Bestemmelsen supplerer artikel 46, litra k, i DORA-forordningen.

Til nr. 10 (§ 280, stk. 7, 1. pkt., i lov om forsikringsvirksomhed)

Lov om forsikringsvirksomhed § 280 indeholder regler om påbud om afsættelse af direktører og bestyrelsesmedlemmer i et forsikringsselskab. § 280, stk. 7, 1. pkt., i lov om forsikringsvirksomhed fastsætter regler om, at Finanstilsynet af egen drift eller efter ansøgning kan tilbagekalde et påbud meddelt efter stk. 2, 3 eller 5.

Det fremgår af bemærkningerne til § 280, stk. 7, i lov om forsikringsvirksomhed, at bestemmelsen viderefører § 351, stk. 8, i lov om finansiel virksomhed uden ændringer, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 525.

I lov om finansiel virksomhed § 351, stk. 8, henvises der til § 351, stk. 5, 3. pkt., i lov om finansiel virksomhed. Med § 1, nr. 35, i lov nr. 409 af 25. april 2023 (Gennemførelse af Ansvarsudvalgets forslag om skærpet ansvarsvurdering for ledelsesmedlemmer m.v. i finansielle virksomheder og

ændring af reglerne om egnethed og hæderlighed) blev der indsat to nye punktummer i § 351, stk. 5. Ved en fejl blev der ikke foretaget en konsekvensændring af henvisningen til stk. 5, 3. pkt., i § 351, stk. 8, i lov om finansiel virksomhed.

Det fremgår af bemærkningerne til § 280, stk. 4, i lov om forsikringsvirksomhed, at bestemmelsen viderefører § 351, stk. 5, i lov om finansiel virksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 524.

Det fremgår af bemærkningerne til § 280, stk. 5, i lov om forsikringsvirksomhed, at bestemmelsen viderefører § 351, stk. 6, i lov om finansiel virksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 524.

Henvisningen til stk. 5 i § 280, stk. 7, i lov om forsikringsvirksomhed er således en fejl. Der burde i stedet henvises til stk. 4, 3. pkt.

Det foreslås i *§ 280, stk. 7, 1. pkt.,* at »stk. 2, 3 eller 5« ændres til »stk. 2 eller 3, eller stk. 4, 3. pkt.«.

Det foreslåede vil medføre, at Finanstilsynet af egen drift eller efter ansøgning kan tilbagekalde et påbud meddelt efter stk. 2 eller 3, eller stk. 4, 3. pkt.

Der henvises derudover til bemærkningerne til lovforslagets § 1, nr. 29.

Til nr. 11 (§ 289, stk. 1, nr. 14, i lov om forsikringsvirksomhed)

Det fremgår af § 285, stk. 1, i lov om forsikringsvirksomhed, at Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e bl.a. er forpligtet til at hemmeligholde fortrolige oplysninger, som de får kendskab til gennem tilsynsvirksomheden.

§ 289, stk. 1, i lov om forsikringsformidling er en undtagelse til tavshedspligten i § 285, stk. 1. Bestemmelsen fastsætter i hvilke tilfælde, der ikke er noget til hinder for, at fortrolige oplysninger videregives til en række institutioner, myndigheder og organer mv. i et andet EU/EØS-land mv.

I medfør af § 289, stk. 1, har Finanstilsynet ikke mulighed for at videregive oplysninger til Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 289, stk. 1,* at indsætte *nr. 14,* hvorefter Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til SRB og ENISA.

Når Finanstilsynet modtager en indberetning om en større it-relateret hændelse fra et forsikrings- eller genforsikringsselskab, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 12 (§ 302, stk. 1, i lov om forsikringsvirksomhed)

§ 302, stk. 1, i lov om forsikringsvirksomhed nævner de virksomheder, der kan anses som part i forhold til Finanstilsynet i sager, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af bl.a. lov om forsikringsvirksomhed.

Det foreslås at ændre *§ 302, stk. 1,* således, at der fremgår en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at virksomheder, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af DORA-forordningen eller regler udstedt i medfør heraf, også vil være at anse som parter i afgørelsessagen.

Til nr. 13 (§ 309, stk. 1, nr. 9, i lov om forsikringsvirksomhed)
§ 309, stk. 1, i lov om forsikringsvirksomhed indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet retter sig til. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet i medfør af lov om forsikringsvirksomhed og en række forordninger.

Det foreslås i *§ 309, stk. 1, nr. 9,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at afgørelser truffet af Finanstilsynet i medfør af DORA-forordningen eller regler udstedt i medfør heraf kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, som afgørelsen retter sig til.

Til nr. 14 (§ 310, nr. 9, i lov om forsikringsvirksomhed)

§ 310 i lov om forsikringsvirksomhed er en generel bemyndigelsesbestemmelse, der giver erhvervsministeren bemyndigelse til at fastsætte regler, som er nødvendige for at anvende eller gennemføre de afgørelser eller retsakter, som vedtages af Kommissionen i medfør af en række direktiver og forordninger.

Det foreslås i *§ 310, nr. 9,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at erhvervsministeren bemyndiges til at fastsætte regulering på de områder, hvor det som følge af delegerede retsakter, udstedt i medfør af DORA-forordningen, måtte være nødvendigt.
Til nr.16 15 (§ 312, stk. 1, nr. 3, i lov om forsikringsvirksomhed)

Det foreslås at ændre *§ 312, stk. 1, nr. 3,* i lov om forsikringsvirksomhed, så overtrædelser af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-4, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1 og 2, stk. 3, 1. og 2. pkt., stk. 4, 6 og 7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26, stk. 1, stk. 2, stk. 3, stk. 5, stk. 6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) straffes med bøde.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at

det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der forsikrings- og genforsikringsselskaber, jf. artikel 2, stk. 1, litra n, jf. artikel 2, stk. 2, i DORA-forordningen.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen

af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel

virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og

informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre

sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende

inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og

-tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-

systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en

samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige

kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som

beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er

nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik

på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger

passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og

værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang

med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres

strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille

det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og

indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af

insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan

træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner

eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til nr. 16 (§ 312, stk. 2, i lov om forsikringsvirksomhed)

Bestemmelser om straf i lov om forsikringsvirksomhed findes i § 312. Af stk. 1 fremgår det, hvilke bestemmelser der kan medføre straf i form af bøde for overtrædelse.

Lov om forsikringsvirksomhed § 125, 1. pkt., fastsætter, at den eksterne revision i revisionsprotokollatet vedrørende årsrapporten skal afgive erklæring om, hvorvidt forsikringsselskabet har eksponering mod erhvervsvirksomheder omfattet af §§ 121 og 122 i lov om forsikringsvirksomhed. Bestemmelsen fastsætter i 2. pkt., at føres der ikke en revisionsprotokol, skal erklæringen nævnt i 1. pkt. fremgå af anden tilsvarende dokumentation.

Det fremgår af bemærkningerne til § 125 i lov om forsikringsvirksomhed, at bestemmelsen er en videreførelse af § 80, stk. 8, 2. og 3. pkt., i lov om finansiel virksomhed. Det fremgår også af bemærkningerne til § 125 i lov om forsikringsvirksomhed, at bestemmelsen kan straffes efter § 312, stk. 1, i lov om forsikringsvirksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 305.

I § 373, stk. 2, i lov om finansiel virksomhed er det fastsat, at overtrædelse af § 80, stk. 8, i lov om finansiel virksomhed, kan straffes med bøde.

Det foreslås at indsætte »§ 125« i *§ 312, stk. 2.*

Forslaget vil medføre, at overtrædelse af § 125 i lov om forsikringsvirksomhed kan straffes med bøde. Forslaget vil rette op på en fejl i lov om forsikringsvirksomhed, hvorefter § 125 ikke fremgår af straffebestemmelsen i § 312, stk. 2.

Til nr. 17 (§ 313, stk. 1, i lov om forsikringsvirksomhed)

Lov om forsikringsvirksomhed § 313 indeholder regler om straf for manglende overholdelse af påbud. § 313, stk. 1, fastsætter regler om, at et forsikringsselskabs eller en forsikringsholdingvirksomheds manglende efterkommelse af et påbud, der er udstedt i medfør af nærmere angivne bestemmelser, kan straffes med bøde.

I § 313, stk. 1, findes en henvisning til § 275, stk. 2, i lov om forsikringsvirksomhed. § 275 i lov om forsikringsvirksomhed har alene et stykke.

Det fremgår af bemærkningerne til § 275 i lov om forsikringsvirksomhed, at bestemmelsen viderefører § 348, stk. 2, 1. pkt., i lov om finansiel virksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 517. Ligeledes er § 313 en videreførelse af § 373, stk. 3 og 5, i lov om finansiel virksomhed, jf. Folketingstidende 2022-23, tillæg A, L 88 som fremsat, side 598. I § 373, stk. 3, i lov om finansiel virksomhed findes en henvisning til § 348, stk. 2, i lov om finansiel virksomhed.

Det foreslås, at ændre *§ 313, stk. 1,* så henvisningen til § 275, stk. 2, ændres til § 275.

Det foreslåede vil medføre, at et forsikringsselskab eller en forsikringsholdingvirksomhed, der ikke efterkommer et påbud udstedt i medfør af § 275 i lov om forsikringsvirksomhed, kan straffes med bøde. Forslaget retter op på en fejl i lov om forsikringsvirksomhed, hvorefter bestemmelsen indeholder en upræcis henvisning til § 275.

Til § 9

Til nr. 1 (§ 22, stk. 1, 2. pkt., i lov om forsikringsformidling)

Det fremgår af § 22, stk. 1, 1. pkt., i lov om forsikringsformidling, at Finanstilsynet påser overholdelsen af denne lov og regler udstedt i medfør af loven. Det fremgår videre af § 22, stk. 1, 2. pkt., at Finanstilsynet påser overholdelsen af de i bestemmelsen nævnte forordninger og regler udstedt i medfør heraf.

Det foreslås i *§ 22, stk. 1, 2. pkt.,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring vil medføre, at Finanstilsynet bliver udpeget som kompetent myndighed efter DORA-forordningen til at føre tilsyn med overholdelsen af forordningen.

Forordningen finder bl.a. anvendelse på forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere, jf. artikel 2, stk. 1, litra o. Forordningen finder dog ikke anvendelse på denne type af virksomheder, der er mikrovirksomheder eller små og mellemstore virksomheder, jf. artikel 2, stk. 3, litra e.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningen, jf. § 26 i lov om forsikringsformidlere.

Finanstilsynet får med bestemmelsen bl.a. også mulighed for at give påbud og påtaler for overtrædelser af forordningen, jf. § 22.

Efter artikel 46, litra l, i DORA-forordningen skal den kompetente myndighed, der er udpeget i medfør af Europa-Parlamentets og Rådets direktiv (EU) 2016/97 af 20. januar 2016 om forsikringsdistribution sikre overholdelsen af DORA-forordningen for forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringsformidlere.

Bestemmelsen supplerer artikel 46, litra l, i DORA-forordningen.

Til nr. 2 (§ 31, stk. 6, nr. 18, i lov om forsikringsformidling)

I medfør af § 31, stk. 1, i lov om forsikringsformidling er Finanstilsynets ansatte under ansvar efter straffelovens §§ 152-152 e forpligtet til at hemmeligholde fortrolige oplysninger som de bl.a. får kendskab til gennem tilsynsvirksomheden.

§ 31, stk. 6, i lov om forsikringsformidling er en undtagelse til tavshedspligten i stk. 1. Bestemmelsen fastsætter til hvem og i hvilke tilfælde Finanstilsynet kan videregive fortrolige oplysninger, uanset § 31, stk. 1.

I medfør af § 31, stk. 6, har Finanstilsynet ikke mulighed for at videregive oplysninger til Center for Cybersikkerhed, Den Fælles Afviklingsinstans (SRB) eller Den Europæiske Unions Agentur for Cybersikkerhed (ENISA).

Det foreslås i *§ 31, stk. 6, nr. 18,* at Finanstilsynet kan videregive oplysninger til myndigheder, der varetager opgaver i henhold til DORA-

forordningen, under forudsætning af at oplysningerne er nødvendige for disse myndigheders varetagelse af opgaver i henhold til forordningen.

Med den foreslåede bestemmelse, vil det bl.a. blive muligt for Finanstilsynet at videregive fortrolige oplysninger til Center for Cybersikkerhed, SRB og ENISA.

Når Finanstilsynet modtager en indberetning fra en forsikringsformidler, en genforsikringsformidler eller en accessorisk forsikringsformidler om en større it-relateret hændelse, jf. artikel 19, stk. 1, 1. pkt., i DORA-forordningen, skal Finanstilsynet alt efter hvad der er relevant, rettidigt forelægge nærmere oplysninger om hændelsen til nationale og EU-retlige myndigheder og organer, jf. artikel 19, stk. 6, i DORA-forordningen.

Artikel 19, stk. 6, nævner bl.a. de centrale kontaktpunkter eller CSIRT'er, der er udpeget eller oprettet i overensstemmelse med NIS 2-direktivet, dvs. Center for Cybersikkerhed. Bestemmelsen nævner også SRB for så vidt angår de enheder eller koncerner, der er omhandlet i henholdsvis artikel 7, stk. 2, artikel 7, stk. 4, litra b, og artikel 7, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) nr. 806/2014 af 15. juli 2014 om ensartede regler og en ensartet procedure for afvikling af kreditinstitutter og visse investeringsselskaber inden for rammerne af en fælles afviklingsmekanisme og en fælles afviklingsfond, dvs. bl.a. pengeinstitutter, der er underlagt tilsyn af Den Europæiske Centralbank, hvis sådanne oplysninger vedrører hændelser, der udgør en risiko for sikringen af kritiske funktioner, jf. artikel 2, stk. 1, nr. 35, i direktiv 2014/59/EU Europa-Parlamentets og Rådets direktiv 2014/59/EU af 15. maj 2014 om et regelsæt for genopretning og afvikling af kreditinstitutter og investeringsselskaber (BRRD).

En underretning om større it-relaterede hændelser til SRB kan eksempelvis blive relevant, hvor en hændelse kan få systemiske konsekvenser og dermed også konsekvenser for virksomheder, der er omfatter af Den Fælles Afviklingsmekanisme.

For så vidt angår videregivelse af fortrolige oplysninger til ENISA kan dette bl.a. blive relevant i de tilfælde, hvor hændelsesindberetninger til Finanstilsynet videreformidles i forbindelse med det samarbejde, der bliver iværksat på tværs af de nationale og europæiske finansielle tilsynsmyndigheder og afviklingsmyndigheder, SRB og ENISA i henhold til artikel 49 i DORA-forordningen. Samarbejdet i henhold til artikel 49 går ud på udveksling af effektive fremgangsmåder på tværs af den finansielle sektor for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer.

Til nr. 3 og 5 (§ 33, stk. 1, 8. og 10. pkt., i lov om forsikringsformidling)

Det følger § 33, stk. 1, 1. pkt., i lov om forsikringsformidling, at der skal ske offentliggørelse af reaktioner, som Finanstilsynets bestyrelse har truffet beslutning om, eller som Finanstilsynets har givet efter delegation fra Finanstilsynets bestyrelse. Offentliggørelsen skal ske med angivelse virksomhedens navn. § 33, stk. 1, regulerer ikke det tilfælde, hvor det alene er Finanstilsynet uden delegation fra bestyrelsen, der har truffet afgørelse om at give en reaktion til en virksomhed.

Videre fremgår det af § 33, stk. 1, 9. pkt., at indbringes en reaktion, der offentliggøres i henhold til stk. 1, 1. pkt., for Erhvervsankenævnet eller domstolene, skal dette fremgå af Finanstilsynets offentliggørelse, og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Det foreslås i *§ 33, stk. 1, 8. pkt.,* at reaktioner givet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og forordninger udstedt i medfør heraf, skal offentliggøres på Finanstilsynets hjemmeside med angivelse af virksomhedens navn.

Med den foreslåede ændring vil Finanstilsynet skulle offentliggøre reaktioner, der er givet af Finanstilsynet til en virksomhed for en overtrædelse af DORA-forordningen. Ved reaktioner forstås f.eks. påbud eller påtaler. Reaktionen skal offentliggøres på Finanstilsynets hjemmeside. Derimod er virksomheden ikke selv forpligtet til at offentliggøre reaktionen. Virksomheden vil kun være forpligtet til at offentliggøre reaktionen, hvis bestyrelsen har truffet beslutning herom i henhold til DORA-forordningen, jf. § 33, stk. 1, 1. pkt.

Videre foreslås det i *§ 33, stk. 1, 9. pkt.,* der bliver 10. pkt., at indsætte en henvisning til 8. pkt., hvorefter det skal fremgå af Finanstilsynets offentliggørelse, at en reaktion, der offentliggøres i henhold til enten stk. 1, 1. pkt., eller 8. pkt., indbringes for Erhvervsankenævnet eller domstolene, og det efterfølgende resultat af Erhvervsankenævnets eller domstolenes afgørelse skal ligeledes offentliggøres på Finanstilsynets hjemmeside hurtigst muligt.

Den foreslåede ændring i § 33, stk. 1, 8. og 10. pkt., gennemfører artikel 54, stk. 1, i DORA-forordningen, hvormed de kompetente myndigheder uden unødigt ophold på deres officielle websteder skal offentliggøre enhver afgørelse om pålæggelse af en administrativ sanktion, som ikke kan

påklages, efter at modtageren af sanktionen er blevet underrettet om afgørelsen. En administrativ sanktion kan bl.a. være et påbud eller en påtale.

Det fremgår dog videre af artikel 54, stk. 5, i DORA-forordningen, at hvis den kompetente myndighed offentliggør en afgørelse om at pålægge en administrativ sanktion, der kan indbringes for de relevante judicielle myndigheder, lægger de kompetente myndigheder straks denne oplysning på deres officielle websted sammen med eventuelle efterfølgende oplysninger om resultatet af denne indbringelse på et senere tidspunkt. En judiciel afgørelse, som annullerer en afgørelse om at pålægge en administrativ sanktion, skal også offentliggøres.

Artikel 54, stk. 1 og 5, svarer derfor til kravet om offentliggørelse af reaktioner i henhold til DORA-forordningen og den efterfølgende offentliggørelse af indbringelse af en reaktion til enten Erhvervsankenævnet eller domstolene i henhold til de to forslag i § 33, stk. 1, 8. og 10. pkt.

Til nr. 4 (§ 33, stk. 1, 9. pkt., i lov om forsikringsformidling)

Det følger af § 33, stk. 1, 8. pkt., i lov om forsikringsformidling, at reaktioner givet af Finanstilsynets bestyrelse i henhold til lovens § 22, stk. 2, jf. § 345, stk. 12, nr. 6, i lov om finansiel virksomhed, dvs. Finanstilsynets bestyrelses beslutninger om at overgive sager af principiel karakter, og sager der har videregående betydelige følger til politimæssig efterforskning, og Finanstilsynets beslutninger om at overgive sager efter denne lov eller regler udstedt i medfør af loven eller efter forordninger udstedt i medfør af Europa-Parlamentets og Rådets direktiv (EU) 2016/97 af 20. januar 2016 om forsikringsdistribution til politimæssig efterforskning skal offentliggøres som resumé på Finanstilsynets hjemmeside med angivelse af virksomhedens navn, jf. dog stk. 4.

Det foreslås i *§ 33, stk. 1, 8. pkt.,* der bliver 9. pkt., at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Med den foreslåede ændring vil Finanstilsynet også skulle offentliggøre beslutninger truffet af bestyrelsen eller af Finanstilsynet efter delegation fra bestyrelsen om at overgive sager om overtrædelse af bestemmelser i DORA-forordningen til politimæssig efterforskning i form af resumé på Finanstilsynets hjemmeside. Der henvises i det hele til bemærkningerne til § 33, stk. 1, jf. Folketingstidende 2017-2018, tillæg A, L 8 som fremsat, side 89-91.

