UDKAST

Dato: 12. december 2024
Kontor: Sikkerhed
Sagsbeh: Akashdip Kaur Sahota
Sagsnr.: 2024-13723
Dok.: 3499872

Forslag
til
Lov om sikkerhed og beredskab i telesektoren[1]

Kapitel 1
Anvendelsesområde og definitioner

§ 1. Denne lov finder anvendelse for udbydere, der stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed i Danmark, jf. dog stk. 2.

Stk. 2. Loven finder ikke anvendelse for kommuner og regioner, der stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed i Danmark.

Stk. 3. Teleudbydere kan, uanset om de er omfattet af lovens anvendelsesområde, give frivillig underretning til Center for Cybersikkerhed og CSIRT'en efter § 9.

Stk. 4. § 17 om CSIRT'ens opgaver i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau finder tilsvarende anvendelse for denne lov.

§ 2. I denne lov forstås ved:

1) Beredskabssituationer og andre ekstraordinære situationer: Situationer, hvor der allerede er, eller hvor der kan opstå større ulykker, katastrofer eller

---

[1] Loven gennemfører dele af Europa-Parlamentets og Rådets direktiv 2018/1972/EU af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning), EU-Tidende 2018, nr. L 321, side 36. Loven indeholder desuden bestemmelser, der gennemfører 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, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), EU-Tidende 2022, nr. L 333, side 80 i telesektoren.

hændelser, herunder krise eller krig og hvor der er risiko for påvirkning af udbuddet af net og tjenester.

2) Cybertrussel: Enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer.

3) Elektronisk kommunikationsnet: Transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrati-onskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres.

4) Elektronisk kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester, omfatter følgende typer tjenester

a) internetadgangstjenester,

b) interpersonelle kommunikationstjenester og

c) tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

5) Hændelse: En begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.

6) Håndtering af hændelser: Enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.

7) Interpersonel kommunikationstjeneste: En tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, undtaget tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

8) Net- og informationssystem:

a) Et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres.
b) Enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data.
c) Digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.
9) Nærvedhændelse: En begivenhed, der kunne have bragt tilgængeligheden, autenciteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke indtraf.
10) Offentligt elektronisk kommunikationsnet: Et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem netterminerringspunkter.
11) Offentligt tilgængelige elektroniske kommunikationstjenester: En elektronisk kommunikationstjeneste, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.
12) Radiobaseret lokalnet: et trådløst adgangssystem med lav effekt og lille rækkevidde, der har en lav risiko for at skabe interferens med andre sådanne systemer etableret i nærheden af andre brugere, og som på et ikkeeksklusivt grundlag anvender harmoniserede radiofrekvenser.
13) Sikkerhed i net- og informationssystemer: Net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

14) Teleudbyder: Den, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre.
15) Væsentlig cybertrussel: En cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en udbyders net- og informationssystemer eller på brugerne af udbyderens tjenester ved at forårsage betydelig fysisk eller ikke fysisk skade.

§ 3. Teleudbydere, der med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden, anses for at være væsentlige, hvis de opfylder mindst én af følgende betingelser:
1) Udbyderen beskæftiger mere end 50 ansatte.
2) Udbyderen har en årlig omsætning på over 10 mio. EUR og en årlig balance på over 10 mio. EUR.

Stk. 2. Uanset teleudbyderens størrelse, kan Center for Cybersikkerhed træffe afgørelse om, at følgende teleudbydere skal anses som væsentlige, hvis:
1) Teleudbyderen er den eneste udbyder i Danmark af et net eller en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.
2) En forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden.
3) En forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne medføre en væsentlig systemisk risiko, herunder hvor en sådan forstyrrelse kan have en grænseoverskridende virkning.
4) Teleudbyderen er kritisk på grund af udbyderens specifikke betydning på nationalt eller regionalt plan for sektoren eller typen af net eller tjeneste eller for andre indbyrdes afhængige sektorer i Danmark.
5) Teleudbyderen er identificeret som en kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed.

§ 4. Teleudbydere, der ikke opfylder kriterierne for at være væsentlige udbydere efter lovens § 3, anses som vigtige teleudbydere, såfremt de med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke accessorisk del af virksomheden.

Stk. 2. Center for Cybersikkerhed kan efter en konkret vurdering træffe afgørelse om, at en teleudbyder, der er omfattet af § 3, stk. 2, nr. 1-4, skal anses som en vigtig teleudbyder.

Kapitel 2
Foranstaltninger til styring af sikkerhedsrisici mv.

§ 5. Væsentlige og vigtige teleudbydere skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse udbydere anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere hændelsers indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte eller tage højde for:

1) Politikker for risikoanalyse og informationssystemsikkerhed.
2) Håndtering af hændelser.
3) Driftskontinuitet, eksempelvis backup-styring og reetablering efter en katastrofe, og krisestyring.
4) Forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte teleudbyder og udbyderens 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 sikkerhedsrisici.
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.
10) Brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt hos udbyderen, hvor det er relevant.

Stk. 2. En væsentlig eller en vigtig teleudbyder, der finder, at den pågældende udbyder ikke overholder ét eller flere af de i stk. 1, nævnte krav til foranstaltningerne eller regler om krav til foranstaltninger fastsat i medfør af stk. 3, skal uden unødigt ophold træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om krav til foranstaltninger efter stk. 1, samt krav om yderligere foranstaltninger for teleudbydere omfattet af denne lov.

§ 6. De foranstaltninger, som en væsentlig eller en vigtig teleudbyder træffer på baggrund af forpligtelserne i § 5, stk. 1 og 2, samt regler fastsat i medfør af § 6, stk. 3, skal være godkendt af teleudbyderens ledelsesorgan. Ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse og sikrer, at foranstaltningerne har den fornødne effekt.

Stk. 2. Medlemmerne af ledelsesorganet i en væsentlig eller vigtig teleudbyder skal deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til at tilsvarende kurser tilbydes til udbyderen øvrige ansatte.

§ 7. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i § 5, stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af § 5, stk. 3.

Kapitel 3
Oplysnings- og underretningspligter mv.

§ 8. Væsentlige og vigtige teleudbydere skal registrere sig hos Center for Cybersikkerhed og i den forbindelse oplyse:
1) Teleudbyderens navn.
2) Adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre.
3) Når relevant en liste over de øvrige medlemsstater i Den Europæiske Union, hvor teleudbyderen leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i Europa-Parlamentets og Rådets direktiv 2022/2555/EU 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).

Stk. 2. Oplysningerne efter stk. 1, skal indgives senest den 1. oktober 2025. En væsentlig eller en vigtig teleudbyder, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne senest to uger efter, at teleudbyderen omfattes af loven.

Stk. 3. I tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal den væsentlige eller vigtige teleudbyder give Center for Cybersikkerhed underretning herom senest to uger efter datoen for ændringen.

stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om hvilke yderligere oplysninger væsentlige og vigtige teleudbydere skal afgive ved registrering.

Stk. 5. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder krav om:

1) Afgivelse af oplysninger om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf.

2) Krav om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, herunder regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

§ 9. Teleudbydere skal uden unødigt ophold underrette Center for Cybersikkerhed og CSIRT'en om enhver væsentlig hændelse. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Stk. 2. En hændelse anses for at være væsentlig, hvis den

1) har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af net eller tjenester eller økonomiske tab for den berørte udbyder, eller

2) har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke fysisk skade.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig samt hvilke oplysninger, der skal gives i forbindelse med underretningen.

§ 10. Underretningen efter § 9, stk. 1, skal ske på følgende måde:

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

2) En hændelsesunderretning, som skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindi-

katorerne, hvor sådanne foreligger, sendes uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at udbyderen har fået kendskab til den væsentlige hændelse, jf. dog stk. 2.
3) En foreløbig rapport med relevante statusopdateringer sendes til Center for Cybersikkerhed eller CSIRT'en efter anmodning.
4) En endelig rapport sendes til Center for Cybersikkerhed eller CSIRT'en senest en måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Rapporten skal indeholde 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) De eventuelle grænseoverskridende virkninger af hændelsen.
5) Såfremt hændelsen fortsat pågår på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den berørte udbyder forelægge en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Stk. 2. Center for Cybersikkerhed og CSIRT'en sikrer, at den underrettende teleudbyder uden unødigt ophold og, hvor det er muligt, inden for 24 timer efter modtagelsen af den tidlige varsling, jf. stk. 1, nr. 1, gives et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse. Efter anmodning fra udbyderen skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

§ 11. Teleudbydere kan underrette Center for Cybersikkerhed og CSIRT'en om hændelser, der ikke er omfattet af lovens § 9, nærvedhændelser og cybertrusler.

Stk. 2. Center for Cybersikkerhed og CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 10. CSIRT'en og Center for Cybersikkerhed kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 9.

§ 12. I relevant omfang underretter teleudbydere uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser, jf. § 10, der sandsynligvis vil påvirke leveringen af deres tjenester negativt.

Stk. 2. Teleudbydere oplyser uden unødigt ophold modtagerne af deres tjenester, som potentielt er berørt af en væsentlig hændelse, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som

reaktion på den pågældende hændelse. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om den væsentlige hændelse.

§ 13. Center for Cybersikkerhed kan efter høring af en teleudbyder, der er ramt af en væsentlig hændelse, jf. § 9, informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Stk. 2. Center for Cybersikkerhed kan i de situationer, der er nævnt i stk. 1, kræve, at den relevante teleudbyder informerer offentligheden om den væsentlige hændelse.

Stk. 3. CSIRT'en kan efter samme kriterier som i stk. 1 informere offentligheden om væsentlige hændelser, der kan påvirke mere end én sektor.

Stk. 4. CSIRT'en kan efter samme kriterier som i stk. 1 informere offentligheden om væsentlige hændelser i andre medlemsstater.

Kapitel 4
Beredskabs- og andre ekstraordinære situationer

§ 14 Center for Cybersikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Stk. 2. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal underrette Center for Cybersikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder, herunder regler om, hvordan underretningen skal foretages.

Stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Stk. 5. I beredskabssituationer og i andre ekstraordinære situationer kan Center for Cybersikkerhed påbyde væsentlige og vigtige teleudbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i

tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.

Kapitel 5
Aktindsigt i oplysninger og underretninger

§ 15. Underretninger modtaget i medfør af § 9, stk. 1-2, og § 11 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

§ 16. Det kan i regler udstedt i medfør af § 8, stk. 5, og § 14, stk. 3, fastsættes, at underretninger og afgivelse af oplysninger efter disse bestemmelser er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Kapitel 6
Sikkerhedsgodkendelser

§ 17. Medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse udbydere skal sikkerhedsgodkendes af Center for Cybersikkerhed, når:
1) det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage.
2) den pågældende varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 14, stk. 3.

Stk. 2. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med justitsministeren fastsætte regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgninger samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser.

Kapitel 8
Tilsyn og håndhævelse

§ 18. Center for Cybersikkerhed fører tilsyn med overholdelse af denne lov og regler, der er udstedt i medfør af loven.

§ 19. Såfremt det er nødvendigt af hensyn til sikkerheden i net- og informationssystemer, har Center for Cybersikkerhed efter et skriftligt varsel på mindst syv arbejdsdage uden retskendelse mod behørig legitimation adgang

til forretningslokaler hos væsentlige og vigtige teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, herunder i relation til outsourcet aktivitet.

Stk. 2. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler efter stk. 1, tilgå kommunikation til, fra eller mellem udbyderens kunder.

§ 20. Center for Cybersikkerhed kan påbyde væsentlige og vigtige teleudbydere at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net- og informationssystemer i deres risikostyringsprocesser efter § 5.

Stk. 2. Såfremt det er af væsentlig samfundsmæssig betydning, kan Center for Cybersikkerhed påbyde væsentlige og vigtige teleudbydere at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net- og informationssystemer. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler herom.

Væsentlige teleudbydere

§ 21. Center for Cybersikkerhed kan som led i sit tilsyn ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger over for en væsentlig teleudbyder:

1) Foretage kontrol på stedet og eksternt tilsyn, herunder foretage stikprøvekontroller.
2) Foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Center for Cybersikkerhed.
3) Foretage sikkerhedsaudits ad hoc.
4) Foretage sikkerhedsscanninger.
5) Kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført.
6) Kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.
7) Kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker.

8) Kræve at få skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Center for Cybersikkerheds tilsynsvirksomhed.

Stk. 2. Ved anvendelsen af tiltagene i stk. 1, nr. 5-8, skal Center for Cybersikkerhed angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret.

Stk. 3. Center for Cybersikkerhed kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 5-8, skal afgives.

§ 22. Center for Cybersikkerhed kan ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende håndhævelsesforanstaltninger over for en væsentlig teleudbyder:

1) Udstede advarsler om teleudbyderens overtrædelse af denne lov.

2) Udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.

3) Påbyde teleudbyderen at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

4) Meddele teleudbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.

5) Påbyde teleudbyderen at underrette de fysiske eller juridiske personer, som teleudbyderen leverer tjenester til eller udfører aktiviteter for, og som potentielt kan være berørt af en væsentlig trussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.

6) Påbyde teleudbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

7) Udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med teleudbyderens overholdelse af lovens kapitel 2 og 3 samt regler udstedt i medfør heraf.

8) Påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

§ 23. Har de håndhævelsesforanstaltninger, der er pålagt i medfør af § 26, nr. 1-6, vist sig at være utilstrækkelige, kan Center for Cybersikkerhed fastsætte en frist, inden for hvilken den væsentlige teleudbyder skal foretage de

nødvendige tiltag for at afhjælpe manglerne eller opfylde Center for Cybersikkerheds krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan Center for Cybersikkerhed træffe afgørelse om:

1) Midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, teleudbyderen leverer, eller aktiviteter, der udføres af teleudbyderen.

2) Midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner i den pågældende teleudbyder.

Stk. 2. Midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kan kun anvendes, indtil den væsentlige teleudbyder træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningerne blev anvendt.

Stk. 3. En afgørelse efter stk. 1, kan af den væsentlige teleudbyder eller den fysiske person, afgørelsen vedrører, forlanges indbragt for domstolene. Center for Cybersikkerhed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den teleudbyder eller person, som har forlangt sagen indbragt.

Stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om, hvilke certificeringer og godkendelser, der er omfattet af stk. 1, nr. 1.

Vigtige teleudbydere

§ 24. Center for Cybersikkerhed kan som led i sit tilsyn, hvis der er indikationer på, at en vigtig teleudbyder ikke overholder eller ikke har overholdt denne lov eller regler udstedt i medfør af loven, ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger:

1) Foretage kontrol på stedet.

2) Foretage målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Center for Cybersikkerhed.

3) Foretage sikkerhedsscanninger.

4) Kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført.

5) Kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven.

6) Kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker.
7) Kræve at få skriftlige udtalelser og redegørelser om faktisk forhold af betydning for Center for Cybersikkerheds tilsynsvirksomhed.

Stk. 2. Ved anvendelse af tiltagene i stk. 1, nr. 4-7, skal Center for Cybersikkerhed angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret.

Stk. 3. Center for Cybersikkerhed kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 4-7, skal afgives.

§ 25. Center for Cybersikkerhed kan ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende håndhævelsesforanstaltninger over for en vigtig teleudbyder:
1) Udstede advarsler om teleudbyderens overtrædelse af denne lov.
2) Udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.
3) Meddele teleudbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.
4) Påbyde teleudbyderen at underrette de fysiske eller juridiske personer, som udbyderen leverer tjenester til eller udfører aktiviteter for, og som potentielt kan være berørt af en væsentlig trussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.
5) Påbyde teleudbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.
6) Påbyde teleudbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3, samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Høring af væsentlige og vigtige teleudbydere

§ 26. Inden Center for Cybersikkerhed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 22, 23 og 25, underrettes den berørte væsentlige eller vigtige teleudbyder om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Center for Cybersikkerhed skal give

teleudbyderen en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde hvor formålet med foranstaltningen ellers ville forspildes.

Offentliggørelse

§ 27. Center for Cybersikkerhed kan i ikke-anonymiseret form offentliggøre:
1) Påbud og forbud meddelt i medfør af § 28, og afgørelser truffet i medfør af regler, der er udstedt i medfør af § 5, stk. 3, § 9, stk. 4, § 14, stk. 2, og § 14, stk. 4.
2) Resultater af tilsyn efter 22, stk. 1.
3) Resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov.
4) Resumeer af domme i retssager, hvor Center for Cybersikkerhed er part.

Stk. 2. Offentliggørelse efter stk. 1 må ikke indeholde:
1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den væsentlige eller vigtige teleudbyder, som oplysningerne angår,
2) oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar,
3) klassificerede informationer,
4) fortrolige oplysninger, der hidrører fra nationale tilsynsmyndigheder i andre EU-medlemsstater, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelse, eller
5) oplysninger om enkeltpersoners forhold.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Kapitel 9
Videregivelse af oplysninger, gensidig bistand, gennemførelsesretsakter, digital kommunikation mv.

§ 28. De forpligtelser, der er fastsat i denne lov eller i regler udstedt i medfør af loven, omfatter ikke meddelelse af oplysninger, hvis videregi-

velse ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar.

Stk. 2. Oplysninger, der modtages eller hidrører fra myndigheder i andre EU-medlemsstater, behandles som fortrolige, såfremt den afgivende myndighed betragter oplysningerne som fortrolige i henhold til EU-regler eller nationale regler.

§ 29. Center for Cybersikkerhed kan hos teleudbydere, der omfattet af § 14. stk. 3, indsamle oplysninger med henblik på at videregive disse til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater, i det omfang det er nødvendigt for, at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende EU-ret.

Stk. 2. Center for Cybersikkerhed orienterer de udbydere, der er omfattet af § 14, stk. 3, og som der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

§ 30. Hvor en væsentlig eller vigtig teleudbyder leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor udbyderen leverer tjenester i en eller flere medlemsstater, og udbyderens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder Center for Cybersikkerhed med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet indebærer, at:

1) Center for Cybersikkerhed underretter de kompetente myndigheder i relevante medlemsstater om tilsyns- og håndhævelsesforanstaltninger.
2) Center for Cybersikkerhed kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger.
3) Center for Cybersikkerhed yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

Stk. 2. Center for Cybersikkerhed kan efter nærmere aftale gennemføre fælles tilsynstiltag med kompetente myndigheder fra andre medlemsstater i Den Europæiske Union.

§ 31. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

§ 32. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Kapitel 10
Straf

§ 33. Med bøde straffes den, der:
1) Overtræder § 5, stk. 1, eller 2, eller §§ 6, 8-10 eller 12.
2) Undlader at efterkomme Center for Cybersikkerheds afgørelse efter § 27, stk. 1.
3) Undlader at efterkomme påbud og forbud efter §§ 22 eller 25.
4) Undlader at efterkomme krav efter § 13, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, § 24, stk. 1, nr. 2 eller nr. 4-6.
5) Hindrer Center for Cybersikkerhed i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, stk. 1, nr. 1-3.

Stk. 2. Der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 3. Hvis der er pålagt en bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven, kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd som den, der var genstand for bøden i medfør af nævnte forordning eller databeskyttelsesloven.

Stk. 4. I regler udstedt i medfør af loven kan der fastsættes straf i form af bøde for overtrædelse af regler udstedt i medfør af loven.

Kapitel 11
Ikrafttrædelse og ændringer i anden lovgivning mv.

§ 34. Loven træder i kraft den 1. juli 2025.

Stk. 2. Lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021, ophæves.

§ 35. Loven gælder ikke for Færøerne og Grønland.

§ 36. I lov om leverandørsikkerhed i den kritiske teleinfrastruktur, jf. lov nr. 1156 af 8. juni 2021, foretages følgende ændringer.

1. § 1, nr. 3, affattes således:

»3) Vigtig teleudbyder: En teleudbyder, som er identificeret som en vigtig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«

2. I § 1 indsættes som *nr. 4:*

»4) Væsentlig teleudbyder: En teleudbyder, som er identificeret som en væsentlig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«

3. I § 2, stk. 1, § 3, stk. 1-2, og § 15, ændres »væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester« til: »væsentlig eller vigtig teleudbyder«.

Bilag 1

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)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Den Europæiske Centralbank ([1]),

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([2]),

efter høring af Regionsudvalget,

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([4]) tog sigte på at opbygge cybersikkerhedskapaciteter i hele Unionen, afbøde trusler mod net- og informationssystemer, der anvendes til at levere væsentlige tjenester i nøglesektorer, og sikre kontinuiteten af sådanne tjenester, når de står over for hændelser, og dermed bidrage til Unionens sikkerhed og til, at dens økonomi og samfund kan fungere effektivt.

(2) Siden ikrafttrædelsen af direktiv (EU) 2016/1148 er der gjort betydelige fremskridt med hensyn til at øge Unionens niveau af cyberrobusthed. Evalueringen af nævnte direktiv har vist, at det har fungeret som katalysator for den institutionelle og lovgivningsmæs-

sige tilgang til cybersikkerhed i Unionen og har banet vejen for en betydelig holdningsændring. Nævnte direktiv har sikret færdiggørelsen af nationale rammer for sikkerheden i net- og informationssystemer ved at fastlægge nationale strategier for sikkerheden i net- og informationssystemer og etablere nationale kapaciteter og ved at gennemføre lovgivningsmæssige foranstaltninger, der omfatter væsentlige infrastrukturer og enheder, som hver medlemsstat har identificeret. Direktiv (EU) 2016/1148 har også bidraget til samarbejdet på EU-plan gennem oprettelsen af samarbejdsgruppen og netværket af nationale enheder, der håndterer IT-sikkerhedshændelser. Uanset disse resultater har evalueringen af direktiv (EU) 2016/1148 afsløret iboende mangler, der forhindrer det i effektivt at tackle aktuelle og nye cybersikkerhedsudfordringer.

(3) Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af cybertrusler og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater. Antallet, omfanget, den avancerede karakter, hyppigheden og virkningen af hændelser er stigende og udgør en alvorlig trussel mod net- og informationssystemernes funktion. Som følge heraf kan hændelser hindre udøvelsen af økonomiske aktiviteter i det indre marked, medføre økonomiske tab, underminere brugernes tillid og forårsage store skader på Unionens økonomi og samfund. Cybersikkerhedsberedskab og -effektivitet er derfor mere afgørende for et velfungerende indre marked end nogensinde før. Cybersikkerhed er desuden en vigtig katalysator for, at mange kritiske sektorer kan tage den digitale omstilling til sig med et positivt resultat og fuldt ud kan udnytte de økonomiske, sociale og bæredygtige fordele ved digitalisering.

(4) Retsgrundlaget for direktiv (EU) 2016/1148 var artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), hvis formål er det indre markeds oprettelse og funktion ved at styrke foranstaltninger til indbyrdes tilnærmelse af de nationale regler. De cybersikkerhedskrav, der pålægges enheder, som leverer tjenester eller som udfører aktiviteter, der er økonomisk betydningsfulde, varierer betydeligt fra medlemsstat til medlemsstat med hensyn til typen af krav, detaljeringsgrad og tilsynsmetode. Disse forskelle medfører yderligere omkostninger og skaber vanskeligheder for

enheder, der udbyder varer eller tjenester på tværs af grænserne. Krav, der stilles af en medlemsstat, og som er forskellige fra eller endog i konflikt med dem, der er pålagt af en anden medlemsstat, kan påvirke sådanne grænseoverskridende aktiviteter i væsentlig grad. Desuden har muligheden for en utilstrækkelig udformning eller gennemførelse af cybersikkerhedskravene i én medlemsstat sandsynligvis konsekvenser for cybersikkerhedsniveauet i andre medlemsstater, navnlig i betragtning af intensiteten af grænseoverskridende udvekslinger. Evalueringen af direktiv (EU) 2016/1148 har vist, at der er store forskelle i medlemsstaternes gennemførelse af det, herunder med hensyn til dets anvendelsesområde, hvis afgrænsning i vid udstrækning blev overladt til medlemsstaternes skøn. Direktiv (EU) 2016/1148 gav også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af de sikkerheds- og hændelsesrapporteringsforpligtelser, der er fastsat deri. Disse forpligtelser blev derfor gennemført på vidt forskellige måder på nationalt plan. Der er lignende forskelle i gennemførelsen af bestemmelserne i direktiv (EU) 2016/1148 om tilsyn og håndhævelse.

(5) Alle disse forskelle medfører en fragmentering af det indre marked og kan have en negativ indvirkning på dets funktion og navnlig påvirke den grænseoverskridende levering af tjenester og cyberrobustheden som følge af anvendelsen af forskellige foranstaltninger. Disse forskelle kan i sidste ende føre til, at visse medlemsstater har en højere sårbarhed over for cybertrusler, hvilket potentielt kan have afsmittende virkninger i hele Unionen. Dette direktiv sigter mod at fjerne sådanne store forskelle mellem medlemsstaterne, navnlig ved at fastsætte minimumsregler for, hvordan en koordineret reguleringsramme fungerer, ved at fastlægge mekanismer for effektivt samarbejde mellem de ansvarlige myndigheder i hver medlemsstat, ved at ajourføre listen over sektorer og aktiviteter, der er omfattet af cybersikkerhedsforpligtelser, og ved at tilvejebringe effektive retsmidler og håndhævelsesforanstaltninger, der er afgørende for effektiv håndhævelse af disse forpligtelser. Derfor bør direktiv (EU) 2016/1148 ophæves og erstattes af nærværende direktiv.

(6) Med ophævelsen af direktiv (EU) 2016/1148 bør anvendelsesområdet for de enkelte sektorer udvides til at omfatte en større del af økonomien for at give en omfattende dækning af sektorer og tjenester af vital betydning for vigtige samfundsmæssige og økonomiske

aktiviteter i det indre marked. Nærværende direktiv sigter navnlig mod at afhjælpe manglerne i differentieringen mellem operatører af væsentlige tjenester og udbydere af digitale tjenester, som har vist sig at være forældet, da den ikke afspejler sektorernes eller tjenesternes betydning for de samfundsmæssige og økonomiske aktiviteter i det indre marked.

(7) I henhold til direktiv (EU) 2016/1148 havde medlemsstaterne ansvaret for at identificere de enheder, der opfyldte kriterierne for at blive betragtet som operatører af væsentlige tjenester. For at fjerne de store forskelle mellem medlemsstaterne i denne henseende og garantere retssikkerhed for så vidt angår foranstaltningerne til styring af cybersikkerhedsrisici og rapporteringsforpligtelserne for alle relevante enheder bør der fastsættes et ensartet kriterium for, hvilke enheder der er omfattet af nærværende direktivs anvendelsesområde. Dette kriterium bør bestå i anvendelsen af en regel om størrelsesloft, ifølge hvilken alle enheder, der udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til Kommissionens henstilling 2003/361/EF ([5]), eller overskrider tærsklerne for mellemstore virksomheder fastsat i nævnte artikels stk. 1, og som opererer inden for de sektorer og leverer de typer tjenester eller udfører de aktiviteter, der er omfattet af nærværende direktiv, er omfattet af dets anvendelsesområde. Medlemsstaterne bør også sørge for, at visse små virksomheder og mikrovirksomheder, som defineret i nævnte bilags artikel 2, stk. 2 og 3, der opfylder specifikke kriterier, der tyder på en central rolle for samfundet eller økonomien eller bestemte sektorer eller typer af tjenester, omfattes af nærværende direktivs anvendelsesområde.