Der henvises i øvrigt til § 9, nr. 8, i lovforslaget, der nævner de bestemmelser i forordningen, der er strafbelagte.

Til nr. 6 (§ 36, stk. 1, i lov om forsikringsformidling)

§ 36, stk. 1, nævner de virksomheder, der kan anses som part i forhold til Finanstilsynet i sager, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af bl.a. lov om forsikringsformidlere.

Det foreslås i *§ 36, stk. 1,* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Det foreslåede medfører, at virksomheder, som Finanstilsynet har truffet eller vil træffe afgørelse over for i medfør af DORA-forordningen eller regler udstedt i medfør heraf, også vil være at anse som parter i afgørelsessagen.

Til nr. 7 (§ 37 i lov om forsikringsformidling)

§ 37 indeholder en klageadgang til Erhvervsankenævnet for den, som en afgørelse truffet af Finanstilsynet retter sig til. Bestemmelsen nævner bl.a. afgørelser truffet af Finanstilsynet i medfør af lov om forsikringsformidling og de i bestemmelsen nævnte forordninger.

Det foreslås i *§ 37* at indsætte en henvisning til Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Den foreslåede ændring vil medføre, at afgørelser truffet af Finanstilsynet i medfør af DORA-forordningen og regler udstedt i medfør heraf kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, som afgørelsen retter sig til.

Til nr. 8 (§ 42, stk. 2, i lov om forsikringsformidling)

Det foreslås at ændre *§ 42, stk. 2,* i lov om forsikringsformidling, så overtrædelser af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-4, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1 og 2, stk. 3, 1. og 2. pkt., stk. 4, 6 og 7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26,

stk. 1, stk. 2, stk. 3, stk. 5, stk. 6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) straffes med bøde.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der forsikringsformidlere, genforsikringsformidlere og accessoriske forsikringformidlere, jf. artikel 2, stk. 1, litra o, jf. artikel 2, stk. 2, i DORA forordningen.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med

tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de

kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt

være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er

teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke

foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-

processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i

overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -

genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for

dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en

genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om

ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i

forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året

aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier

mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der

foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn

til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af

artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i

forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den

kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en

forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges

skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-

tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 10

Til nr. 1 (§ 12 a i lov om en garantifond for skadesforsikringsselskaber)

Det fremgår af den gældende § 12, stk. 1, i lov om en garantifond for skadesforsikringsselskaber, at Garantifondens (Fonden) bestyrelse antager fornøden medhjælp.

Bestemmelsen fastsætter, at Fonden antager fornøden medhjælp, men indeholder ikke en direkte forpligtigelse for Fondens bestyrelse til at antage medhjælp blandt andet i form af et administrationsselskab.

Det foreslås, at der indsættes en ny § 12 a.

Det foreslås i *§ 12 a, stk. 1*, at Fondens bestyrelse, som en del af at antage fornøden medhjælp efter § 12, stk. 1, skal forsøge at indgå aftale med et forsikringsselskab som administrationsselskab, jf. dog stk. 3.

Det foreslåede vil medføre, at Fonden skal forsøge at indgå en aftale med et forsikringsselskab om varetagelse af opgaven som administrationsselskab for Fonden efter et evt. forudgående udbud af opgaven.

Det foreslåede skal ses i sammenhæng med den foreslåede § 12 a, stk. 3, hvorefter Finanstilsynet skal udnævne et administrationsselskab for Fonden, der opfylder kriterierne fastsat i stk. 4, og i overensstemmelse med stk. 5 og stk. 6, såfremt Fondens bestyrelse ikke kan indgå aftale med et forsikringsselskab som administrationsselskab.

Det betyder, at Fondens bestyrelse skal forsøge at indgå en aftale med et forsikringsselskab som administrationsselskab evt. på baggrund af et offentligt udbud, og at hvis det ikke kan lade sig gøre, skal Finanstilsynet ud fra en række i loven oplistede objektive kriterier udnævne et administrationsselskab for Fonden.

Forslaget om at Finanstilsynet skal udnævne et forsikringsselskab som administrationsselskab efter stk. 3 udelukker ikke, at Fonden efter stk. 1 kan indgå aftale med et udenlandsk forsikringsselskab som administrationsselskab.

Det foreslåede medfører ikke, at Fondens bestyrelse ved indgåelse af en aftale efter den foreslåede § 12 a, stk. 1, kun kan indgå aftale med forsikringsselskaber, der opfylder kriterierne fastsat i den foreslåede § 12 a, stk. 4, nr. 1-5.

Det foreslås i *§ 12 a, stk. 2,* at Fonden skriftligt skal orientere Finanstilsynet, når en aftale efter stk. 1 er indgået. Fonden skal ligeledes skriftligt orientere Finanstilsynet, hvis Fonden ikke kan indgå en aftale efter stk. 1.

Det foreslåede vil medføre, at Fonden får pligt til skriftligt at orientere Finanstilsynet, når en eventuel aftale med et forsikringsselskab som administrationsselskab er indgået mellem Fonden og forsikringsselskabet. Det foreslåede vil endvidere medføre, at Fonden også får pligt til at orientere Finanstilsynet, hvis Fonden ikke er lykkedes med på frivilligt grundlag at indgå aftale med et forsikringsselskab som administrationsselskab.

Det foreslåede skal sikre, at Finanstilsynet, uanset om Fondens bestyrelse har indgået en aftale med et forsikringsselskab som administrationsselskab eller ej, er orienteret herom. Finanstilsynet kan i så fald i tilfælde af, at det ikke har været muligt for Fondens bestyrelse at indgå en aftale med et forsikringsselskab som administrationsselskab, efter den foreslåede § 12 a, stk. 3, udnævne et forsikringsselskab som administrationsselskab for Fonden.

Det foreslås i *§ 12 a, stk. 3,* at hvis Fondens bestyrelse ikke kan indgå aftale med et forsikringsselskab som administrationsselskab, skal Finanstilsynet udnævne et administrationsselskab for Fonden, der opfylder kriterierne fastsat i stk. 4, nr. 1-5, og i overensstemmelse med stk. 5 og 6.

Det foreslåede vil medføre, at i de tilfælde, hvor Fonden ikke selv kan indgå en aftale med et forsikringsselskab som administrationsselskab for Fonden, vil Finanstilsynet på baggrund af objektivt fastsatte kriterier i den foreslåede § 12 a, stk. 4, nr. 1-5, og i overensstemmelse med principperne fastlagt i den foreslåede § 12 a, stk. 5 og 6, udnævne et forsikringsselskab som administrationsselskab for Fonden.

Der henvises til bemærkningerne til den foreslåede § 12 a, stk. 4, nr. 1-5, og § 12 a, stk. 5 og 6.

Det foreslås i *§ 12 a, stk. 4,* at fastlægge kravene til, hvornår et forsikringsselskab efter stk. 3, jf. dog stk. 5 og 6, kan udnævnes som administrationsselskab for Fonden.

Det foreslåede vil medføre, at Finanstilsynet i sin afgørelse af, om et forsikringsselskab skal udnævnes som administrationsselskab for Fonden, skal inddrage om forsikringsselskabet opfylder kriterierne fastsat i § 12 a, stk. 4, nr. 1-5.

Et forsikringsselskab skal opfylde alle kriterierne fastsat i § 12 a, stk. 4, nr. 1-5, for at Finanstilsynet kan udnævne forsikringsselskabet som administrationsselskab for Fonden. Kriterierne er fastlagt ud fra et hensyn til, at alene de største forsikringsselskaber skal kunne udnævnes som administrationsselskab for Fonden, idet det kræver en vis størrelse, erfaring med en række forskellige forsikringsklasser, samt økonomisk robusthed for at være administrationsselskab for Fonden.

Det foreslås i *§ 12 a, stk. 4, nr. 1,* at forsikringsselskabet skal have Finanstilsynets tilladelse til at drive forsikringsvirksomhed uden begrænsninger til forsikringsklasserne 1-3, 6, 8-10, 12, 13, 16, 17 og 18 i bilag 1 i lov om forsikringsvirksomhed.

Det foreslåede vil medføre, at kun danske forsikringsselskaber kan udnævnes af Finanstilsynet som administrationsselskab. Derudover vil kriteriet om, at forsikringsselskabet uden begrænsninger skal have tilladelse til forsikringsklasserne 1-3, 6, 8-10, 12, 13, 16, 17 og 18 i bilag 1 i lov om forsikringsvirksomhed, medføre, at administrationsselskabet vil kunne håndtere næsten alle typer af skader i tilfælde af, at der i perioden hvor forsikringsselskabet et udnævnt som administrationsselskab, indtræder en konkurs.

Det foreslås i *§ 12 a, stk. 4, nr. 2,* at forsikringsselskabet skal have en årlig bruttopræmieindtægt på minimum 2 mia. kr. om året.

Det foreslåede vil medføre, at for et forsikringsselskab kan udnævnes som administrationsselskab, skal forsikringsselskabet have en årlig bruttopræmieindtægt på minimum 2. mia. kr. Opfylder forsikringsselskabet ikke kriteriet, kan forsikringsselskabet ikke udnævnes som administrationsselskab. Kriteriet sikrer, at det kun er de største forsikringsselskaber, der kan udnævnes som administrationsselskab for Fonden.

Det foreslås i *§ 12 a, stk. 4, nr. 3,* at forsikringsselskabet i de to seneste regnskabsår på balancetidspunktet i gennemsnit skal have haft minimum 125 eller flere fuldtidsansatte.

Det foreslåede vil medføre, at forsikringsselskabet har en størrelse, hvorefter der er krav om intern revision. Dette vil sikre, at der er en intern kontrol i forsikringsselskabet, som bidrager til øget sikkerhed i form af blandt andet rapportering til ledelsen, overvågning af det interne regnskab m.v.

Det foreslås i *§ 12 a, stk. 4, nr. 4,* at forsikringsselskabet skal overholde det for forsikringsselskabet fastsatte solvenskrav.

Det foreslåede vil medføre, at forsikringsselskabet skal have en vis økonomisk robusthed. Kriteriet er fastsat ud fra et hensyn om, at opgaven som administrationsselskab er en krævende opgave, hvis der indtræder en konkurs i et forsikringsselskab, hvorfor det vil være uhensigtsmæssigt, hvis et forsikringsselskab, der selv er i økonomiske vanskeligheder, ligeledes er administrationsselskab for Fonden.

Det foreslås i *§ 12 a, stk. 4, nr. 5,* at forsikringsselskabet minimum skal have en markedsandel i Danmark på 3 pct. målt på bruttopræmie.

Det foreslåede vil medføre, at for et forsikringsselskab af Finanstilsynet kan udnævnes som administrationsselskab for Fonden, skal forsikringsselskabet minimum have en markedsandel i Danmark på 3 pct. målt på bruttopræmie. Markedsandelen vil være for danske forsikringsselskaber for dansk bruttopræmie.

Kriteriet skal sikre, at det kun er de største forsikringsselskaber i Danmark, der kan udnævnes som administrationsselskab for Fonden, da opgaven som administrationsselskab kræver en vis størrelse samt erfaring med skadesbehandling.

Det foreslås i *§ 12 a, stk. 5, 1. pkt.,* at i tilfælde af, at flere forsikringsselskaber opfylder kriterierne i stk. 4, skal Finanstilsynet udnævne et forsikringsselskab som administrationsselskab på baggrund af en rotationsordning.

Det foreslåede medfører en rotationsordning for de forsikringsselskaber, som opfylder kriterierne fastsat i stk. 4, nr. 1-5, og som dermed kan udnævnes af Finanstilsynet som administrationsselskab for Fonden.

Rotationsordningen skal sikre, at alle forsikringsselskaber, der opfylder de fastsatte objektive kriterier, på et tidspunkt skal være administrationsselskab for Fonden.

Rotationsordningen vil kun være aktuel, hvis det ikke er muligt for Fondens bestyrelse selv at indgå aftale med et forsikringsselskab som administrationsselskab, og Finanstilsynet derfor skal udnævne et forsikringsselskab som administrationsselskab.

Det foreslås videre i *§ 12 a, stk. 5, 2. pkt.,* at Finanstilsynet dog i sin afgørelse skal inddrage relevante forhold relateret til de omfattede

forsikringsselskaber i sin vurdering af hvilket forsikringsselskab, der skal udnævnes som administrationsselskab.

Det foreslåede vil medføre, at Finanstilsynet i sin afgørelse skal inddrage relevante forhold i sin vurdering af hvilket forsikringsselskab, der skal udnævnes som administrationsselskab.

Det foreslåede vil medføre en forpligtigelse for Finanstilsynet til i sin afgørelse at inddrage, om et forsikringsselskab tidligere har fungeret som administrationsselskab for Fonden, idet der skal lægges vægt på, at et enkelt selskab ikke i urimeligt omfang skal pålægges opgaven med at være administrationsselskab. Finanstilsynet skal endvidere inddrage om forsikringsselskabet før rotationsordningens ikrafttræden har været administrationsselskab for Fonden.

Det foreslåede vil desuden medføre, at Finanstilsynet i sin afgørelse skal tage hensyn til, om der er forhold i et forsikringsselskab, der gør det uhensigtsmæssigt, at et forsikringsselskab udnævnes som administrationsselskab for Fonden, jf. nedenfor.

Eksempler på dette kan være en igangværende fusion eller andre tungtvejende administrative årsager. Det vil således ikke være tilstrækkeligt, at forsikringsselskabet eksempelvis oplever travlhed. Finanstilsynet skal som følge heraf som udgangspunkt udnævne det næste forsikringsselskab i rotationsordningen som administrationsselskab for Fonden, og forsikringsselskabet, der springes over, vil herefter som udgangspunkt være det næste i rotationsordningen til at blive udnævnt som administrationsselskab for Fonden.

Forsikringsselskaber som ved f.eks. vækst i markedsandel kommer til at opfylde alle kriterierne fastsat i § 12 a, stk. 4, nr. 1-5, vil kunne udnævnes af Finanstilsynet som administrationsselskab for Fonden. Det pågældende forsikringsselskab vil herefter indgå som det sidste forsikringsselskab i rotationsordningen, medmindre forsikringsselskaberne sidst i rotationsordningen tidligere har være administrationsselskab for Fonden. Finanstilsynet skal som følge heraf udnævne det nye forsikringsselskab i rotationsordningen som administrationsselskab, før Finanstilsynet kan udnævne de forsikringsselskaber, som tidligere har været administrationsselskab for Fonden.

Et forsikringsselskab, der ikke længere opfylder kriterierne fastsat i § 12 a, stk. 4, nr. 1-5, kan ikke udnævnes af Finanstilsynet som administrationsselskab. Det pågældende forsikringsselskab vil herefter udgå

af rotationsordningen, hvorefter de efterfølgende forsikringsselskaber vil rykke op i rækken.

Opfylder et forsikringsselskab ikke længere kriterierne fastsat i § 12 a, stk. 4, nr. 1-5 i løbet af perioden, hvor forsikringsselskabet er udnævnt som administrationsselskab for Fonden, skal forsikringsselskabet fortsætte med at være administrationsselskab for Fonden indtil perioden på 48 måneder er udløbet. Opstår der i perioden, hvor forsikringsselskabet er udnævnt som administrationsselskab for Fonden, en konkurs i et andet forsikringsselskab, skal forsikringsselskabet, som er udnævnt som administrationsselskab, bistå Fonden indtil sagsbehandlingen i forbindelse med konkursen er afsluttet, uanset om perioden på de 48 måneder i mellemtiden måtte være ophørt, og at det ikke længere opfylder kriterierne i § 12 a, stk. 4, nr. 1-5.

Rotationsordningen er ikke til hinder for, at et forsikringsselskab frivilligt indgår aftale med Fonden om, at det pågældende forsikringsselskab skal varetage opgaven som administrationsselskab. Dog vil et forsikringsselskab, som frivilligt indgår aftale med Fonden om opgaven som administrationsselskab, efter endt periode være nederst i rotationsordningen, såfremt forsikringsselskabet ellers opfylder kriterierne fastsat i § 12 a, stk. 4, nr. 1-5. Det skyldes, at Finanstilsynet ved udnævnelsen af et forsikringsselskab som administrationsselskab skal inddrage, om de omfattede forsikringsselskaber tidligere har været administrationsselskab for Fonden.

Finanstilsynets afgørelse om, at et forsikringsselskab skal være administrationsselskab for Fonden, er en forvaltningsretlig afgørelse og skal dermed overholde de almindelige forvaltningsretlige regler.

Afgørelser truffet af Finanstilsynet i medfør af den foreslåede § 12 a, stk. 3, kan af den, som afgørelsen retter sig mod, indbringes for Erhvervsankenævnet, senest 4 uger efter, at afgørelsen er meddelt den pågældende, jf. den foreslåede § 17 b.

Der henvises i øvrigt til bemærkningerne til lovforslagets § 10, nr. 2.

Det foreslås i *§ 12 a, stk. 6,* at Finanstilsynet, medmindre særlige forhold taler herfor, ikke kan udnævne et forsikringsselskab som administrationsselskab i to af hinanden efterfølgende perioder.

Det foreslåede vil medføre, at et forsikringsselskab som udgangspunkt ikke kan udnævnes som administrationsselskab, hvis forsikringsselskabet allerede er administrationsselskab på tidspunktet, hvor Finanstilsynet skal udnævne et forsikringsselskab som administrationsselskab. Skal et

forsikringsselskab udnævnes som administrationsselskab i to af hinanden efterfølgende perioder, skal særlige forhold tale herfor.

Særlige forhold kan eksempelvis være, at de øvrige forsikringsselskaber i rotationsordningen ikke er egnet som administrationsselskab grundet en igangværende fusion eller andre administrative årsager. Det kan også være, at de øvrige forsikringsselskaber ikke længere opfylder kriterierne fastsat i den foreslåede § 12 a, stk. 4, nr. 1-5. Det vil herefter være nødvendigt at udnævne forsikringsselskabet, som allerede er administrationsselskab for Fonden, som administrationsselskab for endnu en periode.

Det foreslåede vil bidrage til at sikre en rotationsordning for de forsikringsselskaber, der opfylder kriterierne fastsat i den foreslåede § 12 a, stk. 4, nr. 1-5, og som på baggrund heraf kan udnævnes som administrationsselskab for Fonden.

Der henvises i øvrigt til bemærkningerne til den foreslåede § 12 a, stk. 5.

Det foreslås i *§ 12 a, stk. 7,* at Finanstilsynet skal udnævne et forsikringsselskab efter stk. 3, for en periode på 48 måneder, jf. dog stk. 8.

Det foreslåede vil medføre, at der som udgangspunkt ikke er forskel på den periode et forsikringsselskab skal være administrationsselskab, uanset om forsikringsselskabet selv har indgået aftale med Fonden om opgaven som administrationsselskab, da Fondens udbud af opgaven som udgangspunkt er for en periode på 48 måneder, eller forsikringsselskabet er udnævnt af Finanstilsynet som administrationsselskab.

Der henvises derudover til det foreslåede § 12 a, stk. 8, hvorefter perioden på de 48 måneder kan blive forlænget i tilfælde af, at der indtræder en konkurs i et andet forsikringsselskab, idet forsikringsselskabet, som er udnævnt som administrationsselskab for Fonden, skal bistå Fonden med sagsbehandlingen i forbindelse med konkursen indtil denne er afsluttet.