(8) Udelukkelsen af offentlige forvaltningsenheder fra dette direktivs anvendelsesområde bør gælde for enheder, hvis aktiviteter hovedsagelig udføres inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Offentlige forvaltningsenheder, hvis aktiviteter kun er marginalt forbundet med disse områder, bør dog ikke udelukkes fra dette direktivs anvendelsesområde. Med henblik på dette direktiv anses enheder med reguleringsbeføjelser ikke for at udføre aktiviteter inden for retshåndhævelse, og de er derfor ikke på dette grundlag udelukket fra dette direktivs anvendelsesområde. Offentlige forvaltningsenheder, der er etableret i fællesskab med et tredjeland i overensstemmelse med en international aftale, er udelukket fra dette direktivs

anvendelsesområde. Dette direktiv finder ikke anvendelse på medlemsstaternes diplomatiske og konsulære missioner i tredjelande eller på deres net- og informationssystemer, for så vidt sådanne systemer befinder sig i missionens lokaler eller drives for brugere i et tredjeland.

(9) Medlemsstaterne bør kunne træffe de nødvendige foranstaltninger for at sikre beskyttelsen af væsentlige nationale sikkerhedsinteresser, opretholde den offentlige orden og sikkerhed samt tillade forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger. Med henblik herpå bør medlemsstater kunne undtage specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, fra visse forpligtelser, der er fastsat i dette direktiv, for så vidt angår disse aktiviteter. Hvor en enhed udelukkende leverer tjenester til en offentlig forvaltningsenhed, der er udelukket fra dette direktivs anvendelsesområde, bør medlemsstater kunne undtage denne enhed fra visse forpligtelser, der er fastsat i dette direktiv, for så vidt angår disse tjenester. Endvidere bør ingen medlemsstat være forpligtet til at meddele oplysninger, hvis videregivelse efter dens opfattelse ville stride mod dens væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar. Nationale regler eller EU-regler om beskyttelse af fortrolige oplysninger, hemmeligholdelsesaftaler og uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol, bør tages i betragtning i denne sammenhæng. Traffic Light Protocol skal forstås som et middel til at informere om eventuelle begrænsninger for så vidt angår den videre spredning af oplysninger. Den anvendes i næsten alle enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er), og i nogle informationsanalyse- og informationsdelingscentre.

(10) Selv om dette direktiv finder anvendelse på enheder, der beskæftiger sig med produktion af elektricitet fra kernekraftværker, kan nogle af disse aktiviteter være knyttet til den nationale sikkerhed. Hvor det er tilfældet, bør en medlemsstat kunne udøve sit ansvar for at beskytte sin nationale sikkerhed med hensyn til disse aktiviteter, herunder aktiviteter inden for den nukleare værdikæde, i overensstemmelse med traktaterne.

(11) Nogle enheder udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder fore-

byggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, og leverer samtidig tillidstjenester. Tillidstjenesteudbydere, der er omfattet af anvendelsesområdet for Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 ([6]), bør være omfattet af dette direktivs anvendelsesområde for at sikre samme niveau af sikkerhedskrav og tilsyn som det, der tidligere var fastsat i nævnte forordning, for så vidt angår tillidstjenesteudbydere. I overensstemmelse med udelukkelsen af visse specifikke tjenester fra forordning (EU) nr. 910/2014 bør dette direktiv ikke finde anvendelse på levering af tillidstjenester, der udelukkende anvendes i lukkede systemer i henhold til national ret eller aftaler mellem et defineret sæt deltagere.

(12) Postbefordrende virksomheder som defineret i Europa-Parlamentets og Rådets direktiv 97/67/EF ([7]), herunder udbydere af kurertjenester, bør være omfattet af nærværende direktiv, hvis de leverer mindst ét led i postbefordringskæden, navnlig indsamling, sortering, transport eller omdeling, herunder afhentning, samtidig med at der tages hensyn til omfanget af deres afhængighed af net- og informationssystemer. Transporttjenester, der ikke udføres i forbindelse med et af disse trin, bør udelukkes fra anvendelsesområdet for posttjenester.

(13) I betragtning af intensiveringen og den stadig mere sofistikerede karakter af cybertrusler bør medlemsstaterne bestræbe sig på at sikre, at enheder, der er udelukket fra dette direktivs anvendelsesområde, opnår et højt cybersikkerhedsniveau, og på at støtte gennemførelsen af tilsvarende foranstaltninger til styring af cybersikkerhedsrisici, der afspejler disse enheders følsomme karakter.

(14) EU-retten om databeskyttelse og privatlivets fred finder anvendelse på enhver behandling af personoplysninger i henhold til dette direktiv. Navnlig berører dette direktiv ikke Europa-Parlamentets og Rådets direktiv (EU) 2016/679 ([8]) og Europa-Parlamentets og Rådets direktiv 2002/58/EF ([9]). Nærværende direktiv bør derfor ikke berøre bl.a. de opgaver og beføjelser, der påhviler de myndigheder, der har kompetence til at overvåge overholdelsen af gældende EU-ret om databeskyttelse og om privatlivets fred.

(15) Enheder, der er omfattet af dette direktiv med henblik på overholdelse af foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, bør inddeles i to kategorier, væsentlige

enheder og vigtige enheder, der afspejler, i hvilket omfang de er kritiske for så vidt angår deres sektor eller den type tjenester, de leverer, samt deres størrelse. I den henseende bør der tages behørigt hensyn til eventuelle relevante sektorspecifikke risikovurderinger eller vejledning fra de kompetente myndigheder, hvor det er relevant. Tilsyns- og håndhævelsesordningerne for disse to kategorier af enheder bør differentieres for at sikre en fair balance mellem risikobaserede krav og forpligtelser på den ene side og den administrative byrde, der følger af tilsynet med overholdelsen, på den anden side.

(16) For at undgå, at enheder, der har partnervirksomheder eller er tilknyttede virksomheder, betragtes som væsentlige eller vigtige enheder, hvor dette ville være uforholdsmæssigt, kan medlemsstaterne tage hensyn til den grad af uafhængighed, som en enhed har i forhold til sine partnervirksomheder eller tilknyttede virksomheder, når artikel 6, stk. 2, i bilaget til henstilling 2003/361/EF anvendes. Medlemsstaterne kan navnlig tage hensyn til, at en enhed er uafhængig af sine partnervirksomheder eller tilknyttede virksomheder med hensyn til de net- og informationssystemer, som enheden anvender i forbindelse med leveringen af sine tjenester, og med hensyn til de tjenester, som enheden leverer. På dette grundlag kan medlemsstaterne, hvor det er hensigtsmæssigt, anse en sådan enhed for ikke at udgøre en mellemstor virksomhed i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, eller for ikke at overskride tærsklerne for en mellemstor virksomhed fastsat i nævnte artikels stk. 1, hvis den pågældende enhed i betragtning af dennes grad af uafhængighed ikke ville være blevet anset for at udgøre en mellemstor virksomhed eller at overskride disse tærskler, hvis kun dens egne data var blevet taget i betragtning. Dette berører ikke forpligtelserne fastsat i dette direktiv for partnervirksomheder og tilknyttede virksomheder, som er omfattet af dette direktivs anvendelsesområde.

(17) Medlemsstaterne bør kunne bestemme, at enheder, der inden dette direktivs ikrafttræden er identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148, skal betragtes som væsentlige enheder.

(18) For at sikre et klart overblik over de enheder, der er omfattet af dette direktivs anvendelsesområde, bør medlemsstaterne udarbejde en liste over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester. Med henblik

herpå bør medlemsstaterne kræve, at enheder mindst indgiver følgende oplysninger til de kompetente myndigheder: navn, adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre for enheden, og i givet fald den relevante sektor og delsektor omhandlet i bilagene samt i givet fald en liste over de medlemsstater, hvor de leverer tjenester, der er omfattet af dette direktivs anvendelsesområde. Med henblik herpå bør Kommissionen med bistand fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) uden unødigt ophold fastlægge retningslinjer og skabeloner vedrørende forpligtelsen til at indgive oplysninger. For at lette udarbejdelsen og ajourføringen af listen over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester, bør medlemsstaterne kunne indføre nationale mekanismer, hvorigennem enheder kan registrere sig selv. Hvor der findes registre på nationalt plan, kan medlemsstaterne træffe afgørelse om passende mekanismer, der gør det muligt at identificere enheder, der er omfattet af dette direktivs anvendelsesområde.

(19) Medlemsstaterne bør være ansvarlige for mindst at oplyse Kommissionen om antallet af væsentlige og vigtige enheder for hver sektor og delsektor omhandlet i bilagene, samt give relevante oplysninger om antallet af identificerede enheder og den bestemmelse blandt dem, der er fastsat i dette direktiv, på grundlag af hvilken de blev identificeret og den type tjeneste de leverer. Medlemsstaterne opfordres til at udveksle oplysninger med Kommissionen om væsentlige og vigtige enheder og, i tilfælde af en omfattende cybersikkerhedshændelse, relevante oplysninger såsom navnet på den berørte enhed.

(20) Kommissionen bør i samarbejde med samarbejdsgruppen og efter høring af de relevante interessenter fastlægge retningslinjer for gennemførelsen af de kriterier, der gælder for mikrovirksomheder og små virksomheder, for vurderingen af, om de er omfattet af dette direktivs anvendelsesområde. Kommissionen bør også sikre, at der gives passende vejledning til mikrovirksomheder og små virksomheder, som hører under dette direktivs anvendelsesområde. Kommissionen bør med bistand fra medlemsstaterne stille oplysninger til rådighed for mikrovirksomheder og små virksomheder i denne henseende.

(21) Kommissionen vil kunne yde vejledning med henblik på at bistå medlemsstaterne med gennemførelse af dette direktivs bestem-

melser om anvendelsesområde og evaluering af proportionaliteten af de foranstaltninger, der skal træffes i henhold til dette direktiv, navnlig for så vidt angår enheder med komplekse forretningsmodeller eller driftsmiljøer, hvorved en enhed samtidig kunne opfylde de kriterier, der er tildelt både væsentlige og vigtige enheder, eller samtidig kunne udføre aktiviteter, hvoraf nogle falder inden for og nogle uden for dette direktivs anvendelsesområde.

(22) Dette direktiv fastsætter referencescenariet for foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser på tværs af de sektorer, der er omfattet af dets anvendelsesområde. For at undgå fragmentering af EU-retsakters cybersikkerhedsbestemmelser bør Kommissionen, hvor yderligere sektorspecifikke EU-retsakter vedrørende foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser vedrørende cybersikkerhed anses for nødvendige for at sikre et højt cybersikkerhedsniveau i hele Unionen, vurdere, hvorvidt sådanne yderligere bestemmelser vil kunne fastsættes i en gennemførelsesretsakt til dette direktiv. Er sådan en gennemførelsesretsakt ikke egnede til dette formål, vil sektorspecifikke EU-retsakter kunne bidrage til at sikre et højt cybersikkerhedsniveau i hele Unionen, samtidig med at der fuldt ud tages hensyn til de berørte sektorers specificiteter og kompleksiteter. Med henblik herpå er dette direktiv ikke til hinder for, at der vedtages yderligere sektorspecifikke EU-retsakter, der omhandler foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, der tager behørigt hensyn til behovet for en omfattende og sammenhængende ramme for cybersikkerhed. Dette direktiv berører ikke de eksisterende gennemførelsesbeføjelser, der er tillagt Kommissionen inden for en række sektorer, herunder transport og energi.

(23) Hvor en sektorspecifik EU-retsakt indeholder bestemmelser, der kræver, at væsentlige eller vigtige enheder træffer foranstaltninger til styring af cybersikkerhedsrisici eller underretter om væsentlige hændelser, og hvor disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, bør de pågældende bestemmelser, herunder om tilsyn og håndhævelse, finde anvendelse på sådanne enheder. Hvis en sektorspecifik EU-retsakt ikke omfatter alle enheder i en specifik sektor, der er omfattet af dette direktivs anvendelsesområde, bør de relevante bestemmelser i dette direktiv fortsat finde anvendelse på de enheder, der ikke er omfattet af nævnte retsakt.

(24) Hvor bestemmelser i en sektorspecifik EU-retsakt kræver, at væsentlige eller vigtige enheder overholder rapporteringsforpligtelser med en virkning, der mindst svarer til de rapporteringsforpligtelser, der er fastsat i dette direktiv, bør der sikres sammenhæng og effektivitet i håndteringen af hændelsesunderretninger. Med henblik herpå bør bestemmelserne vedrørende hændelsesunderretninger i den sektorspecifikke EU-retsakt give CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter for cybersikkerhed (det centrale kontaktpunkt) i henhold til dette direktiv øjeblikkelig adgang til de hændelsesunderretninger, der indgives i overensstemmelse med den sektorspecifikke EU-retsakt. En sådan øjeblikkelig adgang kan navnlig sikres, hvis hændelsesunderretninger uden unødigt ophold sendes til CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt i henhold til dette direktiv. Medlemsstaterne bør, hvor det er hensigtsmæssigt, indføre en automatisk og direkte rapporteringsmekanisme, der sikrer systematisk og øjeblikkelig udveksling af oplysninger med CSIRT'er, de kompetente myndigheder eller de centrale kontaktpunkter vedrørende håndtering af sådanne hændelsesunderretninger. Med henblik på at forenkle rapporteringen og gennemføre den automatiske og direkte rapporteringsmekanisme vil medlemsstaterne i overensstemmelse med den sektorspecifikke EU-retsakt kunne anvende et enkelt indgangspunkt.

(25) Sektorspecifikke EU-retsakter, der kræver foranstaltninger til styring af cybersikkerhedsrisici eller rapporteringsforpligtelser med en virkning, der mindst svarer til dem, der er fastsat i dette direktiv, vil kunne fastsætte, at de kompetente myndigheder i henhold til sådanne retsakter udøver deres tilsyns- og håndhævelsesbeføjelser i forbindelse med sådanne foranstaltninger eller forpligtelser med bistand fra de kompetente myndigheder i henhold til dette direktiv. De berørte kompetente myndigheder vil kunne etablere samarbejdsordninger med henblik herpå. Sådanne samarbejdsordninger vil bl.a. kunne præcisere procedurerne for koordinering af tilsynsaktiviteter, herunder procedurerne for undersøgelser og kontrol på stedet i overensstemmelse med national ret og en mekanisme for udveksling af relevante oplysninger om tilsyn og håndhævelse mellem de kompetente myndigheder, herunder adgang til cyberrelaterede oplysninger, som de kompetente myndigheder i henhold til dette direktiv anmoder om.

(26) Hvor sektorspecifikke EU-retsakter kræver eller skaber incitamenter for enheder til at underrette om væsentlige cybertrusler, bør medlemsstaterne også tilskynde til udveksling af væsentlige cybertrusler med CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv for at sikre, at disse organer i højere grad er opmærksomme på cybertrusselsbilledet, og for at sætte dem i stand til at reagere effektivt og rettidigt, såfremt de væsentlige cybertrusler bliver til virkelighed.

(27) Fremtidige sektorspecifikke EU-retsakter bør tage behørigt hensyn til de definitioner og tilsyns- og håndhævelsesrammer, der er fastsat i dette direktiv.

(28) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 ([10]) bør betragtes som en sektorspecifik EU-retsakt i forbindelse med dette direktiv for så vidt angår finansielle enheder. Bestemmelserne i forordning (EU) 2022/2554 om risikostyring inden for informations- og kommunikationsteknologi (IKT), styring af IKT-relaterede hændelser og navnlig indberetning af større IKT-relaterede hændelser, samt om test af digital operationel modstandsdygtighed, ordninger for udveksling af oplysninger og IKT-tredjepartsrisiko bør finde anvendelse i stedet for bestemmelserne i dette direktiv. Medlemsstaterne bør derfor ikke anvende bestemmelserne i dette direktiv om risikostyrings- og rapporterings forpligtelser vedrørende cybersikkerhed samt tilsyn og håndhævelse på finansielle enheder, der er omfattet af forordning (EU) 2022/2554. Samtidig er det vigtigt at opretholde stærke forbindelser og udveksle oplysninger med den finansielle sektor i henhold til dette direktiv. Med henblik herpå giver forordning (EU) 2022/2554 de europæiske tilsynsmyndigheder (ESA'erne) og de kompetente myndigheder i henhold til nævnte forordning mulighed for at deltage i samarbejdsgruppens aktiviteter samt udveksle oplysninger og samarbejde med de centrale kontaktpunkter såvel som CSIRT'erne og de kompetente myndigheder i henhold til dette direktiv. De kompetente myndigheder i henhold til forordning (EU) 2022/2554 bør også fremsende oplysninger om større IKT-relaterede hændelser og, hvor det er relevant, væsentlige cybertrusler til CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv. Dette kan opnås ved at sikre øjeblikkelig adgang til hændelsesunderretninger og videresende af dem enten direkte eller via et enkelt indgangspunkt. Desuden bør medlemsstaterne fortsat medtage den fi-

nansielle sektor i deres cybersikkerhedsstrategier, og CSIRT'er kan dække den finansielle sektor i deres aktiviteter.

(29)For at undgå huller mellem eller overlapning af cybersikkerhedsforpligtelser, der pålægges enheder i luftfartssektoren, bør nationale myndigheder i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 ([11]) og (EU) 2018/1139 ([12]), og de kompetente myndigheder i henhold til dette direktiv samarbejde om gennemførelsen af foranstaltninger til styring af cybersikkerhedsrisici og tilsynet med overholdelsen af disse foranstaltninger på nationalt plan. En enheds overholdelse af sikkerhedskravene i forordning (EF) nr. 300/2008 og (EU) 2018/1139 og i de relevante delegerede retsakter og gennemførelsesretsakter, der er vedtaget i henhold til nævnte forordninger, vil af de kompetente myndigheder i henhold til dette direktiv kunne anses for at udgøre opfyldelse af de tilsvarende krav, der er fastsat i dette direktiv.

(30)I betragtning af de indbyrdes forbindelser mellem cybersikkerhed og enheders fysiske sikkerhed bør der sikres en sammenhængende tilgang mellem Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 ([13]) og nærværende direktiv. Med henblik herpå bør enheder identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557 betragtes som væsentlige enheder i henhold til nærværende direktiv. Endvidere bør hver medlemsstat sikre, at dens nationale cybersikkerhedsstrategi skaber en politisk ramme for øget koordinering i nævnte medlemsstat mellem dens kompetente myndigheder i henhold til nærværende direktiv og dem i henhold til direktiv (EU) 2022/2557 i forbindelse med udveksling af oplysninger om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser samt om udøvelse af tilsynsopgaver. De kompetente myndigheder i henhold til nærværende direktiv og de i henhold til direktiv (EU) 2022/2557 bør samarbejde og udveksle oplysninger uden unødigt ophold, navnlig vedrørende identifikation af kritiske enheder, om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser, der påvirker kritiske enheder, herunder cybersikkerhedsforanstaltninger og fysiske foranstaltninger, der træffes af kritiske enheder, såvel som resultaterne af tilsynsaktiviteter, der udføres med hensyn til sådanne enheder.

For at strømline tilsynsaktiviteterne mellem de kompetente myndigheder i henhold til nærværende direktiv og i henhold til direktiv (EU) 2022/2557 og for at mindske den administrative byrde

mest muligt for de berørte enheder bør disse kompetente myndigheder desuden bestræbe sig på at harmonisere modeller til hændelsesunderretning og tilsynsprocesser. Hvor det er hensigtsmæssigt, bør de kompetente myndigheder i henhold til direktiv (EU) 2022/2557 kunne anmode de kompetente myndigheder i henhold til nærværende direktiv om at udøve deres tilsyns- og håndhævelsesbeføjelser med hensyn til en enhed, som er identificeret som en kritisk enhed i henhold til direktiv (EU) 2022/2557. De kompetente myndigheder i henhold til nærværende direktiv og de i henhold til direktiv (EU) 2022/2557 bør samarbejde og udveksle oplysninger, om muligt i realtid, med henblik herpå.

(31) Enheder, der tilhører sektoren for digital infrastruktur, er i det væsentlige baseret på net- og informationssystemer, og derfor bør de forpligtelser, der pålægges disse enheder i medfør af dette direktiv, på en omfattende måde omhandle sådanne systemers fysiske sikkerhed som led i deres foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser. Da disse spørgsmål er omfattet af dette direktiv, finder forpligtelserne i kapitel III, IV og VI i direktiv (EU) 2022/2557 ikke anvendelse på sådanne enheder.

(32) Opretholdelse og bevarelse af et pålideligt, modstandsdygtigt og sikkert domænenavnesystem (DNS) er afgørende faktorer for at bevare internettets integritet og er afgørende for dets fortsatte og stabile drift, som den digitale økonomi og det digitale samfund afhænger af. Derfor bør dette direktiv finde anvendelse på topdomænenavneadministratorer og DNS-tjenesteudbydere, der skal forstås som enheder, der leverer offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere eller autoritative domænenavnsoversættelsestjenester til tredjepartsbrug. Dette direktiv bør ikke finde anvendelse på rodnavneservere.

(33) Cloudcomputingtjenester bør omfatte digitale tjenester, der giver mulighed for on demand-administration og bred fjernadgang til en skalerbar og elastisk pulje af delbare computerressourcer, herunder hvor sådanne ressourcer er fordelt mellem flere lokaliteter. Computerressourcer omfatter ressourcer såsom netværk, servere og anden infrastruktur, operativsystemer, software, lagring, applikationer og tjenester. Tjenestemodellerne for cloudcomputing omfatter bl.a. infrastruktur som en service (IaaS), platform som en service (PaaS), software som en service (SaaS) og netværk som

en service (NaaS). Ibrugtagningsmodellerne for cloudcomputing bør omfatte privat, samfundsmæssig, offentlig og hybrid cloud. Cloudcomputingtjeneste- og ibrugtagningsmodellerne har samme betydning som de tjeneste- og ibrugtagningsmodeller, der er defineret i ISO/IEC 17788: 2014-standarden. Cloudcomputing-brugerens mulighed for ensidigt selvforsynende databehandlingskapacitet såsom servertid eller netlagring uden nogen menneskelig interaktion fra udbyderen af cloudcomputingtjenesters side kan beskrives som on demand-administration.

Udtrykket »bred fjernadgang« anvendes til at beskrive, at cloudkapaciteten leveres over nettet og tilgås gennem mekanismer, der fremmer brugen af heterogene tynde eller tykke klientplatforme, herunder mobiltelefoner, tablets, bærbare computere og arbejdsstationer. Udtrykket »skalerbar« henviser til databehandlingsressourcer, der fordeles fleksibelt af udbyderen af cloudcomputingtjenester, uanset ressourcernes geografiske placering, med henblik på at håndtere udsving i efterspørgslen. Udtrykket »elastisk pulje« bruges til at beskrive IT-ressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbyrden. Udtrykket »delbar« bruges til at beskrive IT-ressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme elektroniske udstyr. Udtrykket »distribueret« anvendes til at beskrive databehandlingsressourcer, der befinder sig på forskellige netforbundne computere eller enheder, og som kommunikerer og koordinerer indbyrdes ved at sende meddelelser.

(34) I lyset af fremkomsten af innovative teknologier og nye forretningsmodeller forventes nye cloudcomputingtjeneste- og ibrugtagningsmodeller at dukke op på markedet som reaktion på nye kundebehov. I den forbindelse kan cloudcomputingtjenester leveres i en meget distribueret form, endnu tættere på de steder, hvor dataene genereres eller indsamles, hvorved man bevæger sig væk fra den traditionelle model og i retning af en meget distribueret model (»edge computing«).

(35) Tjenester, der udbydes af datacentertjenesteudbydere, leveres ikke altid i form af cloudcomputingtjenester. Datacentre udgør derfor ikke altid en del af cloudcomputing-infrastrukturen. For at styre alle de risici, der er forbundet med sikkerheden i net- og in-

formationssystemer, bør dette direktiv derfor omfatte udbydere af datacentertjenester, som ikke er cloudcomputingtjenester. I dette direktiv bør begrebet »datacentertjeneste« omfatte levering af en tjeneste, der omfatter strukturer eller grupper af strukturer, der er beregnet til central opbevaring, sammenkobling og drift af informationsteknologi (IT) og netværksudstyr, der leverer datalagrings-, -behandlings- og -transporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol. Begrebet »datacentertjeneste« bør ikke finde anvendelse på interne datacentre, der ejes og drives af den berørte enhed til dets egne formål.

(36) Forskningsaktiviteter spiller en central rolle i udviklingen af nye produkter og processer. Mange af disse aktiviteter udføres af enheder, der deler, udbreder eller udnytter resultaterne af deres forskning til kommercielle formål. Disse enheder kan derfor være vigtige led i værdikæder, hvilket gør sikkerheden af deres net- og informationssystemer til en integreret del af det indre markeds overordnede cybersikkerhed. Begrebet »forskningsorganisationer« bør forstås som omfattende enheder, der primært beskæftiger sig med anvendt forskning eller udvikling i den i Organisationen for Økonomisk Samarbejde og Udviklings Frascati-manual fra 2015 (»Guidelines for Collecting and Reporting Data on Research and Experimental Development«) anvendte betydning med henblik på at udnytte resultaterne heraf til kommercielle formål såsom fremstilling eller udvikling af et produkt eller proces, levering af en tjeneste eller markedsføringen heraf.

(37) Den voksende indbyrdes afhængighed er resultatet af et stadig mere grænseoverskridende og indbyrdes afhængigt net af tjenester, der anvender centrale infrastrukturer i hele Unionen inden for sektorer såsom energi, transport, digital infrastruktur, drikkevand og spildevand, sundhed, visse aspekter af offentlig forvaltning samt rummet, for så vidt angår levering af visse tjenester, der er afhængige af jordbaserede infrastrukturer, som ejes, forvaltes og drives enten af medlemsstaterne eller af private parter, men ikke infrastruktur, der ejes, forvaltes eller drives af eller på vegne af Unionen som en del af dens rumprogram. Disse indbyrdes afhængighedsforhold betyder, at enhver afbrydelse, selv en, der oprindeligt var begrænset til én enhed eller én sektor, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for leveringen af tjenester i hele det indre marked. De intensiverede cyberangreb under

covid-19-pandemien har vist stadig mere indbyrdes afhængige samfunds sårbarhed over for risici med lav sandsynlighed.

(38) I betragtning af forskellene i de nationale forvaltningsstrukturer og for at beskytte allerede eksisterende sektorspecifikke ordninger eller Unionens tilsyns- og kontrolorganer bør medlemsstaterne kunne udpege eller oprette én eller flere nationale kompetente myndigheder med ansvar for cybersikkerhed og for tilsynsopgaverne i henhold til dette direktiv.

(39) For at lette grænseoverskridende samarbejde og kommunikation mellem myndigheder og muliggøre en effektiv gennemførelse af dette direktiv er det nødvendigt, at hver medlemsstat udpeger et centralt kontaktpunkt med ansvar for koordinering af spørgsmål vedrørende sikkerheden i net- og informationssystemer og grænseoverskridende samarbejde på EU-plan.