Det foreslåede betyder ikke, at Fonden og et forsikringsselskab ved indgåelse af en aftale om opgaven som administrationsselskab, jf. stk. 1, eventuelt kan forhandle længden af den periode, hvor forsikringsselskabet skal være administrationsselskab for Fonden.

Det foreslås i *§ 12 a, stk. 8, 1. pkt.,* at hvis der i løbet af de 48 måneder, hvor et forsikringsselskab er udnævnt som administrationsselskab, opstår en konkurs i et andet forsikringsselskab, skal Fondens bestyrelse indgå aftale med et nyt forsikringsselskab som administrationsselskab, jf. stk. 1, jf. dog stk. 3.

Det foreslåede vil medføre, at Fondens bestyrelse, er forpligtet til at forsøge at indgå aftale med et nyt forsikringsselskab som administrationsselskab, hvis der i den igangværende periode opstår en konkurs i et forsikringsselskab.

Det foreslåede vil endvidere medføre, at hvis det ikke er muligt for Fondens bestyrelse at indgå aftale med et forsikringsselskab som administrationsselskab, skal Finanstilsynet udnævne et forsikringsselskab som administrationsselskab efter den foreslåede § 12 a, stk. 3.

Det foreslåede vil sikre, at et forsikringsselskab udnævnt som administrationsselskab ikke skal skadebehandle to eller flere konkurser i forsikringsselskaber i træk.

Det foreslåede er ikke til hinder for, at Fondens bestyrelse, inden perioden hvor et forsikringsselskab er administrationsselskab udløber, indgår aftale med et forsikringsselskab om, at dette forsikringsselskab ved indeværende periodes udløb skal overtage opgaven som administrationsselskab. Det vil dog være hensigtsmæssigt, hvis Fonden så tidligt som muligt og inden perioden hvor et forsikringsselskab er administrationsselskab udløber, indgår aftale med et forsikringsselskab om, at dette forsikringsselskab ved indeværende periodes udløb skal overtage opgaven som administrationsselskab.

Det foreslåede udelukker endvidere ikke, at forsikringsselskabet, der er administrationsselskab på tidspunktet for konkursens indtræden, kan indgå aftale med Fondens bestyrelse om, at forsikringsselskabet skal fortsætte som administrationsselskab for Fonden i den efterfølgende periode. Forsikringsselskabet kan derfor påtage sig opgaven som administrationsselskab for endnu en periode, selvom forsikringsselskabet på tidspunktet for en konkurs indtræden allerede er administrationsselskab.

Det foreslås i *§ 12 a, stk. 8, 2. pkt.*, at det forsikringsselskab, der på tidspunktet for konkursens indtræden er administrationsselskab, skal bistå Fonden indtil sagsbehandlingen af konkursen er afsluttet, uanset om perioden på 48 måneder i mellemtiden måtte være ophørt.

Det forslåede vil medføre, at forsikringsselskabet, der på tidspunktet for en konkurs indtræden er administrationsselskab, skal færdiggøre sagsbehandlingen i forbindelse med denne konkurs, uanset om perioden på 48 måneder i mellemtiden måtte være ophørt. Dette skal sikre en hurtig og effektiv sagsbehandling, samt sikre at det konkursramte forsikringsselskabs

forsikringstagere og sikrede ikke skal være i kontakt med f.eks. to forskellige forsikringsselskaber.

Det forslås i *§ 12 a, stk. 9,* at indgår Fondens bestyrelse aftale efter stk. 1 med et forsikringsselskab om at varetage opgaven som administrationsselskab for Fonden efter udløb af en periode, jf. stk. 7, og indtræder der en konkurs i et forsikringsselskab inden den igangværende periode, jf. stk. 7, udløber, skal forsikringsselskabet, som Fondens bestyrelse har indgået aftale med, overtage opgaven som administrationsselskab på tidspunktet for konkursens indtræden.

Derimod vil det stadig være forsikringsselskabet, der på tidspunktet for konkursens indtræden er administrationsselskab, som skal bistå Fonden indtil sagsbehandlingen af konkursen er afsluttet.

Det foreslåede vil medføre, at hvis Fondens bestyrelse har indgået aftale med et forsikringsselskab, der skal indtræde som administrationsselskab ved udløbet af en periode, hvor Finanstilsynet har udnævnt et forsikringsselskab som administrationsselskab, og der i perioden inden forsikringsselskabet, som Fondens bestyrelse har indgået aftale med, indtræder en konkurs i et forsikringsselskab, så skal det forsikringsselskab, som Fondens bestyrelse har indgået aftale med, varetage opgaven fra tidspunktet for konkursens indtræden, hvilket vil være før den ellers aftalte ikrafttræden.

Det foreslåede skal sikre, at det forsikringsselskab, som er administrationsselskab for Fonden på tidspunktet for en konkurs alene skal behandle en konkurs, inden der skal træde et nyt administrationsselskab til. Det foreslåede skal endvidere sikre, at Fonden selv i en kortere periode ikke står uden administrationsselskab.

Det forslås i *§ 12 a, stk. 10,* at Fonden skal betale vederlag til administrationsselskabet udnævnt af Finanstilsynet. Vederlaget fastlægges efter vilkårene i Fondens udbudsmateriale eller andet dokument indeholdende Fondens specificering af opgaverne. Er det ikke muligt for parterne at blive enige om størrelsen på vederlaget, skal Finanstilsynet fastsætte vederlagets størrelse på baggrund af et oplæg fra Fonden.

Det foreslåede vil medføre, at vederlagets størrelse er til forhandling mellem parterne. Det vil betyde, at Fondens bestyrelse kan afslå forsikringsselskabets bud på vederlagets størrelse, hvis dette vurderes urimeligt.

Det foreslåede vil desuden medføre, at Finanstilsynet tillægges beføjelse til at fastsætte vederlagets størrelse på baggrund af et oplæg fra Fonden, hvis

Fondens bestyrelse og forsikringsselskabet ikke kan nå til enighed herom. Afgørelser truffet af Finanstilsynet i medfør af den foreslåede § 12 a, stk. 10, 3. pkt., kan af den som afgørelsen retter sig mod, indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt den pågældende, jf. den foreslåede § 17 b, i lov om en garantifond for skadesforsikringsselskaber.

Der henvises i øvrigt til bemærkningerne til lovforslagets § 10, nr. *2*.

Det foreslås i *§ 12 a, stk. 11*, at forsikringsselskabet, der af Finanstilsynet er udnævnt som administrationsselskab for Fonden, jf. stk. 3, skal varetage de opgaver, der fremgår af Fondens udbudsmateriale eller andet dokument indeholdende Fondens specificering af opgaverne.

Det foreslåede vil medføre, at Fonden i sit udbudsmateriale eller i et andet dokument selv kan fastsætte og beskrive de opgaver, som forsikringsselskabet skal varetage i den periode, hvor forsikringsselskabet er administrationsselskab for Fonden. Det vil betyde en vis fleksibilitet i omfanget af opgaver, som forsikringsselskabet skal varetage som administrationsselskab.

Til nr. 2 (§ 17 b i en lov om en garantifond for skadesforsikringsselskaber)

Der er i lov om en garantifond for skadesforsikringsselskaber ikke en generel klageadgang i forbindelse med afgørelser truffet af Finanstilsynet.

Det foreslås i *§ 17 b*, at afgørelser truffet af Finanstilsynet i medfør af § 12 a, stk. 3 og 10, 3. pkt., kan indbringes for Erhvervsankenævnet senest 4 uger efter, at afgørelsen er meddelt det pågældende forsikringsselskab.

Det foreslåede vil medføre, at det forsikringsselskab som Finanstilsynets afgørelse retter sig mod, kan indbringes for Erhvervsankenævnet. Klagen skal senest indbringes for Erhvervsankenævnet 4 uger efter, at afgørelsen er meddelt det pågældende forsikringsselskab.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 12 a, stk. 3 og 10, 3. pkt., hvorefter Finanstilsynet kan udnævne et forsikringsselskab som administrationsselskab og fastsætte størrelsen på vederlaget, som administrationsselskabet skal have, hvis Fonden og det pågældende forsikringsselskab ikke kan blive enige om herom.

Til § 11

Til nr. 1 (§ 21, stk. 1, 2. pkt., i lov om Kreditforeningen af kommuner og regioner i Danmark)

Det fremgår af § 21 i lov om kreditforeningen af kommuner og regioner i Danmark, at Finanstilsynet påser overholdelsen af lov om Kreditforeningen af kommuner og regioner i Danmark og regler udstedt i medfør heraf.

Det foreslås i *§ 21* at indsætte et *2. pkt.,* hvoraf det fremgår, at Finanstilsynet endvidere påser overholdelsen af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og regler udstedt i medfør heraf.

Den foreslåede ændring vil medføre, at Finanstilsynet udpeges som kompetent myndighed til at påse KommuneKredits overholdelse af reglerne i DORA-forordningen, der finder anvendelse på foreningen i medfør af artikel 2, stk. 1, litra a, i DORA-forordningen.

DORA-forordningen har til formål at modernisere og harmonisere reglerne indenfor it- og cybersikkerhed på tværs af den finansielle sektor ved at fastsætte regler, der skal styrke den operationelle modstandsdygtighed i virksomhedernes informations- og kommunikationsteknologi og hermed mindske risikoen for navnlig cyberangreb og begrænse skaden og prioritere genoptagelsen af aktiviteter i tilfælde af et cyberangreb.

Forordningen indeholder bl.a. regler om risikostyring indenfor informations- og kommunikationsteknologi, styring og indberetning af hændelser der kompromitterer sikkerheden i net- og informationssystemer, test af digital operationel modstandsdygtighed og styring af tredjepartsrisici, dvs. risici der kan opstå ved brug af en virksomheds brug af tjenester indenfor informations- og kommunikationsteknologi, der leveres af en tredjepartsudbyder heraf.

Forordningen finder bl.a. anvendelse på kreditinstitutter, jf. artikel 2, stk. 1, litra a, hvorfor også KommuneKredit omfattes af regelsættet.

I forbindelse med udførelsen af sit tilsyn får Finanstilsynet bl.a. mulighed for at kræve alle oplysninger m.v., som Finanstilsynet skønner nødvendige for Finanstilsynets virksomhed eller til afgørelse af, om der er sket en overtrædelse af forordningen, jf. § 22 i lov om kreditforeningen af kommuner og regioner i Danmark, hvorefter § 347, stk. 1-6, i lov om finansiel virksomhed om indhentelse af oplysninger finder tilsvarende anvendelse på Kreditforeningen af kommuner og regioner i Danmark.

Finanstilsynet får med tilsynskompetencen i bestemmelsen bl.a. også mulighed for at give KommuneKredit påbud og påtaler for overtrædelser af forordningen.

Til nr. 2 (§ 22, stk. 2 og 3, i lov om Kreditforeningen af kommuner og regioner i Danmark)

Det fremgår af § 22, stk. 1, i lov om kreditforeningen af kommuner og regioner i Danmark, at § 346, stk. 1-3, § 347, stk. 1-6, §§ 347 a, 354, 354 a, 354 g og 355, og § 372, stk. 1, i lov om finansiel virksomhed finder tilsvarende anvendelse på foreningen.

Bestemmelsen indebærer, at de udvalgte bestemmelser i lov om finansiel virksomhed, der fastlægger regler om Finanstilsynets tilsyn, finder tilsvarende anvendelse for KommuneKredit. Det omfatter bl.a. oplysningsforpligtelsen overfor Finanstilsynet, jf. § 347 i lov finansiel virksomhed, tavshedspligtsbestemmelsen, jf. § 354 i lov finansiel virksomhed og offentliggørelsesbestemmelsen, jf. § 354 a i lov om finansiel virksomhed.

Som følge af at KommuneKredit bliver omfattet af reglerne i DORA-forordningen, jf. også bemærkningerne til den foreslåede ændring af § 21 i lov om kreditforeningen af kommuner og regioner i Danmark ovenfor, er det nødvendigt, at offentliggørelsesbestemmelsen i § 354 e, i lov om finansiel virksomhed tillige kan finde tilsvarende anvendelse for KommuneKredit, for så vidt angår sager om overtrædelse af DORA-forordningen. Det er også nødvendigt at bemyndigelsesbestemmelsen i § 372 a i lov om finansiel virksomhed til at udstede regler, som er nødvendige for at anvende eller gennemføre de afgørelser eller retsakter, der følger af DORA-forordningen, kan finde tilsvarende anvendelse for KommuneKredit.

Derfor foreslås det i *§ 22* at indsætte et *stk. 2,* hvorefter § 354 e i lov om finansiel virksomhed finder tilsvarende anvendelse på foreningen for sager om overtrædelse af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Bestemmelsen vil indebære, at Finanstilsynet i overensstemmelse med § 354 e i lov om finansiel virksomhed kan offentliggøre påtaler, påbud eller tvangsbøder, som Finanstilsynet kan give til KommuneKredit i sager om overtrædelse af DORA-forordningen. Med den foreslåede bestemmelse sikres det således, at Finanstilsynet kan opfylde de krav til offentliggørelse

af sine tilsynsreaktioner overfor KommuneKredit, der følger af forordningens artikel 54.

Bestemmelsen skal ses i sammenhæng med den ændring, der med lovforslaget også foreslås til § 354 e, stk. 2, 2. pkt., i lov om finansiel virksomhed. Der henvises derfor i det hele til lovforslagets bemærkninger herom.

Det foreslås også at indsætte et *stk. 3* i § 22 i lov om kreditforeningen af kommuner og regioner i Danmark, hvorefter § 372 a i lov om finansiel virksomhed finder tilsvarende anvendelse på foreningen for regler, som er nødvendige for at anvende eller gennemføre de afgørelser eller retsakter, som vedtages af Europa-Kommissionen i medfør af Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor.

Bestemmelsen vil indebære, at erhvervsministeren i overensstemmelse med § 372 a i lov om finansiel virksomhed vil blive bemyndiget til at fastsætte regler for KommuneKredit på de områder, hvor det måtte være nødvendigt for at anvende eller gennemføre de afgørelser eller retsakter, der eventuelt bliver udstedt i medfør af DORA-forordningen.

Bestemmelsen skal ses i sammenhæng med den ændring, der med lovforslaget også foreslås til § 372 a, stk. 1, i lov om finansiel virksomhed. Der henvises derfor i det hele til lovforslagets bemærkninger herom.

Til nr. 3 (§ 25, stk. 2, i lov om Kreditforeningen af kommuner og regioner i Danmark)

Det foreslås at ændre *§ 25, stk. 2,* i lov om kreditforeningen af kommuner og regioner i Danmark, så overtrædelser af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-4, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1 og 2, stk. 3, 1. og 2. pkt., stk. 4, 6 og 7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26, stk. 1, stk. 2, stk. 3, stk. 5, stk. 6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) straffes med bøde.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om

administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der KommuneKredit.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne

kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -

procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig

forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og

efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer

for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen

af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I

sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan

analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede

ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger

om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at

enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle

programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor

kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere

cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed

gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og

forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder

og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 12

Det foreslås at ændre *§ 14, stk. 1, 1. pkt.,* i lov om et skibsfinansieringsinstitut, så overtrædelser af artikel 5, stk. 1-3, artikel 6, stk. 1-8, artikel 7, stk. 1, artikel 8, stk. 1-7, artikel 9, stk. 1-4, artikel 10, stk. 1-4, artikel 11, stk. 1-10, artikel 12, stk. 1 og 2, stk. 3, 1. og 2. pkt., stk. 4, 6

og 7, artikel 13, stk. 1-7, artikel 14, stk. 1-3, artikel 16, stk. 1 og 2, artikel 17, stk. 1-3, artikel 18, stk. 1 og 2, artikel 19, stk. 1, 3 og 4, artikel 24, stk. 1-6, artikel 25, stk. 1-3, artikel 26, stk. 1, stk. 2, stk. 3, stk. 5, stk. 6 og 8, artikel 28, stk. 1-4, 7 og 8, artikel 29, stk. 1 og 2, og artikel 30, stk. 1-3, i Europa-Parlamentets og Rådets forordning (EU) nr. 2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) straffes med bøde.

Med den foreslåede bestemmelse strafbelægges en række overtrædelser af DORA-forordningen i overensstemmelse med forordningens artikel 52, hvorefter medlemsstaterne kan beslutte ikke at fastsætte bestemmelser om administrative sanktioner eller afhjælpende foranstaltninger for overtrædelser, der er omfattet af strafferetlige sanktioner i henhold til national ret.

Overtrædelser af DORA-forordningen kan ske af både fysiske og juridiske personer. I de situationer, hvor ansvarssubjektet er en virksomhed, vil det være udgangspunktet, at tiltalen rejses mod den juridiske person. Der kan i en række tilfælde være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, hvis den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. For virksomheder under stiftelse vil ansvarssubjektet være de personer, der stifter virksomheden, da en virksomhed under stiftelse ikke kan være ansvarssubjekt.

Bødeniveauet tiltænkes fastsat i overensstemmelse med § 372, stk. 12, i lov om finansiel virksomhed. Det fremgår heraf, at der ved udmåling af bøder lægges vægt på overtrædelsens grovhed og gerningsmandens økonomiske forhold. For overtrædelser begået af juridiske personer lægges ved vurderingen af gerningsmandens økonomiske forhold vægt på virksomhedens nettoårsomsætning på gerningstidspunktet. For overtrædelser begået af fysiske personer lægges vægt på den pågældendes indtægtsforhold på gerningstidspunktet. Det er afgørende, at der ved strafudmålingen lægges vægt på de nævnte faktorer, således at bøder vil have en pønal og præventiv effekt på alle aktører på markedet, og således at det finansielle incitament til at overtræde bestemmelserne reduceres. Vurderingen af overtrædelsens grovhed bør foregå uafhængig af gerningsmandens økonomiske forhold.

Nedenfor anføres en uddybende beskrivelse af indholdet af de enkelte artikler i DORA-forordningen, der strafbelægges med den foreslåede bestemmelse. Når der nedenfor henvises til finansielle enheder, menes der et skibsfinansieringsinstitut.

Artikel 5 indeholder regler om forvaltning og organisationen af en finansiel enheds it-risikostyring. Intern forvaltning og organisation af it-risikostyring omfatter fastlæggelsen og tilsynet af de foranstaltninger for it-risikostyring. En sikker forvaltning af risikostyringen sikrer et højt niveau af digital operationel modstandsdygtighed og bidrager til en finansielle stabilitet.

I medfør af artikel 5, stk. 1, skal en finansiel enhed have indført en intern forvaltnings og kontrolramme, der sikrer en effektiv og forsigtig styring af it-risiko, i overensstemmelse med artikel 6, stk. 4. Artikel 6, stk. 4, der bl.a. fastsætter krav om, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau for at undgå interessekonflikter mellem den finansielle enhed og kontrolfunktionen.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har overdraget ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion, der har et passende uafhængighedsniveau i forhold til den finansielle enhed.

Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1. Artikel 6, stk. 1, vedrører at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. De nærmere krav til ledelsesorganet er nærmere beskrevet i artikel 5, stk. 2, litra a-i. Det fremgår bl.a. af stk. 2, litra b, at ledelsesorganet skal indføre politikker, der har en formål at sikre høje standarder for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data. Videre fremgår det af stk. 2, litra f, at ledelsesorganet godkender og regelmæssigt gennemgår den finansielle enheds interne it-revisionsplaner, it-revisioner og væsentlige ændringer heraf.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 2, er den finansielle enhed. En strafbar handling kan eksempelvis være, at et ledelsesorgan ikke har indført politikker for tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i henhold til stk. 2, litra b. En strafbar handling kan også være at ledelsesorganet enten ikke har godkendt eller gennemgået den finansielle enheds interne it-revisionsplan i henhold til stk. 2, litra f.