(40) De centrale kontaktpunkter bør sikre et effektivt grænseoverskridende samarbejde med andre medlemsstaters relevante myndigheder og, hvor det er relevant, med Kommissionen og ENISA. De centrale kontaktpunkter bør derfor efter anmodning fra CSIRT'en eller den kompetente myndighed have til opgave at videresende underretninger om væsentlige hændelser med grænseoverskridende virkninger til de centrale kontaktpunkter i andre berørte medlemsstater. På nationalt plan bør de centrale kontaktpunkter muliggøre et gnidningsløst tværsektorielt samarbejde med andre kompetente myndigheder. De centrale kontaktpunkter kan også være adressaterne for relevante oplysninger om hændelser vedrørende finansielle enheder fra de kompetente myndigheder i henhold til forordning (EU) 2022/2554, som de i givet fald bør kunne fremsende til CSIRT'erne eller de kompetente myndigheder i henhold til dette direktiv.

(41) Medlemsstaterne bør være tilstrækkelig udstyret med både teknisk og organisatorisk kapacitet til at forebygge, opdage, reagere på og reetablere sig efter hændelser og risici og afbøde deres virkninger. Medlemsstaterne bør derfor oprette eller udpege en eller flere CSIRT'er i henhold til dette direktiv og sikre, at de har tilstrækkelige ressourcer og tekniske kapaciteter. CSIRT'erne bør opfylde kravene, der er fastsat i dette direktiv, med henblik på at sikre effektive og kompatible kapaciteter til at håndtere hændelser og risici og til at sikre et effektivt samarbejde på EU-plan. Medlemsstaterne bør kunne udpege eksisterende IT-beredskabsenhe-

der (CERT'er) som CSIRT'er. Med henblik på at styrke tillidsforholdet mellem enhederne og CSIRT'erne bør medlemsstaterne, hvor en CSIRT er en del af en kompetent myndighed, kunne overveje en funktionel adskillelse mellem CSIRT'ernes operationelle opgaver, navnlig i forbindelse med udveksling af oplysninger og støtte til enhederne, og de kompetente myndigheders tilsynsaktiviteter.

(42) CSIRT'erne har til opgave at håndtere hændelser. Dette omfatter behandling af store mængder til tider følsomme oplysninger. Medlemsstaterne bør sikre, at CSIRT'erne har en infrastruktur til udveksling og behandling af oplysninger samt veludstyrede medarbejdere, hvilket sikrer fortroligheden og pålideligheden af deres operationer. CSIRT'erne vil også kunne vedtage adfærdskodekser i den henseende.

(43) For så vidt angår personoplysninger bør CSIRT'erne i overensstemmelse med forordning (EU) 2016/679 efter anmodning fra en væsentlig eller vigtig enhed være i stand til at foretage en proaktiv scanning af de net- og informationssystemer, der anvendes til levering af enhedens tjenester. I givet fald bør medlemsstaterne tilstræbe at sikre et ensartet niveau af teknisk kapacitet for alle sektorspecifikke CSIRT'er. Medlemsstaterne bør kunne anmode ENISA om bistand til at udvikle deres CSIRT'er.

(44) CSIRT'erne bør være i stand til på anmodning fra en væsentlig eller vigtig enhed at overvåge de af enhedens aktiver, der har internetopkobling, både i og uden for enhedens lokaler, for at kortlægge, forstå og styre enhedens samlede organisatoriske risici hvad angår nyopdagede trusler fra forsyningskæden eller kritiske sårbarheder. Enheden bør tilskyndes til at meddele CSIRT'en, hvorvidt den driver en privilegeret forvaltningsgrænseflade, da dette vil kunne påvirke hastigheden af gennemførelsen af afbødende foranstaltninger.

(45) I betragtning af betydningen af internationalt samarbejde om cybersikkerhed bør CSIRT'erne kunne deltage i internationale samarbejdsnetværk i tillæg til det CSIRT-netværk, der oprettes ved dette direktiv. Med henblik på udførelsen af deres opgaver bør CSIRT'erne og de kompetente myndigheder derfor kunne udveksle oplysninger, herunder personoplysninger, med nationale enheder i tredjelande, der håndterer IT-sikkerhedshændelser, eller tredjelandes kompetente myndigheder, forudsat at betingelserne i

henhold til EU-databeskyttelsesretten for overførsel af personoplysninger til tredjelande, bl.a. betingelserne i artikel 49 i forordning (EU) 2016/679, er opfyldt.

(46) Det er afgørende at sikre tilstrækkelige ressourcer til at opfylde målene i dette direktiv og gøre det muligt for de kompetente myndigheder og CSIRT'erne udføre opgaverne heri. Medlemsstaterne kan på nationalt plan indføre en finansieringsmekanisme til dækning af de nødvendige udgifter i forbindelse med udførelsen af opgaver, der påhviler offentlige enheder med ansvar for cybersikkerhed i medlemsstaten i henhold til dette direktiv. En sådan mekanisme bør overholde EU-retten og bør være forholdsmæssig og ikkediskriminerende og bør tage hensyn til forskellige tilgange til levering af sikre tjenester.

(47) CSIRT-netværket bør fortsat bidrage til at styrke fortroligheden og tilliden og til at fremme hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne. For at styrke det operationelle samarbejde på EU-plan bør CSIRT-netværket overveje at indbyde EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europol, til at deltage i sit arbejde.

(48) Med henblik på at opnå og opretholde et højt cybersikkerhedsniveau bør de nationale cybersikkerhedsstrategier, der kræves i henhold til dette direktiv, bestå af sammenhængende rammer med strategiske mål og prioriteter på cybersikkerhedsområdet og den styring, der skal til for at nå dem. Disse strategier kan bestå af et eller flere lovgivningsmæssige eller ikkelovgivningsmæssige instrumenter.

(49) Cyberhygiejnepolitikker danner grundlaget for beskyttelse af net- og informationssysteminfrastrukturer, sikkerheden af hardware, software og onlineapplikationer samt virksomheds- eller slutbrugerdata, som enhederne er afhængige af. Cyberhygiejnepolitikker med et fælles grundsæt af praksisser, herunder software- og hardwareopdateringer, ændringer af passwords, styring af nye installeringer, begrænsning af adgangskonti på administratorniveau og backup af data, fremmer en proaktiv ramme for beredskab og generel sikkerhed i tilfælde af hændelser eller cybertrusler. ENISA bør overvåge og analysere medlemsstaternes cyberhygiejne politikker.

(50) Bevidsthed om cybersikkerhed og cyberhygiejne er afgørende for at forbedre cybersikkerhedsniveauet i Unionen, navnlig i lyset af

det stigende antal forbundne enheder, der i stigende grad anvendes til cyberangreb. Der bør gøres en indsats for at øge den generelle bevidsthed om risici i forbindelse med sådant udstyr, mens vurderinger på EU-plan vil kunne bidrage til at sikre en fælles forståelse af sådanne risici inden for det indre marked.

(51) Medlemsstaterne bør tilskynde til anvendelse af enhver form for innovativ teknologi, herunder kunstig intelligens, hvis anvendelse kan forbedre opdagelsen og forebyggelsen af cyberangreb og gøre det muligt at omdirigere ressourcer til cyberangreb mere effektivt. Medlemsstaterne bør derfor i deres nationale cybersikkerhedsstrategi tilskynde til aktiviteter inden for forskning og udvikling for at lette anvendelsen af sådanne teknologier, navnlig dem, der vedrører automatiserede eller halvautomatiske værktøjer inden for cybersikkerhed, og, hvor det er relevant, deling af data, der er nødvendige for at uddanne brugerne af en sådan teknologi og forbedre den. Anvendelsen af enhver innovativ teknologi, herunder kunstig intelligens, bør overholde EU-databeskyttelsesretten, herunder databeskyttelsesprincipperne om datanøjagtighed, dataminimering, rimelighed og gennemsigtighed samt datasikkerhed såsom kryptering på det aktuelle teknologiske stade. Kravene om databeskyttelse gennem design og gennem standardindstillinger, der er fastsat i forordning (EU) 2016/679, bør udnyttes fuldt ud.

(52) Open source-cybersikkerhedsværktøjer og -applikationer kan bidrage til en højere grad af åbenhed og kan have en positiv indvirkning på effektiviteten af industriel innovation. Åbne standarder fremmer interoperabiliteten mellem sikkerhedsværktøjer, hvilket gavner industrielle interessenters sikkerhed. Open source-cybersikkerhedsværktøjer og -applikationer kan fungere som løftestang for det bredere udviklersamfund og give mulighed for leverandørdiversificering. Open source kan føre til en mere gennemsigtig proces for kontrol af cybersikkerhedsrelaterede værktøjer og en brugerdrevet proces for opdagelse af sårbarheder. Medlemsstaterne bør derfor kunne fremme anvendelsen af open source-software og åbne standarder ved at føre politikker vedrørende brugen af åbne data og open source som en del af konceptet »sikkerhed gennem gennemsigtighed«. Politikker, der fremmer indførelse og bæredygtig anvendelse af open source-cybersikkerhedsværktøjer, er af særlig betydning for små og mellemstore virksomheder, der står med høje gennemførelsesomkostninger, som kan

reduceres ved at mindske behovet for bestemte applikationer eller værktøjer.

(53)Forsyningsselskaberne er i stigende grad forbundet med digitale netværk i byerne med henblik på at forbedre byernes transportnet, opgradere vandforsynings- og affaldsbortskaffelsesfaciliteter og øge effektiviteten af belysning og opvarmning af bygninger. Disse digitaliserede forsyningsvirksomheder er sårbare over for cyberangreb og risikerer i tilfælde af et vellykket cyberangreb at skade borgerne i stor skala på grund af deres indbyrdes forbundethed. Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategi udvikle en politik, der tager højde for udviklingen af sådanne forbundne eller intelligente byer og deres potentielle indvirkning på samfundet.

(54)I de senere år har Unionen oplevet en eksponentiel stigning i antallet af ransomwareangreb, hvor malware krypterer data og systemer og kræver betaling af løsepenge for at dekryptere dem. Den stigende hyppighed og alvor af ransomware-angreb kan være drevet af flere faktorer såsom forskellige angrebsmønstre, kriminelle forretningsmodeller omkring »ransomware som en service« og kryptovalutaer, krav om løsepenge og stigningen i angreb i forsyningskæden. Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategi udvikle en politik til håndtering af stigningen i antallet af ransomware-angreb.

(55)Offentlig-private partnerskaber (OPP'er) inden for cybersikkerhed kan skabe en passende ramme for udveksling af viden, deling af bedste praksis og etablering af et fælles forståelsesniveau blandt interessenter. Medlemsstaterne bør fremme politikker til støtte for oprettelsen af cybersikkerhedsspecifikke OPP'er. Disse politikker bør bl.a. klarlægge anvendelsesområdet og de involverede interessenter, styringsmodellen, de tilgængelige finansieringsmuligheder og samspillet mellem de deltagende interessenter med hensyn til OPP'er. OPP'er kan udnytte ekspertisen i enheder inden for den private sektor med henblik på at bistå de kompetente myndigheder i udviklingen af tjenester og processer på det aktuelle teknologiske stade, herunder udveksling af oplysninger, tidlig varsling, cybertrussels- og -hændelsesøvelser, krisestyring og planlægning af modstandsdygtighed.

(56)Medlemsstaterne bør i deres nationale cybersikkerhedsstrategier tackle små og mellemstore virksomheders specifikke cybersikker-

hedsbehov. Små og mellemstore virksomheder udgør på tværs af Unionen en stor procentdel af industri- og forretningsmarkedet og kæmper ofte med at tilpasse sig nye forretningspraksisser i en mere forbundet verden og til det digitale miljø, hvor medarbejdere arbejder hjemmefra, og forretning i stigende grad drives online. Nogle små og mellemstore virksomheder står over for specifikke cybersikkerhedsudfordringer, såsom ringe cyberbevidsthed, manglende IT-sikkerhed i forbindelse med fjernarbejde, de store omkostninger forbundet med cybersikkerhedsløsninger og et øget trusselsniveau, som f.eks. ransomware, som de bør modtage vejledning i og assistance til. Små og mellemstore virksomheder er i stigende grad mål for angreb i forsyningskæden på grund af deres mindre strenge foranstaltninger til styring af cybersikkerhedsrisici og angrebsstyring, samt det faktum at de har begrænsede sikkerhedsressourcer. Sådanne angreb i forsyningskæden har ikke kun indvirkning på små og mellemstore virksomheder og deres aktiviteter isoleret set, men kan også have en kaskadevirkning på større angreb på enheder, som de leverede varer til. Medlemsstaterne bør gennem deres nationale cybersikkerhedsstrategier hjælpe små og mellemstore virksomheder med at tackle de udfordringer, de står over for i deres forsyningskæder. Medlemsstaterne bør have et kontaktpunkt for små og mellemstore virksomheder på nationalt eller regionalt plan, som enten yder vejledning og bistand til små og mellemstore virksomheder eller retter dem mod de relevante organer med henblik på vejledning og bistand med hensyn til cybersikkerhedsrelaterede spørgsmål. Medlemsstaterne tilskyndes også til at tilbyde tjenester såsom webstedskonfigurering og muliggørelse af logning til mikrovirksomheder og små virksomheder, der mangler disse kapaciteter.