Artikel 5, stk. 3, fastsætter at finansielle enheder skal oprette en funktion med henblik på overvågning af de ordninger, der er indgået med

tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester, eller udpege et medlem af den øverste ledelse som tilsynsansvarlig for den dermed forbundne risikoeksponering og relevante dokumentation.

Ansvarssubjektet for overtrædelse af artikel 5, stk. 3, er den finansielle enhed. Et eksempel på en strafbar handling kan være, at ledelsesorganet ikke har oprettet en funktion der har til formål at overvåge de ordninger, der er indgået med tredjepartsudbydere af it-tjenester vedrørende brugen af it-tjenester.

Artikel 6 indeholder regler om en finansiel enheds ramme for it-risikostyring. Rammen for it-risikostyring omfatter hvilke tiltag en operatør af et reguleret marked har opsat.

I medfør af artikel 6, stk. 1, skal en finansiel enhed have indført en robust, omfattende og veldokumenteret ramme for deres it-risikostyring, som en del af deres samlede risikostyringssystem der sikrer et højt niveau af digital operationel modstandsdygtighed.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 1, er den finansielle enhed.

Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har formået at dokumentere deres ramme for deres it-risikostyring i en tilstrækkelig grad.

Det fremgår af artikel 6, stk. 2, at rammen for it-risikostyring, som minimum skal omfatte strategier, politikker, procedurer, it-protokoller og værktøjer, som er nødvendige for på behørig vis og i tilstrækkelig grad, at beskytte alle informationsaktiver og it-aktiver.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 2, er ledelsesorganet. Det fremgår af artikel 5. stk. 2, at ledelsesorganet i den finansielle enhed skal fastlægge, godkende og føre tilsyn med og har ansvaret for gennemførelsen af alle ordninger vedrørende rammer for it-risikostyring, der er omhandlet i artikel 6, stk. 1.

Den strafbare handling kan eksempelvis bestå i, at ledelsesorganet ikke har indført sikkerhedsforanstaltninger der i tilstrækkeliggrad beskytter relevante fysiske komponenter, som eksempelvis virksomhedens lokaler, mod uautoriseret adgang.

Artikel 6, stk. 3, omhandler de finansielle enheders forpligtigelse til at forelægge fuldstændige og ajourførte oplysninger om deres it-risiko på de

kompetente myndigheders anmodning. Ved at indføre passende strategier, politikker, procedurer, it-protokoller og -værktøjer, minimerer den finansielle enhed deres it-risiko.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 3, er den finansielle enhed. Et eksempel på den strafbare handling kan være, at den finansielle enhed ikke på Finanstilsynets anmodning, har fremlagt en opdateret strategi for deres it-risikostyring, efter nye tiltag trådte i kraft for virksomheden.

Det fremgår af artikel 6, stk. 4, at finansielle enheder skal overdrage ansvaret for styring af og tilsyn med it-risikoen til en kontrolfunktion og sikre, at denne kontrolfunktion har et passende uafhængighedsniveau, så interessekonflikter kan undgås. Videre fremgår det af artikel 6, stk. 4, 2. pkt., at en finansiel enhed skal sikre en passende adskillelse og uafhængighed af it-risikostyringsfunktioner, kontrolfunktioner og interne revisionsfunktioner efter modellen med tre forsvarslinjer eller en intern model for risikostyring og kontrol.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af bestemmelsen kan eksempelvis bestå i, at en finansiel enhed har en intern styring af og tilsyn med it-risikoen og derfor ikke har sikret en passende adskillelse og uafhængighed af deres it-risikostyringsfunktioner.

Artikel 6, stk. 5, indeholder krav om dokumentationen og tilsyn med it-risikostyringens ramme. Det følger af bestemmelsen, at rammen for it-risikostyringen skal dokumenteres og gennemgås mindst én gang om året, samt når der forekommer større it-relaterede hændelser, og i henhold til tilsynsmæssige instrukser eller konklusioner, som er udledt af relevant test af digital operationel modstandsdygtighed eller revisionsprocesser. Den skal forbedres løbende på grundlag af indhøstede gennemførelses- og overvågningserfaringer. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dens anmodning.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 5, er den finansielle virksomhed. Den strafbare handling kan eksempelvis bestå i, at en finansiel enhed ved en større it-relateret hændelse, efterfølgende ikke formår at dokumentere rammen for risikostyringen. En strafbar handling kunne også bestå i, at den finansielle enhed ikke har forbedret rammen for deres risikostyring på baggrund af løbende overvågningserfaringer.

Artikel 6, stk. 6, omhandler revisorernes interne revision af rammen for it-risikostyring. Det følger af bestemmelsen, at revisorerne skal besidde egenskaber som tilstrækkelig viden, faglig kompetence og ekspertise, samt

være tilstrækkeligt uafhængige. Der skal være overensstemmelse mellem hyppigheden af revisioner og omfanget af it-risikoen hos den finansielle enhed.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan eksempelvis bestå i, at den finansielle enheds revisor har foretaget en revision af rammen for it-risikostyring, uden at have det fornødne egenskaber. Det kan ligeledes anses for strafbart såfremt revisoren ikke kan anses som værende uafhængig.

Artikel 6, stk. 7, omhandler den formelle opfølgningsproces på den interne revisionsgang som den finansielle enhed skal etablere. Opfølgningsprocessen skal indeholde regler for rettidig efterprøvning og udbedring af kritiske resultater af it-revisioner.

Ansvarssubjektet for overtrædelse af artikel 6, stk. 7, er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke etablerer en opfølgningsproces, der indeholder regler for rettidig efterprøvning af kritiske konklusionerne fra en interne revision.

I medfør af artikel 6, stk. 8, skal en finansiel enheds ramme for it-risikostyring omfatte en strategi for digital operationel modstandsdygtighed, der fastsætter, hvordan rammen gennemføres. Strategien for digital operationel modstandsdygtighed skal omfatte metoderne til håndtering af it-risiko og opfylde specifikke krav, som er oplistet i artikel 6, stk. 8, litra a-h. Et af disse krav er eksempelvis at fastlægge risikotoleranceniveauet for it-risiko i overensstemmelse med den finansielle enheds risikovillighed og analysere tolerancen over for virkninger af it-forstyrrelser, jf. litra b, eller dokumentere den nuværende situation for den digitale operationelle modstandsdygtighed på grundlag af antallet af indberettede større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet, jf. litra f.

Ansvarssubjektet for en overtrædelse af artikel 6, stk. 8, er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enheds strategi, undlader at analysere for virkninger af it-forstyrrelser over for risikotoleranceniveauet. Den strafbare handling kan ligeledes bestå i, at den finansielle enhed ikke formår at dokumentere deres situation for den operationelle robusthed på baggrund af mængden af større it-relaterede hændelser og de forebyggende foranstaltningers effektivitet

Artikel 7, stk. 1, oplister en række krav til den finansielle enheds it-systemer, -protokoller og-værktøjer, jf. litra a-d. Den finansielle enhed skal eksempelvis anvende systemer der er pålidelige, jf. litra b, og som er

teknologisk modstandsdygtige nok til i tilstrækkeligt omfang at håndtere yderligere behov for informationsbehandling som krævet under stressede markedsforhold eller i andre vanskelige situationer, jf. litra d.

Ansvarssubjektet for overtrædelse af bestemmelsen er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke anvender systemer eller værktøjer der pålidelige eller proportionale i forhold til den finansielle enheds udbudte ydelser.

Artikel 8, stk. 1-7, i DORA-forordningen omhandler identifikation af kilder til it-risiko. Artikel 8, stk. 1, fastsætter, at en finansiel enhed, som led i deres ramme for it-risikostyring, skal foretage identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttede forretningsfunktioner, roller og ansvarsområder, informationsaktiver og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici. Bestemmelsen fastsætter endvidere, at en finansiel virksomhed efter behov og mindst én gang om året, vurderer hvorvidt denne klassificering og eventuel relevant dokumentation er tilstrækkelig.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke har identificeret, klassificeret eller dokumenteret deres it-understøttede forretningsfunktioner i en tilstrækkelig grad.

I medfør af artikel 8, stk. 2, skal en finansiel enhed løbende identificere alle kilder til it-risiko, navnlig risikoeksponeringen for og fra andre finansielle enheder, og vurderer cybertrusler og it-sårbarheder, der er relevante for deres it-understøttede forretningsfunktioner, informationsaktiver og it-aktiver. De finansielle enheder skal derfor regelmæssigt og mindst én gang om året gennemgå de risikoscenarier, der har virkninger for dem.

Ansvarssubjektet for overtrædelse af artikel 8, stk. 2, er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel virksomhed ikke mindst én gang årligt har gennemgået de risikoscenarier der er virkninger for dem.

Artikel 8, stk. 3, indeholder krav om, at en finansiel enhed skal foretage en risikovurdering efter hver større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker deres it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan bestå i, at en finansiel enhed har foretaget en større ændring infrastrukturen i deres net- og informationssystem og ikke

foretager en ny risikovurdering, såfremt infrastrukturen påvirker deres it-understøttede forretningsfunktioner.

Det fremgår af artikel 8, stk. 4, at en finansiel enhed skal identificere alle informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr, og kortlægger dem, der anses for kritiske. Den finansielle enhed kortlægger informationsaktivernes og it-aktivernes konfiguration samt forbindelserne og den indbyrdes forbundethed mellem de forskellige informationsaktiver og it-aktiver.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har kortlagt de kritiske informationsaktiver og it-aktiver, herunder på eksterne steder, netværksressourcer og hardwareudstyr.

Artikel 8, stk. 5, fremgår det, at en finansiel enhed skal identificere og dokumentere alle processer, der er afhængige af tredjepartsudbydere af it-tjenester. Det fremgår endvidere, at den finansielle enhed identificerer sammenkoblinger med tredjepartsudbydere af it-tjenester, der udbyder tjenester, som understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed har undladt at dokumentere alle de processer der er afhængige af tredjepartsudbydere af it-tjenester, som den finansielle enhed bruger.

Det fremgår af artikel 8, stk. 6, at den finansielle enhed, med henblik på artikel 6, stk. 1, 4 og 5, opretholder relevante fortegnelser og ajourfører dem regelmæssigt, og hver gang der sker større ændringer som omhandlet i artikel 6, stk. 3.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse kan bestå i, at der ved en større ændring af infrastrukturen i net- og informationssystemerne, i de processer eller procedurer, der påvirker den finansielle enheds it-understøttede forretningsfunktioner, informationsaktiver eller it-aktiver, ikke er foretaget ajourførte fortegnelser over ændringerne.

Til sidst følger det af artikel 8, stk. 7, skal en finansiel enhed foretage en specifik it-risikovurdering regelmæssigt og mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse består eksempelvis i, at en finansiel virksomhed ikke regelmæssigt eller mindst én gang årligt har foretaget en specifik it-risikovurdering.

Artikel 9 indeholder nærmere bestemmelser om beskyttelse af it-systemer og forebyggelse af it-risici.

Det følger af artikel 9, stk. 1, at en finansiel enhed skal sikre løbende overvågning af og kontrol med it-systemer og -værktøjernes sikkerhed og af, hvordan de fungerer, og minimerer virkningerne af it-risikoen for it-systemer ved at indføre passende it-sikkerhedsværktøjer, -politikker og -procedurer, med henblik på, at sikre en passende beskyttelse og tilrettelægge indsatsforanstaltninger der skal sikre de finansielle enheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke løbende at overvåge og kontrollere den finansielle enheds it-systemer og -værktøjers sikkerhed igennem passende it-sikkerhedsværktøjer, -politikker og -procedurer.

I medfør af artikel 9, stk. 2, skal en finansiel enhed udforme, indkøbe og gennemføre it-sikkerhedspolitikker, -procedurer, -protokoller og -værktøjer, der har til formål at sikre it-systemernes modstandsdygtighed, stabilitet og tilgængelighed, især for dem, der understøtter kritiske eller vigtige funktioner, og at opretholde høje standarder for, tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten dataene er inaktive, i brug eller under overførsel.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 2, bestå i, at der ikke er gennemført en it-sikkerhedspolitik for at sikre den finansielle enheds it-systems modstandsdygtighed, stabilitet og tilgængelighed.

Artikel 9, stk. 3, omhandler de it-løsninger og it-processer som den finansielle enhed skal anvende for at nå de i artikel 9, stk. 2, omhandlede mål. It-løsningerne og it-processerne skal være i overensstemmelse med proportionalitetsprincippet i artikel 4 i DORA-forordningen og sikre sikkerheden for metoderne til overførsel af data, minimere risikoen for korruption eller tab af data, uautoriseret adgang og tekniske fejl, der kan hæmme erhvervsaktiviteten og forhindrer manglen på tilgængelighed, forringelsen af autenticiteten og integriteten, bruddene på fortroligheden og tabet af data. Samt sikre, at data beskyttes mod risici, der opstår i forbindelse med dataforvaltning, herunder dårlig administration, procesrelaterede risici og menneskelige fejl.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 9, stk. 3, bestå i at have utilstrækkelige it-løsninger og it-

processer, der ikke lever op til proportionalitetsprincippet i artikel 4, i DORA-forordningen og de i artikel 9, stk. 3, fastsatte krav.

Det følger af artikel 9, stk. 4, at en finansiel enhed som led i deres it-risikostyring skal udvikle og dokumentere en informationspolitik, der fastlægger regler for beskyttelse af tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, informationsaktiver og it-aktiver, herunder deres kunders, hvis det er relevant, jf. litra a. Desuden skal en finansiel enhed følge en risikobaseret tilgang ved at indføre en forsvarlig forvaltningsstruktur for netværk og infrastrukturer ved anvendelse af passende teknikker, metoder og protokoller, der kan omfatte gennemførelse af automatiske mekanismer til isolering af de berørte informationsaktiver i tilfælde af cyberangreb, jf. litra b. Artikel 9, stk. 4, litra c, fastsætter også at en finansiel enhed skal gennemføre politikker, der begrænser den fysiske eller logiske adgang til informationsaktiver og it-aktiver udelukkende til, hvad der er påkrævet for legitime og godkendte funktioner og aktiviteter, og med henblik herpå indføre en række politikker, procedurer og kontroller, der vedrører adgangsrettigheder og sikrer forsvarlig forvaltning heraf.

Desuden skal den finansielle enhed gennemføre politikker og protokoller for stærke autentificeringsmekanismer på grundlag af relevante standarder og særlige kontrolsystemer og beskyttelsesforanstaltninger for krypteringsnøgler, hvorigennem data krypteres baseret på resultaterne fra godkendt dataklassificering og godkendte it-risikovurderingsprocesser, jf. litra d. Samt gennemføre dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, jf. litra e. Slutteligt anfører artikel 9, stk. 4, litra f, at en finansiel enhed skal sørge for, at der indføres passende og omfattende dokumenterede politikker for programrettelser og opdateringer.

Med henblik på første afsnit, litra b, udformer de finansielle enheder infrastrukturen for netværkstilslutning på en sådan måde, at den kan afbrydes eller segmenteres øjeblikkeligt for at minimere og forhindre afsmitning, navnlig i forbindelse med indbyrdes forbundne finansielle processer. Med henblik på første afsnit, litra e, skal it-ændringsstyringsprocessen godkendes på passende ledelsesniveauer og omfatte specifikke protokoller.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke forelægger en tilstrækkelig it-sikkerhedspolitik hos den finansielle enhed til at sikre beskyttelsen af deres kunders data. Den strafbare handling kan desuden også bestå i, at dokumenterede politikker, procedurer og kontroller for styring af it-ændringer, herunder ændringer af software, hardware, firmwarekomponenter, systemer eller sikkerhedsparametre, som er baseret på en risikovurderingstilgang og er en integreret del af den finansielle enheds samlede ændringsstyringsproces, for at sikre, at alle ændringer af it-systemer registreres, testes, vurderes, godkendes, gennemføres og efterprøves på en kontrolleret måde, ikke er blevet godkendt på passende ledelsesniveau.

Artikel 10, stk. 1-4, i DORA-forordningen omhandler detektion af anormale aktiviteter.

Det følger af artikel 10, stk. 1, at en finansiel enhed skal indføre mekanismer til omgående detektion af anormale aktiviteter i overensstemmelse med artikel 17, herunder problemer med it-netværkets ydeevne og it-relaterede hændelser, og til identifikation af potentielt væsentlige single points of failure. Artikel 17 omhandler proces for styring af it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. En overtrædelse af artikel 10, stk. 1, kan bestå i at der i den finansielle enhed ikke bliver opdaget anormale aktiviteter, idet enheden ikke har indført en mekaniske til detektion af disse.

Artikel 10, stk. 2, fastsætter krav til den finansielle enheds mekanismer. I medfør af artikel 10, stk. 2, skal de omtalte mekanismer i stk. 1, anvende flere kontrollag, fastlægge varslingstærskler og -kriterier, som skal udløse og igangsætte indsatsforanstaltninger mod it-relaterede hændelser, herunder automatiske varslingsmekanismer for det relevante personale, som har ansvar for indsatsen mod it-relaterede hændelser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i at have utilstrækkelige mekanismer der ikke lever op til de af artikel 10, stk. 2, fastsatte krav.

Videre fremgår det af artikel 10, stk. 3, at finansielle enheder skal afsætte tilstrækkelige ressourcer og kapaciteter til overvågning af brugeraktiviteter, forekomsten af it-anomalier og it-relaterede hændelser, navnlig cyberangreb.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, ikke at have afsat ressourcer til overvågning af brugeraktiviteter.

Til slut fremgår det af artikel 10, stk. 4, at udbydere af dataindberetningstjenester indfører desuden systemer, som effektivt kan kontrollere, om handelsindberetningerne er fuldstændige, identificere udeladelser og åbenbare fejl og anmode om fornyet fremsendelse af disse indberetninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ikke er indført et system som kan identificere åbenbare fejl.

Artikel 11 i DORA-forordningen omhandler indsats og genopretning at it. Artikel 11, stk. 1, fastsætter, at en finansiel enhed skal indføre en omfattende politik for it-driftsstabilitet. Politikken skal være baseret på de krav til identifikation, der er fastsat i artikel 8 i DORA-forordningen. I henhold til artikel 8, stk. 1, skal en finansiel enhed f.eks. foretage en identifikation, klassificering og tilstrækkelig dokumentering af alle it-understøttende forretningsfunktioner, roller, ansvarsområder, informationsaktiviteter og it-aktiver, der understøtter disse funktioner, samt deres roller og afhængigheder med hensyn til it-risici.

Ansvarssubjektet for overtrædelse af artikel 11, stk. 1, er den finansielle enhed. Den strafbare handling kan enten bestå i ikke at have indført nogen politik for it-driftsstabilitet, eller at have indført en politik, der ikke omhandler alle it-understøttende forretningsfunktioner.

I medfør af artikel 11, stk. 2, skal en finansiel enhed gennemføre politikken for it-driftsstabilitet ved hjælp af særlige veldokumenterede ordninger, planer, procedurer og mekanismer, der skal tage sigte på en række forhold, der er oplistet i stk. 2, litra a - e. En af disse forhold er eksempelvis at sikre, at en finansiel enheds kritiske eller vigtige funktioner er stabile, jf. litra a, eller omgående at aktivere særlige planer, der gør det muligt at avende inddæmningsforanstaltninger, -processer og -teknologier, der er egnede til de enkelte typer af it-relaterede hændelser, og som forhindrer yderligere skade, jf. litra c.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført en politik for it-driftsstabilitet ved hjælp af særlige ordninger, planer, procedurer og mekanismer, der tager sigte på de forhold, der er oplistet i stk. 2, litra a – e.

Artikel 11, stk. 3, indeholder krav om, at en finansiel enhed skal gennemføre planer for it-indsats og -genopretning, som skal underkastes uafhængige interne revisionsgennemgange.

Ansvarssubjektet for en overtrædelse af stk. 3, er den finansielle enhed. Den strafbare handling består i at en finansiel enhed ikke lader planer for it-indsats og -genopretning blive underkastet uafhængige interne revisionsgennemgange.

Det fremgår af artikel 11, stk. 4, at en finansiel enhed skal indføre, vedligeholde og foretage regelmæssig testning af passende planer for it-driftsstabilitet, navnlig med hensyn til kritiske eller vigtige funktioner, som outsources eller udliciteres gennem ordninger, der er indgået med tredjepartsudbydere af it-tjenester. Ved regelmæssig testning forstås mindst én gang om året, jf. artikel 11, stk. 6, litra a.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at vedligeholde planer for it-driftsstabilitet, f.eks. hvis en udskiftning af virksomhedens it-systemer nødvendiggør en opdatering af planerne for it-driftsstyring. En strafbar handling kan også bestå i ikke regelmæssigt at foretage en test af planer for it-driftsstabilitet. Herunder vil det være en særligt skærpende omstændighed, hvis der ikke er foretaget regelmæssig testning af planer for it-driftsstabilitet med hensyn til kritiske eller vigtige funktioner, som eksempelvis er outsourcet til en tredjepartsudbyder af it-tjenester.

Af artikel 11, stk. 5, 1. pkt., fremgår det, at en finansiel enhed som led i den samlede politik for driftsstabilitet skal foretage en forretningskonsekvensanalyse af deres eksponering for alvorlige driftsforstyrrelser. Det fremgår videre af stk. 5, 2. pkt., hvordan en finansiel enhed i konsekvensanalysen skal vurdere potentielle virkninger af alvorlige driftsforstyrrelser. I stk. 5, 3. pkt., fremgår det, at en konsekvensanalyse bl.a. skal tage hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner og andre forhold, der er nævnt i 3. pkt. Til sidst fremgår det af stk. 5, 4. pkt., at en finansiel enhed skal sikre, at it- aktiver og -tjenester udformes og anvendes i fuld overensstemmelse konsekvensanalysen, navnlig med hensyn til tilstrækkeligt at sikre alle kritiske komponenters redundans, dvs. at en kritisk komponent kan erstattes med en tilsvarende komponent, hvis det skulle blive nødvendigt.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå af ikke at foretage en forretningskonsekvensanalyse af enhedens eksponering for alvorlige driftsforstyrrelser. Den kan f.eks. også bestå i ikke at foretage en vurdering af alvorlige driftsforstyrrelser i

overensstemmelse med stk. 5, 2. pkt., eller bestå i at konsekvensanalysen ikke tager hensyn til den kritiske betydning af identificerede og kortlagte forretningsfunktioner eller en af de andre forhold, der er nævnt i det pågældende punkt. Til sidst kan en strafbar handling bestå i f.eks. ikke at sikre, at en kritisk komponent kan erstattes af en tilsvarende komponent, hvis konsekvensanalysen tilsiger dette.

Det fremgår af artikel 11, stk. 6, 1. afsnit, litra a, at en finansiel enhed som led i it-risikostyring skal teste enhedens planer for it-driftsstabilitet og planer for it-indsats og genopretning i forbindelse med it-systemer, der understøtter alle funktioner. En test heraf skal finde sted mindst én gang årligt og i tilfælde af væsentlige ændringer af it-systemer, der understøtter kritiske eller vigtige funktioner. I medfør af stk. 6, 1. afsnit, litra b, skal en finansiel enhed også teste krisekommunikationsplaner, der er udarbejdet i medfør af artikel 14.

Stk. 6, 2. afsnit indeholder nærmere krav til, hvilke forskellige scenarier tests for it-driftsstabilitet og planer for it-indsats og genopretning, jf. stk. 6, litra a, skal medtage. Det drejer sig bl.a. om cyberangrebsscenarier og omstillingsscenarier mellem den primære it-infrastruktur og redundante kapacitet. Ved redundante kapacitet forstås en lignende kapacitet, der skal kunne erstattet den primære it-infrastruktur, hvis denne eksempelvis bliver beskadiget under et cyberangreb. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Videre fremgår det af stk. 6, 3. afsnit, at en finansiel enhed regelmæssigt skal gennemgå sin politik for it-driftsstabilitet og planer for it-indsats og -genopretning. Her skal den finansielle enhed bl.a. tage hensyn til resultaterne af de test, som den finansielle enhed har gennemført i henhold til 1. afsnit.

Ansvarssubjektet for en overtrædelse af artikel 11, stk. 6, er den finansielle enhed. Den strafbare overtrædelse kan eksempelvis bestå i ikke at foretage test for planer for it-driftsstabilitet og planer for it-indsats og -genopretning eller ikke at foretage test af krisekommunikationsplaner, jf. stk. 6, 1. afsnit.

En strafbar overtrædelse kan f.eks. også bestå af ikke at ikke at medtage cyberangrebscenarier og omstillingsscenarier mellem den primære it-infrastruktur og den redundante kapacitet, eller i ikke regelmæssigt at gennemgå enhedens politik for it-driftsstabilitet og planer for it-indsats og -

genopretning under hensyntagen til resultaterne af de test, som enheden har gennemført, jf. henholdsvis 2. og 3. afsnit.

I medfør af artikel 11, stk. 7, skal en finansiel enhed have en krisestyringsfunktion, som, hvis deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres, bl.a. skal indeholde klare procedure for forvaltning af intern og ekstern krisekommunikation i overensstemmelse med artikel 14, der indeholder nærmere regler herfor.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at have en krisestyringsfunktion, der indeholder klare procedure for intern og ekstern krisekommunikation i overensstemmelse med artikel 14.

Artikel 11, stk. 8, indeholder krav om, at en finansiel enhed skal føre let tilgængelige registre over aktiviteter før og under driftsforstyrrelser, når deres planer for it-driftsstabilitet og planer for it-indsats og -genopretning aktiveres.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at føre registre over aktiviteter før og under driftsforstyrrelser, hvor planerne for it-driftsstabilitet og for it-indsats og -genopretning er blevet aktiveret.

Til sidst følger det af artikel 11, stk. 10, at en finansiel enhed skal indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder på deres anmodning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at indberette et overslag over de samlede årlige omkostninger og tab, der opstår som følge af større it-relaterede hændelser, til de kompetente myndigheder, dvs. Finanstilsynet, hvis Finanstilsynet anmoder den finansielle enhed herom.

Artikel 12 indeholder nærmere bestemmelser om politikker og procedurer for sikkerhedskopiering og procedure og metoder for gendannelse og genopretning af it-systemer og data.

Det følger af artikel 12, stk. 1, at en finansiel enhed som led i it-risikostyring skal udvikle og dokumentere politikker og procedure for sikkerhedskopiering, der præciserer omfanget af de data, der er genstand for sikkerhedskopiering, og minimumshyppigheden af sikkerhedskopiering baseret på oplysningernes kritiske betydning eller fortrolighedsniveauet for

dataene. Desuden skal en finansiel enhed udvikle og dokumentere procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består af ikke at udvikle og dokumentere politikker og procedure for enten sikkerhedskopiering eller gendannelse og genopretning.

I medfør af artikel 12, stk. 2, 1. pkt., skal en finansiel enhed etablere systemer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning. Det føler videre af artikel 12, stk. 2, 2. pkt., at aktiveringen af systemerne for sikkerhedskopiering ikke må sætte sikkerheden i net- og informationssystemer eller tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data over styr. Til sidst er det i medfør af stk. 2, 3. pkt., et krav, at der foretages regelmæssig test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan eksempelvis bestå i ikke at etablere systemer for sikkerhedskopiering eller for procedurer og metoder for gendannelse og genopretning. Den kan også bestå i at en finansiel enhed ikke sikrer sig, at systemerne for sikkerhedskopiering ikke sætter sikkerheden i net- og informationssystemer mv. over styr. I henhold til stk. 2, 3. pkt., kan den bestå i at der ikke foretages regelmæssige test af procedurer for sikkerhedskopiering og procedurer og metoder for gendannelse og genopretning.

Det følger af artikel 12, stk. 3, 1 og 2. pkt., at når en finansiel enhed gendanner sikkerhedskopierede data ved anvendelse af egne systemer, skal de anvende de it-systemer, der er fysisk og logisk adskilt fra it-kildesystemet. It-systemerne skal være sikkert beskyttet mod uautoriseret adgang eller it-korruption og give mulighed for rettidig gendannelse af tjenester ved hjælp af data- og systemsikkerhedskopier efter behov.

Ansvarssubjektet i stk. 3, 1. og 2. pkt., er den finansielle enhed. Den strafbare handling kan i medfør af stk. 3, 1. pkt., bestå i at anvende egne it-systemer til gendannelse af sikkerhedskopierede data, der ikke er fysisk og logisk adskilt fra it-kildesystemet. Det vil eksempelvis sige it-systemer, der befinder sig på en anden adresse end kildesystemet, dvs. det it-system, som den finansielle enhed anvender i sit daglige virke. Det kan også være, hvor en finansiel enhed anvender eget it-system, der er fysisk adskilt fra kildesystemet, men hvor systemet ikke logisk er adskilt fra kildesystemet. Den strafbare handling i medfør af stk. 3, 2. pkt., kan f.eks. bestå i ikke at beskytte it-systemerne mod uautoriseret adgang eller it-korruption.

Videre følger det af stk. 3, 3. pkt., at for centrale modparter (CCP'er) skal genopretningsplaner gøre det muligt at genoptage alle transaktioner fra det tidspunkt, hvor de blev afbrudt, således at den berørte centrale modpart (CCP) kan opretholde driftssikkerheden og gennemføre afviklingen på den planlagte dato. Til sidst følger det af stk. 3, 4. pkt., at udbydere af dataindberetningstjenester desuden skal sørge for at råde over passende ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde deres tjenester.

Ansvarssubjektet i stk. 3, 3. pkt., er den centrale modpart (CCP). Den strafbare handling består i, at en genopretningsplan ikke gør det muligt at genoptage alle transaktioner fra det tidspunkt, hvor transaktionerne blev afbrudt.

Ansvarssubjektet i stk. 3, 4. pkt., er udbyderen af dataindberetningstjenester. Den strafbare handling består i ikke at have ressourcer og sikkerhedskopierings- og gendannelsesfaciliteter for til enhver tid at kunne udbyde og opretholde sine tjenester.

Det følger af artikel 12, stk. 4, 1. pkt., at en finansiel enhed opretholder redundante it-kapaciteter, der er udstyret med passende ressourcer og funktioner med henblik på at sikre forretningsmæssige behov. Videre fremgår det af stk. 4, 2. pkt., at mikrovirksomheder vurderer behovet for at opretholde redundante it-kapaciteter på grundlag af deres risikoprofil. Ved redundante it-kapaciteter forstås lignende it-kapaciteter, der skal kunne erstatte de primære it-kapaciteter en finansiel enhed, hvis disse it-kapaciteter eksempelvis bliver ramt af et cyberangreb.

Ansvarssubjektet i stk. 4, 1. pkt., er den finansielle enhed. Den strafbare handling består i ikke at have redundante it-kapaciteter, der sikrer forretningsmæssige behov.

Ansvarssubjektet i stk. 4, 2. pkt., er en finansiel enhed, som er en mikrovirksomheden. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Den strafbare handling består i ikke at have foretaget en vurdering af behovet for at opretholde redundante it-kapaciteter på baggrund af enhedens risikoprofil.

Af artikel 12, stk. 5, fremgår det, at værdipapircentraler (CSD'er) skal bibeholde mindst ét sekundært afviklingssted, der er udstyret med passende ressourcer, kapaciteter, funktioner og personalemæssige ordninger med henblik på at sikre forretningsmæssige behov. Stk. 5, 2. afsnit indeholder nærmere krav til det sekundære afviklingssted. Det fremgår bl.a. af stk. 5, 2. afsnit, litra a, at afviklingsstedet skal befinde sig i en geografisk afstand fra det primære afviklingssted for bl.a. at forhindre, at det påvirkes af den hændelse, der har berørt det primære afviklingssted. Et eksempel på en hændelse kan være en oversvømmelse på det primære afviklingssted. I sådan et tilfælde skal det sekundære afviklingssted ligge i en tilpas afstand fra det primære afviklingssted for ikke at tage skade af oversvømmelsen.

Ansvarssubjektet i stk. 5 er en værdipapircentral (CSD). Den strafbare handling består f.eks. i ikke at have som minimum ét sekundært afviklingssted. Den kan eksempelvis også bestå i ikke at have oprettet det sekundære afviklingssted i en afstand fra det primære afviklingssted, der sikrer, at en hændelse i det primære afviklingssted ikke også rammer det sekundære afviklingssted.

Det fremgår af artikel 12, stk. 6, 1. pkt., at når en finansiel enhed skal fastlægge målene for genopretningstid og genopretningstidspunkt for hver funktion, skal de tage hensyn til, om det er en kritisk eller vigtig funktion og de potentielle samlede virkninger for markedseffektiviteten. Videre fremgår det af stk. 6, 2. pkt., at tidsmålene skal sikre, at de aftalte serviceniveauer kan overholdes i ekstreme scenarier.

Ansvarssubjektet i stk. 6, er den finansielle enhed. Den strafbare handling består i, at en finansiel enhed i sin fastlæggelse af målene for genopretningstid og genopretningstidspunkt, ikke har taget hensyn til, om den pågældende funktion er kritisk, eller hvilken virkning disse tidsmål vil have på markedseffektiviteten. Den kan også bestå i, at den finansielle enhed ikke har sikret sig, at tidsmålene kan overholde de aftalte serviceniveauer i ekstreme scenarier.

Det fremgår af artikel 12, stk. 7, 1. pkt., at når en finansiel enhed foretager genopretning efter en it-relateret hændelse, skal den udføre de nødvendige kontroller, herunder eventuelt flere kontroller og afstemninger, for at sikre, at dataintegriteten bevares på højeste niveau. Videre fremgår det af stk. 7, 2. pkt., at kontroller også skal foretages i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Ansvarssubjektet i stk. 7 er den finansielle enhed. Den strafbare handling består i ikke at udføre de nødvendige kontroller eller afstemninger efter en

genopretning for at sikre, at dataintegriteten bevares på højt niveau. I den forbindelse kan den strafbare handling også bestå i ikke at foretage kontroller i forbindelse med rekonstruktionen af data fra eksterne interessenter for at sikre, at alle systemernes data er sammenhængende.

Artikel 13 indeholder regler om læring og udvikling omkring sårbarheder og cybertrusler, it-relaterede hændelser, herunder navnlig cyberangreb. Stk. 1 indeholder krav om, at en finansiel enhed skal sørge for at råde over kapaciteter og personale, som kan indsamle oplysninger herom, og som kan analysere de virkninger, de forventes at have på deres digitale operationelle modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at have afsat ressourcer til f.eks. et it-system og personale, hvormed enheden kan indsamle oplysninger om sårbarheder og cybertrusler eller it-relaterede hændelser som cyberangreb. Den strafbare handling kan eksempelvis også bestå i ikke at have personale med tilstrækkelige kompetencer til at kunne analysere de virkninger, som bl.a. et cyberangreb kan have på deres digitale operationelle infrastruktur.

Det fremgår af artikel 13, stk. 2, 1. afsnit, at en finansiel enhed skal foretage gennemgange af it-relaterede hændelser, efter at større it-relaterede hændelser har forstyrret deres kerneaktiviteter. Den finansielle enhed skal i den forbindelse analysere årsagerne til forstyrrelserne og identificere nødvendige forbedringer af it-operationerne eller indenfor rammerne af den i artikel 11 omhandlede politik for it-driftsstabilitet.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i ikke at foretage en gennemgang og analyse af en større it-relateret hændelse, der har forstyrret den finansielle enheds kerneaktivitet.

Videre fremgår det af stk. 2, 2. afsnit, at en finansiel enhed på anmodning fra den kompetente myndighed skal underrette den kompetente myndighed om ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser. Bestemmelsen gælder ikke for finansielle enheder, der er mikrovirksomheder. Ved mikrovirksomhed forstås en virksomhed, som beskæftiger under 10 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. euro, jf. artikel 2, stk. 3, i bilag til Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke efter anmodning fra Finanstilsynet at underrette Finanstilsynet om

ændringer, der er blevet gennemført efter en gennemgang af it-relaterede hændelser.

Til sidst fremgår det af stk. 2, 3. afsnit, at det i forbindelse med gennemgangen af it-relaterede hændelser skal fastslås, om de fastlagte procedurer er blevet fulgt, og om de iværksatte foranstaltninger har været effektive. Ved fastlagte procedurer forstås de procedurer, som den finansielle enhed har fastlagt i sin politik for it-driftsstabilitet. Det fremgår af artikel 11, stk. 2, at en finansiel enhed gennemfører politikken for it-driftsstabilitet ved hjælp af særlige, passende og veldokumenterede ordninger, planer, procedurer og mekanismer. Det er derfor procedurer og iværksatte foranstaltninger i henhold til de her ordninger mv., som den finansielle enhed skal fastslå om har været effektive.

Det fremgår nærmere af artikel 13, stk. 2, 3. afsnit, at hvad en finansiel enhed bl.a. skal lægge nærmere vægt på i sin vurdering af, om de iværksatte foranstaltninger har været effektive. Den finansielle enhed skal bl.a. lægge vægt på den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a. Det kan også være i forhold til effektiviteten af den finansielle enheds fejlafhjælpning i forbindelse med hændelser, jf. stk. 2, 3. afsnit, litra c.

Bestemmelsen har til formål at sikre, at en finansiel enhed efter en it-hændelse forholder sig kritisk til sine ordninger, planer, procedure mv. i forbindelse med sin politik for it-driftsstabilitet for evt. at kunne forbedre disse til håndtering af en fremtidig it-relateret hændelse.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at fastslå om ordninger, planer og procedure i forbindelse med politikken for it-driftsstabilitet er blevet fulgt. Den kan også bestå i ikke at fastslå, om de iværksatte foranstaltninger har været effektive, herunder eksempelvis i forhold til den hastighed, med hvilken der er blevet sat ind overfor sikkerhedsvarsler, og med hvilken hastighed virkningerne af it-relaterede hændelser og deres omfang er blevet fastslået, jf. stk. 2, 3. afsnit, litra a.

Det følger af artikel 13, stk. 3, 1. pkt., at erfaringer fra test af digital operationel modstandsdygtighed, som foretages i overensstemmelse med artikel 26 og 27, og fra faktiske it-relaterede hændelser, navnlig cyberangreb, samt udfordringer i forbindelse med aktiveringen af planer for it-driftsstabilitet og planer for it-indsats og -genopretning, sammen med relevante oplysninger, der udveksles med modparter, og som vurderes i

forbindelse med tilsynsmæssige gennemgange, løbende skal indarbejdes i it-risikovurderingsprocessen.

Artikel 26 vedrører avancerede test af IKT-værktøjer, -systemer og -processer baseret på TLPT. TLPT står for Threat Led Penetration Testing, som er en testmetode, hvor en virksomhed engagerer etiske hackere, som skal angribe flere systemer og det tilhørende cyberforsvar i virksomheden. Testene foregår i livesystemer, hvilket vil sige de systemer, som anvendes direkte i den finansielle sektor, og er baseret på konkrete trusler, hvilket betyder, at testene simulerer taktikker, teknikker og procedurer fra aktive, avancerede hackergrupper. Artikel 27 fastsætter de nærmere krav til testere.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke løbende at indarbejde erfaringer fra test af digital operationel modstandsdygtighed i overensstemmelse med artikel 26 og 27, og fra it-relaterede hændelser i it-risikostyringsprocessen.