(57) Medlemsstaterne bør som led i deres nationale cybersikkerhedsstrategier vedtage politikker til fremme af aktiv cyberbeskyttelse som led i en bredere defensiv strategi. Snarere end at svare reaktivt består aktiv cyberbeskyttelse i forebyggelse, opdagelse, overvågning, analyse og afbødning af brud på netsikkerheden på en aktiv måde kombineret med anvendelse af kapaciteter i og uden for det net, der angribes. Dette vil kunne omfatte medlemsstater, der tilbyder gratis tjenester eller værktøjer til visse enheder, herunder selvbetjeningskontrol, opdagelsesværktøjer og fjernelsestjenester. Evnen til hurtigt og automatisk at udveksle og forstå trusselsoplysninger og -analyser, cyberaktivitetsalarmer og reak-

tionsforanstaltninger er helt afgørende for at muliggøre en forenet indsats med hensyn til på vellykket vis at forebygge, opdage, imødegå og blokere angreb på net- og informationssystemer. Aktiv cyberbeskyttelse er baseret på en defensiv strategi, der udelukker offensive foranstaltninger.

(58) Eftersom udnyttelsen af sårbarheder i net- og informationssystemer kan forårsage betydelige forstyrrelser og skader, er hurtig identifikation og afhjælpning af sådanne sårbarheder en vigtig faktor med hensyn til at reducere risici. Enheder, der udvikler eller administrerer net- og informationssystemer, bør derfor indføre passende procedurer til håndtering af sårbarheder, når de opdages. Da sårbarheder ofte opdages og offentliggøres af tredjeparter, bør producenten eller udbyderen af IKT-produkter eller -tjenester også indføre de nødvendige procedurer for at modtage sårbarhedsoplysninger fra tredjeparter. I den forbindelse indeholder de internationale standarder ISO/IEC 30111 og ISO/IEC 29147 vejledning om henholdsvis håndtering af sårbarheder og offentliggørelse af sårbarheder. Styrkelse af koordineringen mellem de underrettende fysiske og juridiske personer og producenter eller udbydere af IKT-produkter eller -tjenester er særlig vigtig med henblik på at lette den frivillige ramme for offentliggørelse af sårbarheder. Koordineret offentliggørelse af sårbarheder angiver en struktureret proces, hvorigennem sårbarheder rapporteres til producenten eller leverandøren af potentielt sårbare IKT-produkter eller -tjenester på en måde, der gør det muligt for den at diagnosticere og afhjælpe sårbarheden, inden detaljerede sårbarhedsoplysninger offentliggøres for tredjeparter eller offentligheden. Koordineret offentliggørelse af sårbarheder bør også omfatte koordinering mellem den rapporterende fysiske eller juridiske person og producenten eller leverandøren af de potentielt sårbare IKT-produkter eller -tjenester med hensyn til tidspunktet for afhjælpning og offentliggørelse af sårbarheder.

(59) Kommissionen, ENISA og medlemsstaterne bør fortsat fremme tilpasning til internationale standarder og industriens eksisterende bedste praksis på området for styring af cybersikkerhedsrisici, f.eks. inden for sikkerhedsvurderinger af forsyningskæden, udveksling af oplysninger og offentliggørelse af sårbarheder.

(60) Medlemsstaterne bør i samarbejde med ENISA træffe foranstaltninger til at fremme koordineret offentliggørelse af sårbarheder ved at fastlægge en relevant national politik. Som led i deres na-

tionale politik bør medlemsstaterne så vidt muligt tackle de udfordringer, som sårbarhedsforskere står over for, herunder deres potentielle strafansvar, i overensstemmelse med nationale ret. Eftersom fysiske og juridiske personer, der forsker i sårbarheder, i nogle medlemsstater vil kunne blive udsat for strafferetligt og civilretligt ansvar, opfordres medlemsstaterne til at vedtage retningslinjer for ikke-retsforfølgelse af informationssikkerhedsforskere og en fritagelse for civilretligt ansvar for deres aktiviteter.

(61) Medlemsstaterne bør udpege en af deres CSIRT'er som koordinator med henblik på at fungere som betroet formidler mellem de rapporterende fysiske eller juridiske personer og producenterne eller udbyderne af IKT-produkter eller -tjenester, som sandsynligvis vil blive berørt af sårbarheden, hvor det er nødvendigt. Den CSIRT, der er udpeget som koordinator, bør bl.a. have til opgave at identificere og kontakte de berørte enheder, at bistå de fysiske eller juridiske personer, der rapporterer en sårbarhed, at forhandle tidsfrister for offentliggørelse og at håndtere sårbarheder, der påvirker flere enheder (koordineret offentliggørelse af sårbarheder med flere parter). Hvor den rapporterede sårbarhed vil kunne have væsentlig indvirkning på enheder i mere end én medlemsstat, bør de CSIRT'er, der er udpeget som koordinatorer, i givet fald samarbejde inden for CSIRT-netværket.

(62) Adgang til korrekte og rettidige oplysninger om sårbarheder, der påvirker IKT-produkter og -tjenester, bidrager til en forbedret styring af cybersikkerhedsrisici. Kilder til offentligt tilgængelige oplysninger om sårbarheder er et vigtigt redskab for enhederne og for brugerne af deres tjenester, men også for de kompetente myndigheder og CSIRT'erne. Derfor bør ENISA oprette en europæisk sårbarhedsdatabase, hvor enheder, uanset om de er omfattet af dette direktiv, og deres leverandører af net- og informationssystemer samt de kompetente myndigheder og CSIRT'erne på frivillig basis kan offentliggøre og registrere offentligt kendte sårbarheder med henblik på at give brugerne mulighed for at træffe passende afbødende foranstaltninger. Formålet med denne database er at tackle de unikke udfordringer, som risiciene udgør for enheder i Unionen. ENISA bør desuden fastlægge en passende procedure for offentliggørelsesprocessen for at give enhederne tid til at træffe afbødende foranstaltninger med hensyn til deres sårbarhed og anvende foranstaltninger på det aktuelle teknologiske stade til styring af cybersikkerhedsrisici samt maskinlæsbare datasæt og

tilhørende grænseflader. For at fremme en kultur med offentliggørelse af sårbarheder bør offentliggørelse ikke have nogen negativ effekt for den rapporterende fysiske eller juridiske person.

(63) Selv om der findes lignende sårbarhedsregistre eller -databaser, hostes og vedligeholdes disse af enheder, der ikke er etableret i Unionen. En europæisk sårbarhedsdatabase, der vedligeholdes af ENISA, vil give større gennemsigtighed med hensyn til offentliggørelsesprocessen, inden sårbarheden offentliggøres, og modstandsdygtighed i tilfælde af en forstyrrelse eller en afbrydelse af leveringen af tilsvarende tjenester. For i videst muligt omfang at undgå dobbeltarbejde og tilstræbe komplementaritet bør ENISA undersøge muligheden for at indgå strukturerede samarbejdsaftaler med lignende registre eller databaser, der henhører under tredjelandes jurisdiktioner. ENISA bør navnlig undersøge muligheden for et tæt samarbejde med operatørerne af det fælles sårbarheds- og eksponeringssystem (CVE).

(64) Samarbejdsgruppen bør støtte og lette strategisk samarbejde og udvekslingen af oplysninger samt styrke tilliden og fortroligheden blandt medlemsstaterne. Samarbejdsgruppen bør udarbejde et arbejdsprogram hvert andet år. Arbejdsprogrammet bør omfatte de foranstaltninger, som samarbejdsgruppen skal gennemføre for at nå sine mål og udføre sine opgaver. Tidsrammen for fastlæggelsen af det første arbejdsprogram i henhold til dette direktiv bør tilpasses tidsrammen for det sidste arbejdsprogram, der blev fastlagt i henhold til direktiv (EU) 2016/1148, for at undgå potentielle forstyrrelser af samarbejdsgruppens arbejde.

(65) Når samarbejdsgruppen udarbejder vejledningsdokumenter, bør den konsekvent kortlægge nationale løsninger og erfaringer, vurdere virkningen af samarbejdsgruppens resultater på nationale tilgange, drøfte gennemførelsesudfordringer og formulere specifikke anbefalinger, navnlig om at lette harmonisering af gennemførelsen af dette direktiv blandt medlemsstaterne, som skal håndteres gennem bedre gennemførelse af eksisterende regler. Samarbejdsgruppen vil også kunne kortlægge de nationale løsninger for at fremme foreneligheden af de cybersikkerhedsløsninger, der anvendes i hver enkelt specifik sektor i hele Unionen. Dette er særligt relevant for sektorer med en international eller grænseoverskridende karakter.

(66) Samarbejdsgruppen bør fortsat være et fleksibelt forum og være i stand til at reagere på skiftende og nye politiske prioriteter og udfordringer, samtidig med at der tages hensyn til de disponible ressourcer. Den vil kunne tilrettelægge regelmæssige fælles møder med relevante private interessenter fra hele Unionen for at drøfte samarbejdsgruppens aktiviteter og indsamle data og input om nye politiske udfordringer. Derudover bør samarbejdsgruppen foretage en regelmæssig vurdering af situationen med hensyn til cybertrusler eller hændelser såsom ransomware. For at styrke samarbejdet på EU-plan bør samarbejdsgruppen overveje at indbyde de relevante EU-institutioner, -organer, -kontorer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Europa-Parlamentet, Europol, Det Europæiske Databeskyttelsesråd, Den Europæiske Unions Luftfartssikkerhedsagentur, oprettet ved forordning (EU) 2018/1139, og Den Europæiske Unions Agentur for Rumprogrammet, oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/696 ([14]), til at deltage i sit arbejde.

(67) De kompetente myndigheder og CSIRT'erne bør kunne deltage i udvekslingsordninger for embedsmænd fra andre medlemsstater inden for specifikke rammer og i givet faldmed forbehold for den påkrævede sikkerhedsgodkendelse af embedsmænd, der deltager i sådanne udvekslingsordninger, med henblik på at forbedre samarbejdet og styrke tilliden medlemsstaterne imellem. De kompetente myndigheder bør træffe de foranstaltninger, der er nødvendige for at sætte embedsmænd fra andre medlemsstater i stand til at spille en effektiv rolle i den kompetente myndigheds eller CSIRT-værtens aktiviteter.

(68) Medlemsstaterne bør bidrage til oprettelsen af EU-krisereaktionsrammen for cybersikkerhed som fastsat i Kommissionens henstilling (EU) 2017/1584 ([15]) gennem de eksisterende samarbejdsnetværk, navnlig det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe), CSIRT-netværket og samarbejdsgruppen. EU-CyCLONe og CSIRT-netværket bør samarbejde på grundlag af proceduremæssige ordninger, der fastlægger den nærmere udformning af dette samarbejde, og undgå dobbeltarbejde. EU-CyCLONe's forretningsorden bør yderligere præcisere, hvordan dette netværk bør fungere, herunder netværkets roller, metoder for samarbejde, interaktion med andre relevante aktører og skabeloner for udveksling af oplysninger samt kommunikationsmidler. Med hensyn til krisestyring på EU-plan bør de re-

levante parter støtte sig til EU's integrerede ordninger for politisk kriserespons i henhold til Rådets gennemførelsesafgørelse (EU) 2018/1993 ([16]) (IPCR-ordningerne). Kommissionen bør anvende den tværsektorielle krisekoordinationsproces på højt niveau, ARGUS, til dette formål. Hvis krisen har en vigtig ekstern dimension eller berører den fælles sikkerheds- og forsvarspolitik, bør EU-Udenrigstjenestens krisereaktionsmekanisme aktiveres.

(69) I overensstemmelse med bilaget til henstilling (EU) 2017/1584 bør en omfattende cybersikkerhedshændelse forstås som en hændelse, der forårsager en forstyrrelse på et niveau, der overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to medlemsstater. Alt efter årsag og virkning kan omfattende cybersikkerhedshændelser eskalere og udvikle sig til fuldgyldige kriser, der forhindrer det indre markeds korrekte funktion eller udgør alvorlige risici for den offentlige sikkerhed for enheder eller borgere i flere medlemsstater eller for Unionen som helhed. I betragtning af sådanne begivenheders vidtrækkende omfang og i de fleste tilfælde grænseoverskridende karakter bør medlemsstaterne og de relevante EU-institutioner, -organer, -kontorer og -agenturer samarbejde på teknisk, operationelt og politisk plan for at koordinere indsatsen i hele Unionen.

(70) Omfattende cybersikkerhedshændelser og kriser på EU-plan kræver en koordineret indsats for at sikre en hurtig og effektiv reaktion på grund af den store indbyrdes afhængighed mellem sektorer og medlemsstater. Tilgængeligheden af cybermodstandsdygtige net- og informationssystemer og tilgængeligheden, fortroligheden og integriteten af data er afgørende for Unionens sikkerhed og for beskyttelsen af dens borgere, virksomheder og institutioner mod hændelser og cybertrusler samt for at øge enkeltpersoners og organisationers tillid til Unionens evne til at fremme og beskytte et globalt, åbent, frit, stabilt og sikkert cyberspace baseret på menneskerettigheder, grundlæggende frihedsrettigheder, demokrati og retsstatsprincippet.

(71) EU-CyCLONe bør fungere som en formidler mellem det tekniske og det politiske niveau under omfattende cybersikkerhedshændelser og kriser og bør styrke samarbejdet på operationelt plan og støtte beslutningstagningen på politisk plan. I samarbejde med Kommissionen og under hensyntagen til Kommissionens kompetence på krisestyringsområdet bør EU-CyCLONe bygge videre på CSIRT-netværkets resultater og anvende sin egen kapacitet til at

udarbejde konsekvensanalyser af omfattende cybersikkerhedshændelser og kriser.