Det fremgår af artikel 13, stk. 4, 1. pkt., at en finansiel enhed skal overvåge effektiviteten af gennemførelse af deres strategi for digital operationel modstandsdygtighed, jf. artikel 6, stk. 8, der fastsætter nærmere krav til strategien. Videre fremgår det af stk. 4, 2. pkt., at en finansiel enhed skal kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed. Den finansielle enhed skal gøre dette med henblik på at forstå graden af it-risikoeksponering, navnlig i forbindelse med kritiske eller vigtige funktioner, og for at forbedre den finansielle enheds cybermodenhed og cyberberedskab.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke at overvåge effektiviteten af gennemførelsen af enhedens strategi for digital operationel modstandsdygtighed eller i ikke at kortlægge it-risikoens udvikling over tid, analysere hyppigheden, typerne, omfanget af og udviklingen i it-relaterede hændelser, navnlig cyberangreb og mønstre forbundet hermed.

Det fremgår af artikel 13, stk. 5, at højtstående it-personale mindst én gang om året skal aflægge rapport til ledelsesorganet om de i stk. 3 omhandlede resultater og fremsætte anbefalinger. Indholdet af artikel 13, stk. 3, er nærmere gennemgået ovenfor under bemærkningerne til strafbelæggelsen af en overtrædelse af stk. 3.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i som finansiel enhed ikke at sørge for, at it-personale mindst én gang om året

aflægger rapport for ledelsesorganet om resultater af f.eks. faktiske it-relaterede hændelser, jf. artikel 13, stk. 3, og fremsætter anbefalinger.

Det fremgår af artikel 13, stk. 6, 1. pkt., at en finansiel enhed skal udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelsesordninger. Videre fremgår det af stk. 6, 2. pkt., at disse kurser skal omfatte alle medarbejdere og den øverste ledelse og skal have en grad af kompleksitet, der svarer til deres opgavers ansvarsområde. Sidst fremgår det af stk. 6, 3. pkt., at en finansiel enhed, hvis det er relevant, inddrager tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, jf. artikel 30, stk. 2, litra i, om kontraktlige ordninger om betingelserne for deltagelse af tredjepartsudbydere i programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består f.eks. i ikke at udvikle programmer til alle medarbejdere og den øverste ledelse til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed som obligatoriske moduler i deres personaleuddannelse. Den strafbare handling kan også bestå i ikke at inddrage tredjepartsudbydere af it-tjenester i relevante uddannelsesordninger, hvis dette viser sig nødvendigt. Det kan eksempelvis være i det tilfælde, hvor kompleksiteten af et uddannelsesprogram når et niveau, hvor den finansielle enhed ikke selv har kompetencerne til at udvikle programmet.

Det fremgår af artikel 13, stk. 7, 1. pkt., at en finansiel enhed løbende skal overvåge den relevante teknologiske udvikling også med henblik på at forstå den mulige virkning af indførelsen af sådanne nye teknologier for kravene til it-sikkerhed og digital operationel modstandsdygtighed. Videre fremgår det af stk. 7, 2. pkt., at en finansiel enhed skal holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb. Bestemmelsen gælder ikke for mikrovirksomheder. Se definitionen af en mikrovirksomhed under bemærkningerne til strafbelæggelse af overtrædelse af artikel 11, stk. 6, 2. afsnit.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i ikke løbende at overvåge den relevante teknologiske udvikling med henblik på evt. at indføre de nye teknologier i enheden i forhold til at leve op til kravene til it-sikkerhed og digital operationel modstandsdygtighed. Den kan også bestå i ikke at holde sig ajour med de seneste it-risikostyringsprocesser for effektivt at bekæmpe aktuelle eller nye former for cyberangreb.

Artikel 14, stk. 1 i DORA-forordningen omhandler, at der som led i den ramme for it-risiko-styring, der er omhandlet i artikel 6, stk. 1, at de finansielle enheder sørger for at have krisekommunikationsplaner, der giver mulighed for ansvarlig offentliggørelse af, som minimum større it-relaterede hændelser eller sårbarheder for kunder og modparter samt for offentligheden, alt efter hvad der er relevant.

Krisekommunikations-planer må forstås sådant, at når der opstår en større ulykke eller katastrofe, så er der et akut behov for viden, og det er derfor nødvendigt at have planer for at kommunikere dette ud til de relevante parter.

It-risiko-styring må forstås sådant, at det er en håndtering af en sådan trussel, som defineres i artikel 3, stk. 1 nr. 5.

Ansvarssubjektet for overtrædelse af artikel 14, stk. 1, er den finansielle enhed. Den strafbare handling kan f.eks. bestå i, at den finansielle enhed ikke har udarbejdet planer for kommunikation af en offentliggørelse af en større it-relateret hændelse.

I medfør af artikel 14, stk. 2, skal en finansiel enhed som led i rammen for i-risikostyring, der er omhandlet i artikel 6, stk. 1. gennemføre kommunikationsplaner for internt personale og eksterne interessenter. Artikel 6, stk. 1, vedrører, at finansielle enheder indfører en robust, omfattende og veldokumenteret ramme for it-risikostyring. Kommunikationspolitikkerne for personalet skal tage hensyn til behovet for at skelne mellem personale der er involveret i it-risiko-styring, navnlig det personale der er ansvarlig for indsats og genopretning, og personale, der skal underrettes.

Ansvarssubjektet for en overtrædelse af artikel 14, stk. 2, er den finansielle enhed. Den strafbare handling består i, ikke at have gennemført kommunikationsplaner for internt personale og eksterne interessenter.

Artikel 14, stk. 3, indeholder krav om, at mindst én person i den finansielle enhed skal have til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og til dette formål varetage funktionen vedrørende offentligheden og medierne.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har mindst én person, der har til opgave at gennemføre kommunikationsstrategien for it-relaterede hændelse, og som til dette formål har varetage funktionen vedrørende offentligheden og medierne.

Det fremgår af artikel 16, stk. 1, at forordningens artikel 5-15 ikke finder anvendelse på små og ikke indbyrdes forbundne investeringsselskaber, betalingsinstitutter, der er undtaget i henhold til direktiv (EU) 2015/2366, institutter, der er fritaget i henhold til direktiv 2013/36/EU, og for hvilke medlemsstaterne har besluttet ikke at anvende den mulighed, der er omhandlet i nærværende forordnings artikel 2, stk. 4, e-pengeinstitutter, der er undtaget i henhold til direktiv 2009/110/EF, og små arbejdsmarkedsrelaterede pensionskasser.

Uden at det berører første afsnit skal de i første afsnit omhandlede enheder overholde det anførte i artikel 16, stk. 1, litra a-e. Det fremgår af litra a, at enhederne skal indføre og vedligeholde en robust og dokumenteret ramme for it-risikostyring, der beskriver de mekanismer og foranstaltninger, der skal muliggøre en hurtig, effektiv og omfattende styring af it-risiko, herunder vedrørende beskyttelse af relevante fysiske komponenter og infrastrukturer.

Det fremgår af litra b, at der løbende skal overvåges alle it-systemers sikkerhed og drift.

Det fremgår af litra c, at virkningen af it-risiko gennem anvendelse af robuste, modstandsdygtige og ajourførte it-systemer, -protokoller og -værktøjer, som er egnede til at understøtte udførelsen af deres aktiviteter og leveringen af tjenester og i tilstrækkelig grad beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data i net- og informationssystemerne skal minimeres.

Det fremgår af litra d, at det skal hurtigt muligt skal konstateres og detekteres it-risikokilder og -anomalier i net- og informationssystemerne og hurtigt at håndtere it-relaterede hændelser.

Det fremgår af litra e, at der skal konstateres stor afhængighed af tredjepartsudbydere af it-tjenester.

Det fremgår af litra f, at der skal sikres kontinuiteten af kritiske eller vigtige funktioner gennem planer for driftsstabiliteten og indsats- og genopretningsforanstaltninger, der som minimum omfatter sikkerhedskopierings- og gendannelsesforanstaltninger.

Det fremgår af litra g, at der regelmæssigt skal testes de planer og foranstaltninger, der er omhandlet i litra f, samt effektiviteten af de gennemførte kontroller i overensstemmelse med litra a og c.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Det fremgår af litra h, at der skal gennemføres, alt efter hvad der er relevant, de relevante operationelle konklusioner, der følger af de test, der er omhandlet i litra g, og af de efterfølgende analyser af hændelserne, i it-risikovurderingsprocessen og efter behov og it-risikoprofil udvikle programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed for personale og ledelse.

Ansvarssubjektet i artikel 16, stk. 1 litra a-h, er den finansielle enhed. Den strafbare handling består i, at de i første afsnit omhandlede enheder ikke overholder det anførte i artikel 16, stk. 1, litra a-e.

I medfør af artikel 16, stk. 2, skal en finansiel enhed i den i stk. 1, andet afsnit, litra a, omhandlede ramme for it-risikostyring dokumenteres og gennemgås regelmæssigt og ved forekomst af større it-relaterede hændelser i overensstemmelse med de tilsynsmæssige instrukser. Den skal forbedres løbende på grundlag af indhøstede erfaringer fra gennemførelse og overvågning. Der skal forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed på dennes anmodning.

Ansvarssubjektet for overtrædelsen af artikel 16, stk. 2, er den finansielle enhed. Den strafbare handling består i, at ikke at have gennemført de handlinger der er oplistet i artikel 16, stk. 2. Dette er eksempelvis at sikre at der forelægges en rapport om gennemgangen af rammen for it-risikostyring for den kompetente myndighed ved anmodning.

Det fremgår af artikel 16, stk. 3, at ESA'erne via Det Fælles Udvalg og i samråd med ENISA fælles udarbejder udkast til reguleringsmæssige af tekniske standarder med henblik på det i litra a-e nævnte.

Det fremgår af litra a, at der yderligere skal præciseres de elementer, der skal indgå i rammen for it-risikostyring, som omhandlet i stk. 1, andet afsnit, litra a.

Det fremgår af litra b, at der yderligere ska præciseres de elementer, der for så vidt angår systemer, protokoller og værktøjer, som mindsker virkningerne af den it-risiko, der er omhandlet i stk. 1, andet afsnit, litra c, med henblik på at garantere netsikkerheden, sikre tilstrækkelige garantier

mod indtrængen og datamisbrug og bevare tilgængeligheden, autenticiteten, integriteten og fortroligheden af data.

Det fremgår af litra c, at der yderligere skal præciseres de komponenter, der er indeholdt i de planer for it-driftsstabilitet, der er omhandlet i stk. 1, andet afsnit, litra f.

Det fremgår af litra d, at der yderligere skal præcisere reglerne om test af planer for driftsstabiliteten og sikre effektiviteten af de kontrolforanstaltninger, der er omhandlet i stk. 1, andet afsnit, litra g, og sikre, at der ved en sådan test tages behørigt hensyn til de scenarier, hvor kvaliteten af leveringen af en kritisk eller vigtig funktion forringes til et uacceptabelt niveau eller mislykkes.

Det fremgår af litra e, at der yderligere skal præciseres indholdet og formatet af den rapport om gennemgangen af rammen for it-risikostyring, der er omhandlet i stk. 2.

Ansvarssubjektet i artikel 16, stk. 3, er den finansielle enhed. Den strafbare handling består i, ikke at overholde det anførte i artikel 16, stk. 3, litra a-e.

Det følger af artikel 17, stk. 1, at de finansielle enheder definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser for at detektere, styre og indberette it-relaterede hændelser.
Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 1 bestå i, at de finansielle enheder ikke definerer, fastlægger og gennemfører en proces for styring af it-relaterede hændelser, som kan detektere, styre og indberette it-relaterede hændelser.

Det følger af artikel 17, stk. 2, at de finansielle enheder er alle, der registrerer it-relaterede hændelser og væsentlige cybertrusler. De finansielle enheder fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Det skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser forekommer.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan i medfør af artikel 17, stk. 2, bestå i, at den finansielle enhed fastlægger passende procedurer og processer, der skal sikre en konsekvent og integreret overvågning, håndtering og opfølgning af it-relaterede hændelser. Dette skal ske således, at de grundlæggende årsager identificeres, dokumenteres og håndteres for at forhindre, at sådanne hændelser kan opstå.

Det følger af artikel 17, stk. 3, at den finansielle enhed som led i den proces for styring af it-relaterede hændelser, der er omhandlet i stk. 1, overholder det anførte i artikel 17, stk. 3, litra a-f.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling i medfør af artikel 17, stk. 3, er en tilsidesættelse af overholdelse af de oplistede krav i artikel 17, stk. 3, litra a-f. Dette kan eksempelvis være, at der ikke tildeles roller og ansvarsområder, som skal aktiveres for forskellige it-relaterede hændelsestyper og -scenarier.

Artikel 18 indeholder en klassificering af it-relaterede hændelser og cybertrusler.

Det følger af artikel 18, stk. 1, at de finansielle enheder klassificerer it-relaterede hændelser og fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af litra a, at antallet og/eller relevansen af kunder eller finansielle modparter, som er berørt, og, hvis det er relevant, beløbet på eller antallet af de transaktioner, som er berørt af den it-relaterede hændelse, og hvorvidt den it-relaterede hændelse har haft indvirkning på omdømmet.

Det fremgår af litra b, at varigheden af den it-relaterede hændelse, herunder tjenestens nedetid.

Det fremgår af litra c, at den geografiske udbredelse med hensyn til de områder, der er berørt af den it-relaterede hændelse, navnlig hvis den berører mere end to medlemsstater.

Det fremgår af litra d, at de datatab, som den it-relaterede hændelse medfører med hensyn til tilgængelighed, autenticitet, integritet eller fortrolighed af data.

Det fremgår af litra e, at den kritiske betydning af de berørte tjenester, herunder den finansielle enheds transaktioner og operationer.

Det fremgår af litra f, at de økonomiske virkninger, navnlig direkte og indirekte omkostninger og tab, af den it-relaterede hændelse i både absolutte og relative tal.

Ansvarssubjektet i stk. 1 er den finansielle enhed. Den strafbare består i, at de finansielle enheder ikke klassificerer it-relaterede hændelser og dermed ikke fastslår deres virkninger på grundlag af følgende kriterier oplistet i artikel 18, stk. 1, litra a-f.

Det fremgår af stk. 2, at de finansielle enheder klassificerer cybertrusler som væsentlige på grundlag af de udsatte tjenesters kritiske betydning, herunder den finansielle enheds transaktioner og operationer, antallet og/eller relevansen af de kunder eller finansielle modparter, som rammes, og risikoområdernes geografiske udbredelse.

Ansvarssubjektet i artikel 18, stk. 2, er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed undlader at klassificere cybertrusler som væsentlige, eksempelvis på grundlag af de udsattes tjenesters kritiske betydning.

Artikel 19, stk. 1, omhandler indberetning af større it-relaterede hændelser. Bestemmelsen forpligter den finansielle enhed til at indberette større it-relaterede hændelser til den relevante kompetente myndighed.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed ikke underretter Finanstilsynet om en større it-relateret hændelse.

I medfør af artikel 19, stk. 3, skal den finansielle enhed underrette Finanstilsynet, uden unødigt ophold, i tilfælde af, at en større it-relateret hændelse indtræffer og har indflydelse på kunders finansielle interesser. Den finansielle enhed underretter også om de foranstaltninger, der er truffet for at afbøde de negative virkninger af en sådan hændelse. I tilfælde af en væsentlig cybertrussel underretter de finansielle enheder, hvis det er relevant, de af deres kunder, som potentielt er berørt heraf, om eventuelle passende beskyttelsesforanstaltninger, som sidstnævnte kan overveje at træffe

Ansvarssubjektet var overtrædelse af artikel 19, stk. 3, er den finansielle enhed. En strafbar handling kan bestå i, at den finansielle enhed ikke underretter Finanstilsynet rettidigt i tilfælde en større it-relateret hændelse indtræffer, som har indflydelse på kunders finansielle interesser. En strafbar handling kan også bestå i at underrette Finanstilsynet om den it-relaterede hændelse, uden at underrette om de foranstaltninger der er truffet for at afbøde de negative virkninger.

Det fremgår af artikel 19, stk. 4, at den finansielle enhed, i tilfælde af en it-relateret hændelse, skal indgive henholdsvis en indledende underretning, jf. litra a, en foreløbig rapport så snart den oprindelige hændelses status har ændret sig betydeligt, eller håndteringen af den større it-relaterede hændelse har ændret sig på grundlag af nye tilgængelige oplysninger, efterfulgt, alt efter hvad der er relevant, af ajourførte underretninger, hver gang der

foreligger en relevant ajourføring af status, samt efter en specifik anmodning fra den kompetente myndighed, jf. litra b. Samt en endelig rapport, når den grundlæggende årsagsanalyse er afsluttet, uanset om der allerede er gennemført afbødende foranstaltninger, og når tallene for de faktiske virkninger foreligger og kan erstatte skøn, jf. litra c. Fristerne for disse skal fastsættes i overensstemmelse med artikel 20, stk. 1, litra a, nr. ii, og skal indgives til Finanstilsynet, som er den kompetente myndighed.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, ikke at indgive en indledende underretning, en foreløbig rapport eller en endelig rapport til Finanstilsynet inden for de af artikel 20, stk. 1, litra a, nr. ii, fastsatte frister.

Artikel 24 i DORA-forordningen omhandler generelle krav til gennemførslen af test af digital operationel modstandsdygtighed.

Det følger af artikel 24, stk. 1, at en finansiel enhed skal udarbejde, opretholde og gennemgå et forsvarligt og omfattende program for test af digital operationel modstandsdygtighed, som en integreret del af den i artikel 6 omhandlede ramme for it-risikostyring. Dette skal ske med henblik på at vurdere beredskabet i forhold til håndtering af it-relaterede hændelser, identificere svagheder, mangler og huller i den digitale operationelle modstandsdygtighed og straks træffe korrigerende foranstaltninger.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling kan eksempelvis bestå i, at den finansielle enhed ikke har udarbejdet et program for test af digital operationel modstandsdygtighed. Den strafbare handling kan også bestå i, at den finansielle enheds program for test af digital operationel modstandsdygtighed ikke er forsvarligt eller omfattende nok.
I medfør af artikel 24, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, omfatte en række vurderinger, test, metodologier, fremgangsmåder og værktøjer, der skal anvendes i overensstemmelse med artikel 25 og 26 i DORA-forordningen.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i at den finansielle enhed gennemfører tests der ikke i tilstrækkelig grad omfatter kravene om vurderinger, test, metodologier, fremgangsmåder og værktøj, der skal anvendes i overensstemmelse med artikel 25 og artikel 26 i DORA-forordningen.

Artikel 24, stk. 3, pålægger den finansielle enhed at følge en risikobaseret tilgang for programmet for test af digital operationel modstandsdygtighed. Den finansielle enhed skal ved gennemførslen af programmet, tage hensyn

til kriterierne i DORA-forordningens artikel 4, stk. 2, og til et it-risikomiljø i udvikling, eventuelle specifikke risici, som den berørte finansielle enhed udsættes for eller kan blive udsat for, informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre faktorer, som den finansielle enhed finder relevante.

Ansvarssubjektet er den finansielle enhed. En strafbar overtrædelse af artikel 24, stk. 3, kunne eksempelvis være, at den finansielle enhed gennemfører et program for test af digital operationel modstandsdygtighed uden at tage hensyn til den finansielles enheds it-risikomiljø.

I medfør af artikel 24, stk. 4, skal den finansielle enhed sikre, at tests gennemføres af uafhængige parter, hvad enten de er interne eller eksterne. Hvis en intern tester gennemfører test, skal de finansielle enheder afsætte tilstrækkelige ressourcer og sikre, at interessekonflikter undgås under testens udformnings- og gennemførelsesfaser.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed der gennemfører tests af deres digitale operationelle modstandsdygtighed ikke sikrer, at testen gennemføres af uafhængige interne eller eksterne parter for at begrænse interessekonflikter.

Artikel 24, stk. 5, pålægger den finansielle enhed at fastlægge procedurer og politikker med henblik på at prioritere, klassificere og afhjælpe alle problemer, der identificeres i forbindelse med gennemførelsen af test, og fastlægger interne valideringsmetoder for at sikre, at alle konstaterede svagheder, mangler eller huller afhjælpes fuldt ud.

Ansvarssubjektet er den finansielle enhed. En strafbare handling består af ikke at fastlægge procedurer og politikker der prioriterer, klassificerer og afhjælper de problemer der identificeres med gennemførslen af testen.

I medfør af artikel 24, stk. 6, skal de finansielle enheder sikre, at der gennemføres passende test af alle it-systemer og -applikationer, der understøtter kritiske eller vigtige funktioner, mindst én gang om året.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kunne bestå i at den finansielle enhed ikke mindst én gang årligt gennemfører tests af alle it-systemer og it-applikationer, der kan anses for passende.

Artikel 25 omhandler test af it-værktøjer og -systemer.

Det følger af artikel 25, stk. 1, at programmet for test af den digitale operationelle modstandsdygtighed skal være i overensstemmelse med de af

artikel 4, stk. 2, kriterier for proportionalitet. I medfør af artikel 4, stk. 2, skal den finansielle enheds styring, klassificering, indberetning af it-relaterede hændelser, test af digital operationel modstandsdygtighed og styring af it-tredjepartsrisici stå i et rimeligt forhold til deres størrelse og samlede risikoprofil og til karakteren, omfanget og kompleksiteten af deres tjenester, aktiviteter og operationer, som specifikt fastsat i de relevante regler i de nævnte kapitler.

I overensstemmelse med de oplistede kriterier i artikel 4, stk. 2, skal programmet for test af digital operationel modstandsdygtighed, nævnt i artikel 24, indeholde bestemmelser om gennemførelse af relevante test såsom sårbarhedsvurderinger og -scanninger, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, når det er praktisk muligt, scenariebaserede test, kompatibilitetstest, præstationstest, end-to-end-test og penetrationstest.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enhed har vedtaget et program for test der ikke er tilstrækkeligt, mangelfuldt eller lever op til de fastsatte krav for programmer for test af digital operationel modstandsdygtighed i artikel 25, stk. 1.

Artikel 25, stk. 2, omhandler værdipapircentraler og centrale modparter. I medfør af bestemmelsen skal værdipapircentraler og centrale modparter foretage sårbarhedsvurderinger inden indførelse eller genindførelse af nye eller eksisterende applikationer og infrastrukturkomponenter og it-tjenester, der understøtter den finansielle enheds kritiske eller vigtige funktioner.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå at en værdipapircentral ikke har foretaget en sårbarhedsvurdering såfremt de skal have nye applikationer, intrastrukturkompotenter og it-tjenester der understøtter den finansielle enheds kritiske eller vigtige funktioner.

I medfør af artikel 25, stk. 3, skal mikrovirksomheder gennemføre de i artikel 25, stk. 1 omhandlede test ved at kombinere en risikobaseret tilgang med strategisk planlægning af it-test under behørig hensyntagen til behovet for at opretholde en afbalanceret tilgang mellem omfanget af ressourcer og den tid, der skal afsættes til it-test som omhandlet i denne artikel, på den ene side og den hastende karakter, risikotype og informationsaktivernes og de leverede tjenesters kritiske betydning samt alle andre relevante faktorer, herunder den finansielle enheds evne til at tage kalkulerede risici, på den anden side.

Ansvarssubjektet er den finansielle enhed. En strafbar handling kan bestå i, at en mikrovirksomhed ikke har taget tilstrækkeligt hensyn til at opretholde en balanceret tilgang til henholdsvis omfanget af ressourcer og andre faktorer, som eksempelvis den finansielle enheds evne til at tage kalkulerede risici.

Artikel 28 omhandler generelle principper for forsvarlig styring af it-tredjepartsrisici.

I medfør af artikel 28, stk. 1, skal den finansielle enhed styre deres it-tredjepartsrisiko som en integreret del af it-risiko, inden for deres ramme for it-risikostyring.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består eksempelvis i, at den finansielle enheds it-tredjepartsrisiko ikke bliver styret som en integreret del af deres samlede it-risiko, inden for den finansielle enheds it-risikostyring.

I medfør af artikel 28, stk. 1, litra b, skal styringen af it-tredjepartsrisikoen hos den finansielle enhed foregå under hensyntagen til proportionalitetsprincippet og skal derfor tage hensyn til henholdsvis artikel 28, stk. 1, litra b, nr. i, som omhandler karakteren, omfanget, kompleksiteten og betydningen af den it-relaterede afhængighed og artikel 28, stk. 1, litra b, nr. ii, som omhandler de risici, der opstår som følge af kontraktlige ordninger for brugen af it-tjenester, der er indgået med tredjepartsudbydere af it-tjenester, under hensyntagen til den kritiske betydning eller vigtighed af den pågældende tjeneste, proces eller funktion og til de potentielle virkninger for driftsstabiliteten og tilgængeligheden af finansielle tjenesteydelser og aktiviteter på individuelt plan og koncernniveau.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at kravene i artikel 28, stk. 1, litra b, nr. i-ii, ikke tages under betragtning ved udformningen af den finansielle enheds styring af it-tredjepartsrisiko.

Artikel 28, stk. 2, omhandler strategien for den finansielle enheds it-tredjepartsrisiko. Den finansielle enhed skal vedtage og gennemgå deres strategi regelmæssigt som led i deres ramme for it-risikostyring. Strategien skal omfatte en politik for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og som leveres af tredjepartsudbydere af it-tjenester. Strategien skal gælde på individuelt grundlag og, hvor det er relevant, på delkonsolideret og konsolideret grundlag. Ledelsesorganet i den finansielle enhed skal på grundlag af en vurdering af den finansielle enheds samlede risikoprofil og omfanget og kompleksiteten af forretningstjenesterne regelmæssigt gennemgå de risici, der er konstateret i

forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i at ledelsesorganet i den finansielle enhed ikke ved vurderingen af den samlede risikoprofil har gennemgået de de risici, der er konstateret i forbindelse med kontraktlige ordninger for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner.

Artikel 28, stk. 3, fastsætter krav for den finansielle enheds dokumentation af kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere. Den finansielle enhed skal som et led i deres ramme for it-risikostyring sørge for at opretholde og ajourføre et register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere på både finansielle enhed på enhedsniveau, delkonsolideret niveau og konsolideret niveau. De kontraktsretlige ordninger skal være skelnet mellem de it-tjenester der understøtter kritiske eller vigtige funktioner, og dem, der ikke gør.

Desuden skal den finansielle enhed mindst én gang årligt indberette nye ordninger for brugen af it-tjenester, kategorierne af tredjepartsudbydere af IKT-tjenester, typen af kontraktlige ordninger og de it-tjenester og funktioner, der leveres, til Finanstilsynet.

Til sidst skal den finansielle enhed efter anmodning, stille det fulde register over oplysninger eller, som anmodet, nærmere angivne afsnit heraf til rådighed for Finanstilsynet sammen med eventuelle oplysninger, som anses for nødvendige for at muliggøre et effektivt tilsyn med den finansielle enhed. Den finansielle enhed underretter rettidigt Finanstilsynet om enhver planlagt kontraktlig ordning for brugen af it-tjenester, der understøtter kritiske eller vigtige funktioner, og når en funktion er blevet kritisk eller vigtig.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den finansielle enhed efter anmodning fra Finanstilsynet, ikke kan stille det fulde register over kontraktsretlige ordninger for brugen af it-tjenester der leveres af tredjepartsudøvere til rådighed.

Artikel 28, stk. 4, litra a-e, fastsætter krav til den finansielle enhed før der indgås en kontraktlig ordning for brugen af it-tjenester. Den finansielle enhed skal vurdere, om den kontraktlige ordning omfatter brugen af it-tjenester, der understøtter en kritisk eller vigtig funktion, jf. litra a, vurdere, om de tilsynsmæssige betingelser for udlicitering er opfyldt, jf. litra b, identificere og vurdere alle relevante risici i forbindelse med den

kontraktlige ordning, herunder muligheden for, at sådanne kontraktlige ordninger kan bidrage til at øge it-koncentrationsrisikoen, jf. artikel 29, jf. litra c, foretage fornøden due diligence over for potentielle tredjepartsudbydere af it-tjenester og under alle udvælgelses- og vurderingsprocesserne sikre, at den pågældende tredjepartsudbyder af it-tjenester er egnet jf. litra d, og identificere og vurdere interessekonflikter, som de kontraktlige ordninger kan give anledning til, jf. litra e.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i at den finansielle enhed indgår en kontraktlig ordning for brugen af it-tjenester, uden at have identificeret og vurderet interessekonflikter, som den kontraktlige ordning kan give anledning til.

I medfør af artikel 28, stk. 7, litra a-d, skal den finansielle enhed sikre sig, at de indgåede kontraktlige ordninger kan opsiges på baggrund af væsentlig overtrædelse begået af tredjepartsudbyderen af it-tjenester af gældende love, administrative bestemmelser eller kontraktvilkår, jf. litra a. Forhold, der er identificeret under overvågningen af it-tredjepartsrisiko, og som anses for at kunne ændre udførelsen af de funktioner, der er leveret gennem den kontraktlige ordning, herunder væsentlige ændringer, der påvirker ordningen eller situationen for tredjepartsudbyderen af it-tjenester skal også kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra b.

Ligeledes skal dokumenterede svagheder hos tredjepartsudbyderen af it-tjenester, som vedrører dennes samlede it-risikostyring, og navnlig i den måde, hvorpå denne garanterer tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, hvad enten det drejer sig om personoplysninger eller på anden måde følsomme data eller andre oplysninger end personoplysninger, kunne lægges til grund for opsigelse af den kontraktlige ordning, jf. litra c. Til sidst skal den kontraktlige ordning kunne opsiges, såfremt Finanstilsynet ikke længere kan føre effektivt tilsyn med den finansielle enhed som følge af betingelserne eller omstændighederne vedrørende de respektive kontraktlige ordninger.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling kan bestå i, at den kontraktlige ordning ikke kan opsiges på baggrund af de af artikel 28, stk. 7, oplistede situationer.

Artikel 28, stk. 8, omhandler exitstrategier. Den finansielle enhed skal indføre exitstrategier for it-tjenester, der understøtter kritiske eller vigtige funktioner.

Exitstrategierne skal tage højde for de risici, der kan opstå hos tredjepartsudbydere af it-tjenester, navnlig mulige svigt fra deres side, en

forringelse af kvaliteten af de leverede it-tjenester, eventuelle driftsforstyrrelser som følge af uhensigtsmæssig eller manglende levering af it-tjenester eller eventuelle væsentlige risici i forbindelse med en passende og løbende anvendelse af de pågældende it-tjenester eller opsigelse af kontraktlige ordninger med tredjepartsudbydere af it-tjenester i en af de i artikel 28, stk. 7, anførte situationer.

Den finansielle enhed skal sikre at de kan opsige den kontraktlige ordning uden at deres forretningsaktivitet afbrydes, jf. litra a, uden at efterlevelsen af de forskriftsmæssige krav begrænses, jf. litra b og uden at kontinuiteten og kvaliteten af de leverede tjenester til kunder lider skade, jf. litra c.

Ligeledes skal exitstrategierne være i overensstemmelse med kriterierne i artikel 4, stk. 2, om proportionalitet, samt være omfattende og veldokumenterede.

Der skal desuden være udarbejdet overgangsplaner der kan fratage tredjepartsudbyderen af it-tjenester de udliciterede it-tjenester og de relevante data og sikkert og fuldstændigt kan overføre disse til alternative udbydere eller på ny indarbejde dem internt. Den finansielle enhed skal derudover identificere alternative løsninger.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke har sikret sig at indføre en exitstrategi i tilfælde af, at en kontrakt ordning med en tredjepartsudbyder af it-tjenester opsiges.

Artikel 29, stk. 1, omhandler foreløbig vurdering af it-koncentrationsrisiko på enhedsniveau. Bestemmelsen fastsætter krav, som den finansielle enhed skal tage hensyn til ved identifikation og vurdering af risici i forbindelse med en kontraktlige ordning, herunder muligheden for, at en kontraktlig ordning kan bidrage til at øge it-koncentrationsrisikoen. Ved indgåelse af en kontraktlig ordning i forbindelse med it-tjenester, der understøtter kritiske eller vigtige funktioner tager den finansielle enhed hensyn til udlicitering til en tredjepartsudbyder af it-tjenester, som ikke er let at erstatte, jf. litra a og indgåelse af flere kontraktlige ordninger om levering af it-tjenester, der understøtter kritiske eller vigtige funktioner, med den samme tredjepartsudbyder af it-tjenester eller med tredjepartsudbydere af it-tjenester, som har tætte forbindelser til denne, jf. litra b.

Den finansielle enhed skal i medfør af bestemmelsen afveje fordele og omkostninger ved alternative løsninger såsom brug af forskellige tredjepartsudbydere af it-tjenester under hensyntagen til, hvorvidt og hvordan de påtænkte løsninger svarer til de forretningsmæssige behov og mål, der er fastsat i deres strategi for digital modstandsdygtighed.

Ansvarssubjektet er den finansielle enhed. Den strafbare handling består i, at den finansielle enhed ikke har taget hensyn til udliciteringen til en tredjepartsudbyder af it-tjenester som ikke er lette at erstatte, ved indgåelsen af en kontraktlig ordning om it-tjenester der understøtter kritiske eller vigtige funktioner.

I medfør af artikel 29, stk. 2, skal den finansielle enhed i tilfælde af, at den kontraktlige ordning for brug af it-tjenester med en tredjepartsudbyder, kan komme videre i underentreprise med hjemsted i tredjeland, overveje de fordele og risici, der kan opstå i forbindelse med underentreprisen, særligt hvis it-tjenesten understøtter kritiske eller vigtige funktioner.

Den finansielle enhed hensyn til de bestemmelser i insolvensretten, som finder anvendelse, hvis tredjepartsudbyderen af it-tjenester går konkurs, samt eventuelle begrænsninger, der kan opstå i forbindelse med en hastende genopretning af den finansielle enheds data, såfremt den kontraktlige ordning vedrører it-tjenester, der understøtter kritiske eller vigtige funktioner.

Den finansielle enhed tager derudover hensyn til overholdelsen af Unionens databeskyttelsesregler og en effektiv håndhævelse af retten i det pågældende tredjeland, såfremt der er indgået kontraktlige ordninger for brug af IKT-tjenester, der understøtter kritiske eller vigtige funktioner, med en tredjepartsudbyder af IKT-tjenester med hjemsted i et tredjeland.

Til sidst vurderer den finansielle enhed hvorvidt og hvordan potentielt lange eller komplekse underentreprisekæder kan påvirke deres evne til fuldt ud at overvåge de udliciterede funktioner og den kompetente myndigheds evne til i denne henseende at føre effektivt tilsyn med den finansielle enhed, såfremt den kontraktlige ordning for brugen af IKT-tjenester, understøtter kritiske eller vigtige funktioner.

Ansvarssubjektet for overtrædelse af bestemmelsen er en finansiel enhed. Den strafbare handling består eksempelvis i, at der ved indgåelse af kontraktlige ordninger med en tredjepartsudbyder af it-tjenester, der understøtter kritiske funktioner, ikke er foretaget en afvejning af fordele og risici såfremt tredjepartsudbyderen giver it-tjenesterne videre til en underentreprise med hjemsted i udlandet.

Artikel 30 omhandler centrale kontrakts bestemmelser.

Artikel 30, stk. 1, fastsætter at rettigheder og forpligtelser mellem den finansielle enhed og tredjepartsudbyderen skal fordeles klart og fastlægges

skriftligt. Serviceniveauaftaler skal være omfattet af den samlede kontrakt og dokumenteres i ét skriftligt dokument. Parterne skal have adgang til dokumentet i papir, eller i et andet varigt og permanent format, der kan downloades.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling kan bestå i, at den finansielle enhed ikke tager højde for, at rettighederne og forpligtelserne mellem parterne skal nedfattes skriftligt og have varig karakter, som enten kan tilgås på papir eller i et format, der kan downloades.

Artikel 30, stk. 2, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester.

Den kontraktlige ordning skal sikre en klar og fuldstændig beskrivelse af alle funktioner og it-tjenester, som tredjepartsudbyderen af it-tjenester skal levere, med angivelse af, om underentreprise af en it-tjeneste, der understøtter en kritisk eller vigtig funktion eller væsentlige dele heraf er tilladt, og, hvis det er tilfældet, de betingelser, der gælder for en sådan underentreprise, jf. litra a.

De steder, navnlig de regioner eller lande, hvor de udliciterede funktioner og it-tjenester eller funktionerne og it-tjenesterne i underentreprise skal leveres, og hvor data skal behandles, herunder lagringsstedet, og kravet om, at tredjepartsudbyderen af it-tjenester på forhånd skal underrette den finansielle enhed, hvis den har planer om at ændre disse steder, jf. litra b.

Den kontraktlige ordning skal ligeledes indeholde bestemmelser om tilgængelighed, autenticitet, integritet og fortrolighed med hensyn til databeskyttelse, herunder personoplysninger, jf. litra c.

Bestemmelser om sikring af adgang, genopretning og tilbagesendelse i et lettilgængeligt format af personoplysninger og andre data end personoplysninger, der behandles af den finansielle enhed, i tilfælde af insolvens, afvikling eller afbrydelse af de forretningsaktiviteter, som tredjepartsudbyderen af it-tjenester varetager, eller i tilfælde af opsigelse af de kontraktlige ordninger skal medtages i den kontraktlige ordning, jf. litra d.

Den kontraktlige ordning skal derudover indeholde beskrivelser af serviceniveauet, herunder ajourføringer og revisioner heraf, jf. litra e.

Forpligtelsen for tredjepartsudbyderen af it-tjenester til at yde bistand til den finansielle enhed uden yderligere omkostninger eller til en omkostning, der fastsættes på forhånd, hvis der opstår en IKT-hændelse, der vedrører den it-

tjeneste, som leveres til den finansielle enhed skal også indgå i den kontraktlige ordning, jf. litra f.

Derudover skal den finansielle enhed medtage forpligtelsen for tredjepartsudbyderen af it-tjenester til at samarbejde fuldt ud med den finansielle enheds kompetente myndigheder og afviklingsmyndigheder, herunder personer, som de har udpeget, jf. litra g og opsigelsesrettigheder og dertil knyttet minimumsfrister for opsigelse af de kontraktlige ordninger i overensstemmelse med de kompetente myndigheders og afviklingsmyndighedernes forventninger, jf. litra h.