(72) Cyberangreb er af grænseoverskridende karakter, og en væsentlig hændelse kan forstyrre og skade kritiske informationsinfrastrukturer, som det indre markeds funktion afhænger af. Henstilling (EU) 2017/1584 omhandler alle relevante aktørers rolle. Desuden er Kommissionen inden for rammerne af EU-civilbeskyttelsesmekanismen, der blev oprettet ved Europa-Parlamentets og Rådets afgørelse 1313/2013/EU ([17]), ansvarlig for generelle beredskabstiltag, herunder forvaltning af katastrofeberedskabskoordinationscentret og det fælles varslings- og informationssystem, opretholdelse og videreudvikling af situationsbevidsthed og analysekapacitet, og tilvejebringelse og forvaltning af kapaciteten til at mobilisere og udsende eksperthold i tilfælde af en anmodning om bistand fra en medlemsstat eller et tredjeland. Kommissionen er også ansvarlig for at udarbejde analytiske rapporter om IPCR-ordningerne i henhold til gennemførelsesafgørelse (EU) 2018/1993, herunder i forbindelse med situationsbevidsthed og beredskab vedrørende cybersikkerhed samt for situationsbevidsthed og kriserespons inden for landbrug, ugunstige vejrforhold, konfliktkortlægning og -prognoser, systemer for tidlig varsling i forbindelse med naturkatastrofer, sundhedskriser, overvågning af infektionssygdomme, plantesundhed, kemiske hændelser, fødevare- og fodersikkerhed, dyresundhed, migration, told, nukleare og radiologiske kriser og energi.

(73) Unionen kan, hvor det er hensigtsmæssigt, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, som giver mulighed for og tilrettelægger disses deltagelse i bestemte aktiviteter, der foretages af samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe. Sådanne aftaler bør sikre Unionens interesser og tilstrækkelig databeskyttelse. Dette bør ikke udelukke medlemsstaternes ret til at samarbejde med tredjelande om håndtering af sårbarheder og styring af cybersikkerhedsrisici og lette rapportering og generel udveksling af oplysninger i overensstemmelse med EU-retten.

(74) For at lette en effektiv gennemførelse af dette direktiv, herunder med hensyn til håndtering af sårbarheder, foranstaltninger til styring af cybersikkerhedsrisici, rapporteringsforpligtelser og ordninger for udveksling af cybersikkerhedsoplysninger, kan med-

lemsstaterne samarbejde med tredjelande og gennemføre aktiviteter, der anses for hensigtsmæssige til dette formål, herunder udveksling af oplysninger om cybertrusler, hændelser, sårbarheder, værktøjer og metoder, taktikker, teknikker og procedurer, beredskab og øvelser i forbindelse med styring af cybersikkerhedskriser, uddannelse, tillidsskabende tiltag og strukturerede ordninger til udveksling af oplysninger.

(75) Der bør indføres peerevalueringer for at gøre det lettere at lære af fælles erfaringer, styrke gensidig tillid og opnå et højt fælles cybersikkerhedsniveau. Peerevalueringer kan føre til værdifuld indsigt og anbefalinger, der kan styrke de overordnede cybersikkerhedskapaciteter, skabe en ny funktionel kanal for udveksling af bedste praksis på tværs af medlemsstaterne og bidrage til at højne medlemsstaternes modenhedsniveauer for så vidt angår cybersikkerhed. Desuden bør peerevalueringer tage hensyn til resultaterne af lignende mekanismer, såsom CSIRT-netværkets peerevalueringssystem, og bør tilføre merværdi og undgå dobbeltarbejde. Gennemførelsen af peerevalueringer bør ikke berøre EU-retten eller national ret om beskyttelse af fortrolige eller klassificerede oplysninger.

(76) Samarbejdsgruppen bør fastlægge en selvevalueringsmetode for medlemsstaterne med henblik på at dække faktorer såsom graden af gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, kapacitetsniveauet og effektiviteten af udførelsen af de kompetente myndigheders opgaver, CSIRT'ernes operationelle kapacitet, graden af gennemførelse af gensidig bistand, graden af gennemførelse af ordningerne for udveksling af cybersikkerhedsoplysninger eller specifikke spørgsmål af grænseoverskridende eller tværsektoriel karakter. Medlemsstaterne bør tilskyndes til at foretage selvevalueringer regelmæssigt og til at fremlægge og drøfte resultaterne heraf i samarbejdsgruppen.

(77) Ansvaret for at sikre sikkerheden i net- og informationssystemer ligger i vid udstrækning hos væsentlige og vigtige enheder. En risikostyringskultur, der indbefatter risikovurderinger og gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici, som står i forhold til de foreliggende risici, bør fremmes og udvikles.

(78) Foranstaltningerne til styring af cybersikkerhedsrisici bør tage hensyn til den væsentlige eller vigtige enheds grad af afhængighed

af net- og informationssystemer og omfatte foranstaltninger til at identificere alle risici for hændelser, til at forebygge, opdage, reagere på og reetablere sig efter hændelser og til at afbøde deres indvirkning. Sikkerheden i net- og informationssystemer bør omfatte lagrede, overførte og behandlede datas sikkerhed. Foranstaltningerne til styring af cybersikkerhedsrisici bør omfatte en systemisk analyse, som tager højde for den menneskelige faktor, for at få et fuldstændigt billede af sikkerheden af net- og informationssystemet.

(79) Da trusler mod sikkerheden i net- og informationssystemer kan have forskellig oprindelse, bør foranstaltninger til styring af cybersikkerhedsrisici bygge på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod enhver begivenhed såsom tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller uautoriseret fysisk adgang til, beskadigelse af eller indgreb i en væsentlig eller vigtig enheds informations- og informationsbehandlingsfaciliteter, som kan kompromittere tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemerne. Foranstaltningerne til styring af cybersikkerhedsrisici bør derfor også adressere den fysiske og miljømæssige sikkerhed i net- og informationssystemerne ved at inkludere foranstaltninger til beskyttelse af sådanne systemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener i overensstemmelse med europæiske og internationale standarder såsom dem, der indgår i ISO/IEC 27000-serien. Væsentlige og vigtige enheder bør med henblik herpå som led i deres foranstaltninger til styring af cybersikkerhedsrisici også adressere sikkerheden vedrørende menneskelige ressourcer og indføre passende adgangskontrolpolitikker. Disse foranstaltninger bør være forenelige med direktiv (EU) 2022/2557.

(80) Med henblik på at påvise overensstemmelse med foranstaltninger til styring af cybersikkerhedsrisici og i mangel af passende europæiske cybersikkerhedscertificeringsordninger vedtaget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([18]) bør medlemsstaterne i samråd med samarbejdsgruppen og Den Europæiske Cybersikkerhedscertificeringsgruppe fremme væsentlige og vigtige enheders anvendelse af re-

levante europæiske og internationale standarder eller kan eventuelt kræve, at enhederne anvender certificerede IKT-produkter, -tjenester og -processer.

(81) Med henblik på at undgå, at operatører af væsentlige og vigtige enheder pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, bør foranstaltninger til styring af cybersikkerhedsrisici stå i et rimeligt forhold til den risiko, det pågældende net- og informationssystem er udsat for, under hensyntagen til sådanne foranstaltningers aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt omkostningerne ved deres gennemførelse.

(82) Foranstaltninger til styring af cybersikkerhedsrisici bør stå i et passende forhold til graden af de væsentlige eller vigtige enheders risikoeksponering og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Ved fastlæggelsen af foranstaltninger til styring af cybersikkerhedsrisici, der er tilpasset væsentlige og vigtige enheder, bør der tages behørigt hensyn til væsentlige og vigtige enheders forskellige risikoeksponering, herunder enhedens kritiske betydning, de risici, herunder samfundsmæssige risici, som den er eksponeret for, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

(83) Væsentlige og vigtige enheder bør garantere sikkerheden af de net- og informationssystemer, som de anvender i forbindelse med deres aktiviteter. Disse systemer er primært private net- og informationssystemer, der forvaltes af de væsentlige og vigtige enheders interne IT-personale, eller hvis sikkerhed er blevet outsourcet. De foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, der er fastsat i dette direktiv, bør finde anvendelse på de relevante væsentlige og vigtige enheder, uanset om disse enheder selv vedligeholder deres net- og informationssystemer eller outsourcer vedligeholdelsen deraf.

(84) DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner, af platforme for sociale netværkstjenester og af tillidstjenester bør i betragtning af deres grænseoverskridende karakter være underlagt en høj grad af harmonisering på EU-plan. Gen-

nemførelsen af foranstaltninger til styring af cybersikkerhedsrisici med hensyn til disse enheder bør derfor lettes ved hjælp af en gennemførelsesretsakt.

(85) Håndtering af risici, der stammer fra en enheds forsyningskæde og dens forhold til sine leverandører såsom udbydere af datalagrings- og databehandlingstjenester eller udbydere af administrerede sikkerhedstjenester og softwareudgivere, er særlig vigtig i betragtning af udbredelsen af hændelser, hvor enheder har været udsat for cyberangreb, og hvor ondsindede gerningspersoner har været i stand til at kompromittere sikkerheden af en enheds net- og informationssystemer ved at udnytte sårbarheder, der påvirker tredjepartsprodukter og -tjenester. Væsentlige og vigtige enheder bør derfor vurdere og tage hensyn til den generelle kvalitet og modstandsdygtighed af produkter og tjenester, de heri integrerede foranstaltninger til styring af cybersikkerhedsrisici og deres leverandørers og tjenesteudbyderes cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer. Væsentlige og vigtige enheder bør navnlig tilskyndes til at indarbejde foranstaltninger til styring af cybersikkerhedsrisici i kontraktlige arrangementer med deres direkte leverandører og tjenesteudbydere. Disse enheder kunne overveje risici hidrørende fra leverandører og tjenesteudbydere i andre led.

(86) Blandt tjenesteudbydere spiller udbydere af administrerede sikkerhedstjenester på områder såsom reaktion på hændelser, penetrationstest, sikkerhedsaudits og konsulentbistand en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at forebygge, opdage, reagere på eller reetablere sig efter hændelser. Udbydere af administrerede sikkerhedstjenester har imidlertid også selv været mål for cyberangreb og udgør på grund af deres høje grad af integration i enheders operationer en særlig risiko. Væsentlige og vigtige enheder bør derfor udvise forøget omhu ved udvælgelsen af en udbyder af administrerede sikkerhedstjenester.

(87) De kompetente myndigheder kan i forbindelse med deres tilsynsopgaver også drage fordel af cybersikkerhedstjenester såsom sikkerhedsaudits, penetrationstest eller reaktion på hændelser.

(88) Væsentlige og vigtige enheder bør også tage højde for risici hidrørende fra deres samspil og relationer med andre interessenter inden for et bredere økosystem, herunder i forbindelse med bekæmpelse af industrispionage og beskyttelse af forretningshem-

meligheder. Navnlig bør disse enheder træffe passende foranstaltninger til at sikre, at deres samarbejde med akademiske institutioner og forskningsinstitutioner finder sted i overensstemmelse med deres cybersikkerhedspolitikker og følger god praksis med hensyn til sikker adgang til og formidling af oplysninger generelt og beskyttelse af intellektuel ejendom i særdeleshed. På samme måde bør væsentlige og vigtige enheder i betragtning af datas betydning og værdi for deres aktiviteter træffe alle passende foranstaltninger til styring af cybersikkerhedsrisici, når disse enheder benytter sig af datatransformations- og dataanalysetjenester fra tredjeparter.

(89) Væsentlige og vigtige enheder bør indføre en bred vifte af grundlæggende cyberhygiejnepraksisser såsom »zero trust«-principper, softwareopdateringer, enhedskonfiguration, netværkssegmentering, identitets- og adgangsstyring eller brugerbevidsthed, arrangere kurser for deres personale og højne bevidstheden om cybertrusler, phishing og social engineering-teknikker. Disse enheder bør desuden evaluere deres egne cybersikkerhedskapaciteter og, hvor det er hensigtsmæssigt, stræbe efter at integrere cybersikkerhedsforstærkende teknologier, såsom systemer baseret på kunstig intelligens eller maskinlæring, for at forstærke deres kapaciteter og sikkerheden i net- og informationssystemerne.

(90) For yderligere at håndtere centrale risici i forsyningskæden og bistå væsentlige og vigtige enheder, der opererer i sektorer, som er omfattet af dette direktiv, med at håndtere forsyningskæde- og leverandørrelaterede risici på en hensigtsmæssig måde, bør samarbejdsgruppen, i samarbejde med Kommissionen og ENISA og, hvor det er hensigtsmæssigt, efter høring af relevante interessenter, herunder fra industrien, foretage koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder som dem, der er foretaget for 5G-net efter Kommissionens henstilling (EU) 2019/534 ([19]), med henblik på inden for hver enkelt sektor at identificere de kritiske IKT-tjenester, -systemer eller -produkter, relevante trusler og sårbarheder Sådanne koordinerede sikkerhedsrisikovurderinger bør identificere foranstaltninger, afbødningsplaner og bedste praksisser for modvirkning af kritiske afhængigheder, potentielle enkelte fejlpunkter, trusler, sårbarheder og andre risici knyttet til forsyningskæden og bør undersøge, hvordan væsentlige og vigtige enheder yderligere kan tilskyndes til at indføre disse. Potentielle ikketekniske risikofaktorer såsom et tredjelands utilbørlige påvirkning af leverandører og tjenesteudbydere, navn-

lig i forbindelse med alternative styringsmodeller, omfatter skjulte sårbarheder eller bagdøre og potentielle systemiske forsyningsforstyrrelser, navnlig i tilfælde af teknologisk fastlåsning eller udbyderafhængighed.