Slutteligt skal betingelserne for deltagelse af tredjepartsudbydere af it-tjenester i de finansielle enheders programmer til bevidstgørelse om it-sikkerhed og kurser i digital operationel modstandsdygtighed, jf. artikel 13, stk. 6, medtages i den kontraktlige ordning.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en kontrakt mellem en finansiel enhed og en tredjepartsudbyder af it-tjenester er mangelfuld og ikke på en klar og tilstrækkelig måde, omfatter de af artikel 30, stk. 2, omfattede minimumskrav til kontraktlige ordninger for brugen af it-tjenester som eksempelvis beskrivelserne af serviceniveauet, herunder ajourføringer og revisioner, jf. litra e og opsigelsesrettigheder, jf. litra h.

Artikel 30, stk. 3, fastsætter en række minimumskrav til den kontraktlige ordning for brugen af it-tjenester der understøtter kritiske eller vigtige funktioner.

Den kontraktlige ordning skal sikre en fuldstændig beskrivelse af serviceniveauer, herunder ajourføringer og revisioner heraf, med præcise kvantitative og kvalitative præstationsmål inden for de aftalte serviceniveauer, således at den finansielle enhed kan foretage en effektiv overvågning af it-tjenester, og således at der uden unødigt ophold kan træffes passende afhjælpende foranstaltninger, når de aftalte serviceniveauer ikke overholdes, jf. litra a.

Den kontraktlige ordning skal derudover omfatte opsigelsesfrister og indberetningsforpligtelser for tredjepartsudbyderen af it-tjenester over for den finansielle enhed, herunder underretning om enhver udvikling, som kan have væsentlig indvirkning på, hvorvidt tredjepartsudbyderen af it-tjenester har evnen til effektivt at levere it-tjenester, der understøtter kritiske eller vigtige funktioner i overensstemmelse med de aftalte serviceniveauer, jf. litra b.

Artikel 30, stk. 3, litra c, fastsætter krav til tredjepartsudbyderen af it-tjenester om at gennemføre og teste beredskabsplaner og indføre it-sikkerhedsforanstaltninger, -værktøjer og -politikker, som giver et passende niveau af sikkerhed for, at den finansielle enhed kan foretage levering af tjenester i overensstemmelse med dens reguleringsramme.

Derudover skal den kontraktlige ordning omfatte en forpligtelse for tredjepartsudbyderen af it-tjenester til at deltage i og fuldt ud samarbejde om den finansielle enheds TLPT som omhandlet i artikel 26 og 27, jf. litra d.

Den kontraktlige ordning skal desuden omfatte retten til løbende at overvåge det præstationsniveau, som tredjepartsudbyderen af it-tjenester leverer for den finansielle enhed, en udpeget tredjeparts og Finanstilsynet. Dette indebærer en uindskrænket ret til adgang, inspektion og revision og ret til at tage kopier af relevant dokumentation på stedet, hvis denne har afgørende betydning for tredjepartsudbyderen af it-tjenesters operationer, hvis faktiske udøvelse ikke hindres eller begrænses af andre kontraktlige ordninger eller gennemførelsespolitikker, jf. litra e, nr. i.

Dernæst fastsætter artikel 30, stk. 3, litra e, nr. ii-iv, retten til at nå til enighed om alternative sikkerhedsniveauer, hvis andre kunders rettigheder påvirkes, forpligtelsen for tredjepartsudbyderen af it-tjenester til fuldt ud at samarbejde under de inspektioner og revisioner på stedet, som de kompetente myndigheder, den ledende tilsynsførende, den finansielle enhed eller en udpeget tredjepart udfører og forpligtelsen til at give nærmere oplysninger om omfanget af, de procedurer, som skal følges, og hyppigheden af sådanne inspektioner og revisioner.

I medfør af artikel 30, stk. 3, litra f, skal den finansielle enhed ved en kontraktlig ordning, sørge for at medtage exitstrategier som indeholder en obligatorisk overgangsperiode. I løbet af denne overgangsperiode skal tredjepartsudbyderen af it-tjenester fortsat levere de respektive funktioner eller it-tjenester med henblik på at mindske risikoen for forstyrrelser i den finansielle enhed eller sikre en effektiv afvikling eller omstrukturering heraf. Exitstrategien skal også give den finansielle enhed mulighed for at migrere til en anden tredjepartsudbyder af it-tjenester eller skifte til interne løsninger, der stemmer overens med den leverede tjenestes kompleksitet.

Ansvarssubjektet er en finansiel enhed. Den strafbare handling består eksempelvis i, at en finansiel enhed, ikke formår at vedtage en exitstrategi i deres kontraktlige ordning som sikrer den finansielle enhed forsat, får leveret de respektive funktioner af it-tjenester fra tredjepartsudbyderen.

Til § 13

Til nr. 1 (§ 15, stk. 2, i lov om Danmarks Eksport- og Investeringsfond)

Danmarks Eksport- og Investeringsfonden er ikke i dag underlagt særskilte regler om it- og cybersikkerhed, men er som statslig institution forpligtet til at følge ISO 27001.

Det foreslås i *stk. 2,* at DORA-forordningen ikke finder anvendelse for Danmarks Eksport- og Investeringsfond og dennes selvstændige offentlige dattervirksomheder og øvrige datterselskaber samt enheder forvaltet af Danmarks Eksport- og Investeringsfond eller Danmarks Eksport- og Investeringsfonds selvstændige offentlige dattervirksomheder.

Det følger af DORA-forordningen, at medlemsstater kan undtage enheder, der er oplistet i artikel 2, stk. 5, nr. 4-23, i direktiv 2013/36/EU. Artikel 2, stk. 5, nr. 5, nævner Eksport Kredit Fonden, det nuværende Danmarks Eksport- og Investeringsfond. DORA-forordningen rummer dermed mulighed for at undtage Danmarks Eksport- og Investeringsfond fra forordningens anvendelsesområde.

Baggrunden for at undtage Danmarks Eksport- og Investeringsfond og dennes selvstændige offentlige dattervirksomheder og øvrige datterselskaber samt enheder forvaltet af Danmarks Eksport- og Investeringsfond eller Danmarks Eksport- og Investeringsfonds selvstændige offentlige dattervirksomheder fra DORA-forordningen skal ses i lyset af virksomhedernes særlige status som offentlige finansieringsinstitutter. Danmarks Eksport- og Investeringsfond er en selvstændig offentlig virksomhed under Erhvervsministeriet, hvis formål er at sikre danske virksomheders indgang til risikovillig statslig medfinansiering, og understøtte danske virksomheders mulighed for bl.a. styrket konkurrenceevne og bedre udviklingsmuligheder. Danmarks Eksport- og Investeringsfond løfter dermed en offentlig opgave.

Dertil skal det bemærkes, at Danmarks Eksport- og Investeringsfond ikke driver en selvstændig bank, men benytter sig af bankkonti i forskellige banker. Disse banker er omfattet af DORA-forordningen, og løfter dermed risiciene for it- og cybersikkerheds hændelser.

Til § 14

Til nr. 1 (§ 299 d, stk. 1, nr. 1, i straffeloven)

Det fremgår af § 299 d, stk. 1, nr. 1, at med fængsel indtil 6 år straffes den, der under særligt skærpende omstændigheder gør sig skyldig i overtrædelse af artikel 14, litra a og b, eller artikel 15 i Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16. april 2014 om markedsmisbrug (forordningen om markedsmisbrug).

Artikel 14, litra a og b, og artikel 15 i forordningen om markedsmisbrug fastsætter forbud mod insiderhandel og markedsmanipulation på de finansielle markeder.

Det foreslås at indsætte et nyt *nr. 1* i § 299 d, stk. 1, hvorefter, den der under særligt skærpende omstændigheder gør sig skyldig i overtrædelse af artikel 89, stk. 2, og artikel 91, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver straffes med fængsel indtil 6 år.

For at sikre tillid til markederne for kryptoaktiver og disse markeders integritet er det nødvendigt at fastsætte bestemmelser, der forbyder handlinger, der er egnede til at svække tilliden til de kryptoaktiver, der optages til handel. Af samme årsager er der behov for, at markedsmisbrug og insiderhandel med kryptoaktiver, der er optaget til handel, begået under særligt skærpende omstændigheder straffes efter en højere strafferamme.

Den foreslåede bestemmelse vil medføre, at de bestemmelser i Europa-Parlamentets og Rådets forordning (EU) 2023/1114 af 31. maj 2023 om markeder for kryptoaktiver (MiCA), der vedrører markedsmanipulation og insiderhandel kan straffes med fængsel indtil 6 år.

Den foreslåede bestemmelse vil medføre, at strafferammen for markedsmanipulation og insiderhandel på markeder for kryptoaktiver vil være den samme som for markedsmanipulation og insiderhandel på kapitalmarkederne i henhold til den gældende § 299 d, stk. 1, nr. 1.

Artikel 89, stk. 2, i MiCA fastsætter, at ingen må deltage i insiderhandel eller forsøge at deltage i insiderhandel eller anvende intern viden om kryptoaktiver til erhvervelse eller til afhændelse af disse kryptoaktiver hverken direkte eller indirekte og hverken for egen regning eller for tredjeparts regning. Ingen må anbefale, at en anden person deltager i insiderhandel, eller tilskynde en anden person til at deltage i insiderhandel. Den strafbare handling består eksempelvis i, at en person er kommet i besiddelse af intern viden

og benytter denne viden til enten at afhænde eller erhverve kryptoaktiver, som den pågældende viden vedrører.

Forbuddet i artikel 89, stk. 2, skal forstås i sammenhæng med artikel 87, der definerer begrebet intern viden. Forbuddet i artikel 89, stk. 2, skal ligeledes forstås i sammenhæng med artikel 89, stk. 1, der fastsætter definitionen på insiderhandel. Forbuddet i artikel 89, stk. 2, skal ligeledes forstås i sammenhæng med artikel 89, stk. 6, der fastsætter, at en fysisk person er omfattet af forbuddet uanset, om det er en juridisk person, der har foretaget insiderhandlen, hvis den fysiske person deltager i beslutningen om at foretage erhvervelse, afhændelse, annullering eller ændring af en handelsordre for den pågældende juridiske persons regning.

Ansvarssubjektet for overtrædelse af artikel 89, stk. 2, er en fysisk eller juridisk person. Det er et krav, at personen er i besiddelse af intern viden i henhold til artikel 89, stk. 5.

Artikel 91, stk. 1, i MiCA fastsætter, at ingen må deltage eller forsøge at deltage i markedsmanipulation. Den strafbare handling består eksempelvis i indgåelse af en transaktion, afgivelse af en handelsordre eller enhver anden adfærd, som giver eller antages at give urigtige eller vildledende signaler om udbuddet af, efterspørgslen efter eller prisen på et kryptoaktiv.

Artikel 91, stk. 1, skal forstås i sammenhæng med artikel 91, stk. 2 og 3, der fastsætter hvilke aktiviteter, der udgør markedsmanipulation i henhold til forordningen.

Ansvarssubjektet for overtrædelse af artikel 91, stk. 1, er en fysisk eller juridisk person.

Til § 15

Det foreslås i *stk. 1*, at loven træder i kraft den 1. juli 2024, jf. dog stk. 2-5.

Det foreslåede vil medføre, at de bestemmelser, der supplerer DORA-forordningen og MiCA ligeledes træder i kraft forud for de pågældende retsakter. Disse bestemmelser vil uanset lovens ikrafttrædelse ikke have materielt indhold forud for forordningernes ikrafttræden.

Det foreslås i *stk. 2*, at §§ 332 b, 332 c, 332 e, 332 f, 332 g og 332 h, som affattet ved denne lovs § 1, nr. 24, træder i kraft den 30. juli 2024.

De oplistede bestemmelser fastsætter regler, der supplerer bestemmelser i MICA, der i henhold til MiCA artikel 149, stk. 3, træder i kraft den 30. juli 2024.

Det foreslås i *stk. 3,* at §§ 332, 332 a og 332 d i lov om finansiel virksomhed, som affattet ved denne lovs § 1, nr. 24, § 1, nr. 37, og § 7 træder i kraft den 30. december 2024.

Lovforslagets § 1, nr. 37, og § 7 implementerer ændringer til 4. hvidvaskdirektiv, jf. artikel 38 i den omarbejdede pengeoverførselsforordning. Den forslåede bestemmelse medfører, at ændringerne træder i kraft samme tid som den omarbejdede pengeoverførselsforordning.

Det foreslåede medfører ligeledes, at §§ 332, 332 a og 332 d i lov om finansiel virksomhed, der foreslås ved lovforslagets§ 1, nr. 24, der supplerer MiCA, træder i kraft samme tidspunkt som MiCA, jf. artikel 149, stk. 2, i MiCA.

Det foreslås i *stk. 4,* at § 1, nr. 6, 23, afsnit IX c som affattet ved denne lovs § 1, nr. 24, § 1, nr. 33, og § 3, nr. 2 og 18, træder i kraft den 18. oktober 2024.

Det foreslåede vil medføre, at afsnit IX c, der fastsætter regler, der til dels implementerer NIS 2-direktivet vil træde i kraft samtidig med, at NIS 2-direktivet træder i kraft, jf. artikel 41, stk. 1, i NIS 2-direktivet.

Det foreslåede vil ligeledes medføre, at ophævelser af bestemmelser, der gennemfører det oprindelige NIS-direktiv fra 2016, træder i kraft på samme tidspunkt.

Det foreslås i *stk. 5,* at § 1, nr. 5, 7 og 8, § 2, nr. 1 og 3-13, § 3, nr. 4-8 og 11-13, § 4, nr. 1 og 4, og § 5, nr. 1 og 3, træder i kraft den 17. januar 2025.

De nævnte bestemmelser implementerer dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022, der er et følgedirektiv til DORA.

Det foreslåede vil medføre, at bestemmelserne finder anvendelse fra den 17. januar 2025, hvilket er i med direktivet, jf. artikel 9, stk. 1, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022. Dette er ligeledes samme dato, som DORA forordningen finder anvendelse, jf. artikel 64 i DORA-forordningen.

Bestemmelserne implementerer artikel 9, stk. 1, 2. afsnit, i Europa-Parlamentets og Rådets direktiv (EU) 2022/2556 af 14. december 2022.

Det foreslås i *stk. 6,* at udbydere af kryptoaktivtjenester, der inden den 30. december 2024 udbyder kryptoaktivtjenester, kan fortsætte med at udbyde kryptoaktivtjenester her i landet uden en tilladelse efter den 30. december 2024 i op til 18 måneder eller indtil virksomheden er meddelt tilladelse eller afslag i henhold til § 332 b, stk. 1, såfremt virksomheden indsender en ansøgning efter § 332 b, stk. 1, til Finanstilsynet senest den 30. december 2024.

Det foreslås i *stk. 7,* at udskydelsesperioden i det foreslåede § 43 h, stk. 1, nr. 5, i lov om firmapensionskasser som affattet ved denne lovs § 6, nr. 2, finder anvendelse for variabel løn optjent fra optjeningsperioden efter lovens ikrafttræden, jf. stk. 1. For variabel løn optjent i optjeningsperioder før lovens ikrafttræden finder de hidtil gældende regler anvendelse i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser.

Denne overgangsbestemmelse medfører, at en variabel løn, der allerede ved lovens ikrafttræden, dvs. den 1. juli 202, er under optjening eller udskydelse, skal opfylde de gældende udskydelsesregler i § 18, stk. 1, nr. 5, i bekendtgørelse nr. 16 af 4. januar 2019 om lønpolitik og aflønning i forsikringsselskaber, forsikringsholdingvirksomheder og firmapensionskasser. Det vil sige, at mellem mindst 40-60 pct. af en variabel løn til en ansat, hvis aktiviteter har væsentlig indflydelse på virksomhedens risikoprofil, skal udbetales over en periode på minimum tre år, mens udbetalingen af en variabel løn til et medlem af direktionen eller bestyrelsen skal udbetales over en periode på minimum fire år efter de gældende regler.

En variabel løn, der optjenes fra optjeningsperioden efter lovens ikrafttrædelsesperiode, skal udbetales over en periode på minimum fire år for væsentlige risikotagere og fem år for medlemmer af direktion og bestyrelse.

Det foreslås i *stk. 8,* at regler fastsat i medfør af § 199, stk. 12, 2. pkt., i lov om finansiel virksomhed, jf. lovbekendtgørelse nr. 406 af 29. marts 2022, forbliver i kraft, indtil de ophæves eller afløses af forskrifter udstedt i medfør af § 333 a, stk. a, som affattet ved § 1, nr. 24.

Det foreslåede vil sikre, at bekendtgørelser udstedt i medfør af § 119, stk. 12, 2. pkt., i lov om finansiel virksomhed forbliver i kraft, selvom bestemmelsen ophæves, som følge af denne lovs § 1, nr. 16. Det betyder, at

bekendtgørelse nr. 1581 af 22. december 2022 om systemrevisionens gennemførelse i fælles datacentraler m.fl. fortsat vil være gældende.

Til § 16

Det foreslås i *stk. 1*, at loven ikke gælder for Færøerne og Grønland, jf. dog stk. 2 og 3.

Det foreslås i *stk. 2*, at lovens §§ 1-10 og 12 ved kongelig anordning helt eller delvis kan sættes i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger.

Det følger af lovene på det finansielle område, at lovene ikke gælder for Grønland, men at lovene ved kongelig anordning kan sættes helt eller delvis i kraft for Grønland med de ændringer, som de grønlandske forhold tilsiger.

Lov om Kreditforeningen af kommuner og regioner i Danmark samt lov om Danmarks Eksport- og Investeringsfond gælder ikke i Grønland. Lovforslagets § 11 og 13 skal derfor ikke kunne sættes i kraft for Grønland.

Ændringerne til straffeloven gælder ikke for Grønland. Det skyldes, at der for Grønland gælder en særlig kriminallov. Lovforslagets § 14 skal derfor ikke kunne sættes i kraft for Grønland.

Lov nr. 453 af 10. juni 2003 om finansiel virksomhed er anordnet på Grønland ved kongelig anordning nr. 1252 af 15. december 2004.

Lov nr. 651 af 8. juni 2017 om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) er sat i kraft for Grønland ved kongelig anordning nr. 812 af 12. august 2019.

Det foreslås i *stk. 3*, at §§ 1-5, 7 og 12 kan ved kongelig anordning helt eller delvis sættes i kraft for Færøerne med de ændringer, som de færøske forhold tilsiger.

Det følger af lovene på det finansielle område, at lovene ikke gælder for Færøerne, men at lovene ved kongelig anordning kan sættes helt eller delvis i kraft for Færøerne med de ændringer, som henholdsvis de færøske forhold tilsiger.

Lovforslagets §§ 6, 8, 9 og 10 skal ikke kunne sættes i kraft for Færøerne, da forsikringsområdet på Færøerne er overtaget og dermed reguleres af færøske love. Lov om firmapensionskasser, lov om forsikringsvirksomhed

og lov om en garantifond for skadesforsikringsselskaber gælder derfor ikke for Færøerne og indeholder ikke en anordningshjemmel.

Lov om Kreditforeningen af kommuner og regioner i Danmark samt lov om Danmarks Eksport- og Investeringsfond gælder ikke i Færøerne. Lovforslagets § 11 og 13 skal derfor ikke kunne sættes i kraft for Færøerne.

Ændringerne til straffeloven gælder ikke for Færøerne. Det skyldes, at Færøerne den 1. marts 2010 overtog lovgivningskompetencen på det strafferetlige område. Lovforslagets § 14 skal derfor ikke kunne sættes i kraft for Færøerne.

Lov nr. 652 af 8. juni 2017 om betalinger er sat i kraft på Færøerne ved kongelig anordning nr. 1223 af 11. juni 2021.

Lov nr. 651 af 8. juni 2017 om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme (hvidvaskloven) er sat i kraft for Færøerne ved kongelig anordning nr. 813 af 16. august 2019.