(91) Ved koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder bør der i lyset af kendetegnene ved den pågældende sektor tages hensyn til både tekniske og, hvor det er relevant, ikketekniske faktorer, herunder dem, der er defineret i henstilling (EU) 2019/534, i den EU- koordinerede risikovurdering af cybersikkerheden af 5G-net og i EU-værktøjskassen til 5G-cybersikkerhed, som samarbejdsgruppen er nået til enighed om. For at identificere de forsyningskæder, der bør gøres til genstand for en koordineret sikkerhedsrisikovurdering, bør følgende kriterier tages i betragtning: i) i hvilket omfang væsentlige og vigtige enheder anvender og er afhængige af specifikke kritiske IKT-tjenester, -systemer eller -produkter, ii) relevansen af specifikke kritiske IKT-tjenester, -systemer eller -produkter til udførelse af kritiske eller følsomme funktioner, herunder behandling af personoplysninger, iii) tilgængeligheden af alternative IKT-tjenester, -systemer eller -produkter, iv) modstandsdygtigheden af den samlede forsyningskæde for IKT-tjenester, -systemer eller -produkter i hele deres livscyklus over for forstyrrelser og v) for nye IKT-tjenester, -systemer eller -produkter, deres potentielle fremtidige betydning for enhedernes aktiviteter. Endvidere bør der lægges særlig vægt på IKT-tjenester, -systemer eller -produkter, der er underlagt specifikke krav hidrørende fra tredjelande.

(92) For at strømline de forpligtelser, der pålægges udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester og tillidstjenesteudbydere med hensyn til sikkerheden af deres net- og informationssystemer, og for at gøre det muligt for de pågældende enheder og de kompetente myndigheder, i henhold til henholdsvis Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 ([20]) og forordning (EU) nr. 910/2014, at drage fordel af de retlige rammer, der er fastsat i dette direktiv, herunder udpegelsen af en CSIRT med ansvar for håndteringen af hændelser, deltagelsen af de berørte kompetente myndigheder i samarbejdsgruppens aktiviteter og CSIRT-netværket, bør de pågældende enheder være omfattet af dette direktivs anvendelsesområde. De tilsvarende bestemmelser i forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 vedrørende

indførelse af sikkerhedskrav og underretningspligt for disse typer enheder bør derfor udgå. Reglerne om rapporteringsforpligtelser, der er fastsat i nærværende direktiv, bør ikke berøre forordning (EU) 2016/679 og direktiv 2002/58/EF.

(93) Cybersikkerhedsforpligtelserne, der er fastsat i dette direktiv, bør betragtes som et supplement til de krav, der pålægges tillidstjenesteudbydere i henhold til forordning (EU) nr. 910/2014. Tillidstjenesteudbydere bør være forpligtet til at træffe alle passende og forholdsmæssige foranstaltninger for at styre de risici, der er forbundet med deres tjenester, herunder i forhold til kunder og tilknyttede tredjeparter, og til at rapportere hændelser i henhold til dette direktiv. Sådanne cybersikkerheds- og rapporteringsforpligtelser bør også vedrøre den fysiske beskyttelse af de udbudte tjenester. Kravene til kvalificerede tillidstjenesteudbydere i artikel 24 i forordning (EU) nr. 910/2014 finder fortsat anvendelse.

(94) Medlemsstaterne kan tildele rollen som de kompetente myndigheder for tillidstjenester til de i forordning (EU) nr. 910/2014 omhandlede tilsynsorganer for at sikre videreførelsen af den nuværende praksis og bygge videre på den viden og erfaring, der er opnået i forbindelse med anvendelsen af nævnte forordning. I sådanne tilfælde bør de kompetente myndigheder i henhold til dette direktiv arbejde tæt sammen med disse tilsynsorganer ved rettidigt at udveksle relevante oplysninger for at sikre effektivt tilsyn med tillidstjenesteudbyderne og sikre deres overholdelse af kravene i dette direktiv og i forordning (EU) nr. 910/2014. I givet fald bør CSIRT'en eller den kompetente myndighed i henhold til dette direktiv straks informere tilsynsorganet i henhold til forordning (EU) nr. 910/2014 om enhver underretning om en væsentlig cybertrussel eller hændelse, der berører tillidstjenester samt om ethvert tilfælde af en tillidstjenesteudbyders overtrædelser af dette direktiv. Medlemsstaterne kan i rapporteringsøjemed i givet fald anvende det enkelte indgangspunkt, der er oprettet for at opnå en fælles og automatisk rapportering af hændelser til både tilsynsorganet i henhold til forordning (EU) nr. 910/2014 og CSIRT eller den kompetente myndighed i henhold til dette direktiv.

(95) Hvor det er hensigtsmæssigt og for at undgå unødige forstyrrelser, bør eksisterende nationale retningslinjer der er vedtaget med henblik på gennemførelse af reglerne vedrørende sikkerhedsforanstaltninger i artikel 40 og 41 i direktiv (EU) 2018/1972, tages i betragtning ved gennemførelsen af nærværende direktiv, så der

kan bygges videre på den viden og de færdigheder, der allerede er erhvervet i forbindelse med direktiv (EU) 2018/1972 med hensyn til sikkerhedsforanstaltninger og hændelsesunderretninger. ENISA kan også udvikle vejledning om sikkerhedskrav og om rapporteringsforpligtelser for udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester for at lette harmonisering og omstilling og minimere forstyrrelser. Medlemsstaterne kan tildele de nationale tilsynsmyndigheder rollen som de kompetente myndigheder for elektronisk kommunikation i henhold til direktiv (EU) 2018/1972 for at sikre videreførelsen af den nuværende praksis og bygge videre på den viden og erfaring, der er opnået som et resultat af gennemførelsen af nævnte direktiv.

(96) I betragtning af den stigende betydning af nummeruafhængige interpersonelle kommunikationstjenester som defineret i direktiv (EU) 2018/1972 er det nødvendigt at sikre, at sådanne tjenester også er omfattet af passende sikkerhedskrav i lyset af deres særlige karakter og økonomiske betydning. Eftersom angrebsfladen bliver stadig større, bliver nummeruafhængige interpersonelle kommunikationstjenester såsom meddelelsestjenester stadig mere udbredte angrebsvektorer. Ondsindede gerningspersoner anvender platforme til at kommunikere med og lokke ofre til at gå ind på kompromitterede websider, hvilket øger sandsynligheden for hændelser, der involverer udnyttelse af personoplysninger og, som følge deraf, sikkerheden i net- og informationssystemer. Udbydere af nummeruafhængige interpersonelle kommunikationstjenester bør sikre et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Da udbydere af nummeruafhængige interpersonelle kommunikationstjenester normalt ikke udøver egentlig kontrol over transmissionen af signaler via net, kan risikoniveauet for sådanne tjenester i visse henseender anses for at være lavere end for traditionelle elektroniske kommunikationstjenester. Det samme gælder interpersonelle kommunikationstjenester, som defineret i direktiv (EU) 2018/1972, der anvender numre, og som ikke udøver faktisk kontrol over signaltransmission.

(97) Det indre marked er mere end nogensinde afhængigt af internettets funktionsdygtighed. Næsten alle væsentlige og vigtige enheders tjenester er afhængige af tjenester, der leveres over internettet. For at sikre en problemfri levering af tjenester, der udbydes af

væsentlige og vigtige enheder, er det vigtigt, at alle udbydere af offentlige elektroniske kommunikationsnet har indført passende foranstaltninger til styring af cybersikkerhedsrisici og rapporterer om væsentlige hændelser i forbindelse hermed. Medlemsstaterne bør sørge for, at sikkerheden af de offentlige elektroniske kommunikationsnet opretholdes, og at deres vitale sikkerhedsinteresser beskyttes mod sabotage og spionage. Eftersom international konnektivitet styrker og fremskynder den konkurrencedygtige digitalisering af Unionen og dens økonomi, bør hændelser, der påvirker undersøiske kommunikationskabler, rapporteres til CSIRT eller i givet fald til den kompetente myndighed. Den nationale cybersikkerhedsstrategi bør, hvor det er relevant, tage hensyn til undersøiske kommunikationskablers cybersikkerhed og omfatte en kortlægning af potentielle cybersikkerhedsrisici og afbødende foranstaltninger for at sikre dem det højeste beskyttelsesniveau.

(98) For at beskytte sikkerheden af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester bør brugen af krypteringsteknologier, navnlig end-to-end-kryptering samt datacentrerede sikkerhedskoncepter såsom kartografi, segmentering, tagging, adgangspolitik og adgangsstyring samt automatiserede adgangsbeslutninger fremmes. Om nødvendigt bør anvendelsen af kryptering, navnlig end-to-end-kryptering, være obligatorisk for udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester i overensstemmelse med principperne om sikkerhed og privatlivsbeskyttelse gennem standardindstillinger og gennem design med henblik på dette direktiv. Brugen af end-to-end-kryptering bør forliges med medlemsstaternes beføjelser til at sikre beskyttelsen af deres væsentlige sikkerhedsinteresser og offentlig sikkerhed og til at tillade forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger i overensstemmelse med EU-retten. Dette bør dog ikke svække end-to-end-kryptering, som er en teknologi af kritisk betydning for den effektive data- og privatlivsbeskyttelse og for kommunikationssikkerheden.

(99) For at beskytte sikkerheden af og forhindre misbrug af og manipulation med offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester bør brugen af sikre routingstandarder fremmes for at sikre integriteten

og robustheden af routingfunktionerne i hele økosystemet af udbydere af internetadgangstjenester.

(100) For at beskytte internettets funktionalitet og integritet og fremme DNS'ens sikkerhed og modstandsdygtighed bør relevante interessenter, herunder enheder i Unionens private sektor, udbydere af offentligt tilgængelige elektroniske kommunikationstjenester, navnlig udbydere af internetadgangstjenester, og udbydere af onlinesøgemaskiner tilskyndes til at vedtage en diversificeringsstrategi for DNS-oversættelse. Endvidere bør medlemsstaterne tilskynde til udvikling og brug af en offentlig og sikker europæisk DNS-oversættelsestjeneste.

(101) I dette direktiv fastlægges en flertrinstilgang for underretning om væsentlige hændelser med henblik på at finde den rette balance mellem på den ene side hurtig underretning, der bidrager til at afbøde den potentielle spredning af væsentlige hændelser og giver væsentlige og vigtige enheder mulighed for at søge assistance, og på den anden side dybdegående underretning, der gør det muligt at høste værdifulde erfaringer af individuelle hændelser og over tid forbedre individuelle virksomheders og hele sektorers cyberrobusthed. Direktivet bør i den henseende omfatte underretning om hændelser, som ud fra en indledende vurdering foretaget af den berørte enhed kunne forårsage alvorlige driftsmæssige forstyrrelser af tjenesterne eller økonomiske tab for denne enhed eller forvolde betydelig materiel eller immateriel skade for andre fysiske eller juridiske personer. En sådan indledende vurdering bør bl.a. tage i betragtning de berørte net- og informationssystemer, navnlig deres betydning for leveringen af enhedens tjenester, alvoren og de tekniske karakteristika af en cybertrussel, eventuelle underliggende sårbarheder, der udnyttes, samt enhedens erfaring med tilsvarende hændelser. Indikatorer såsom graden af påvirkning af tjenestens funktionsdygtighed, varigheden af en hændelse eller antallet af berørte tjenestemodtagere vil kunne spille en vigtig rolle med hensyn til at fastslå, om den driftsmæssige forstyrrelse af tjenesten er alvorlig.

(102) Hvor væsentlige og vigtige enheder bliver opmærksomme på en væsentlig hændelse, bør de være forpligtet til at indgive en tidlig varsling uden unødigt ophold og under alle omstændigheder inden for 24 timer. Denne tidlige varsling bør efterfølges af en hændelsesunderretning. De pågældende enheder bør indgive en hændelsesunderretning uden unødigt ophold og under alle om-

stændigheder inden for 72 timer efter, at have fået kendskab til den væsentlige hændelse, navnlig med henblik på at ajourføre de oplysninger, der blev indgivet ved den tidlige varsling, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning, samt kompromitteringsindikatorer, hvor sådanne foreligger. En endelig rapport bør indgives senest en måned efter hændelsesunderretningen. Den tidlige varsling bør kun indeholde de oplysninger, der er nødvendige for at gøre CSIRT'en eller i givet fald den kompetente myndighed opmærksom på den væsentlige hændelse og give den pågældende enhed mulighed for om nødvendigt at søge assistance. En sådan tidlige varsling bør, hvis det er relevant, angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger, og om den sandsynligvis vil have grænseoverskridende virkninger. Medlemsstaterne bør sikre, at forpligtelsen til at indgive den tidlige varsling eller den efterfølgende hændelsesunderretning ikke medfører, at den underrettende enhed bruger færre ressourcer på aktiviteter vedrørende håndtering af hændelser, idet disse bør prioriteres, så det forhindres, at forpligtelser vedrørende hændelsesrapportering enten omdirigerer ressourcer fra håndtering af væsentlige hændelser eller på anden måde kompromitterer enhedens indsats i denne henseende. I tilfælde af, at en hændelse pågår på tidspunktet for indgivelsen af den endelige rapport, bør medlemsstaterne sikre, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af den væsentlige hændelse.

(103) De væsentlige og vigtige enheder bør i givet fald og uden unødigt ophold underrette deres tjenestemodtagere om enhver foranstaltning eller modforholdsregel, de kan træffe for at afbøde risici fra en væsentlig cybertrussel. Disse enheder bør, hvor det er hensigtsmæssigt, og navnlig hvor den væsentlige cybertrussel sandsynligvis vil materialisere sig, også informere deres tjenestemodtagere om selve truslen. Kravet om at informere modtagerne om væsentlige cybertrusler bør opfyldes efter bedste evne, men bør ikke fritage disse enheder for forpligtelsen til for egen regning at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe enhver trussel af denne art og genoprette tjenestens normale sikkerhedsniveau. Sådanne oplysninger om væsentlige

cybertrusler bør stilles gratis til rådighed for modtagerne i et let forståeligt sprog.

(104) Udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester bør indføre sikkerhed gennem design og gennem standardindstillinger samt informere deres tjenestemodtagere om væsentlige cybertrusler og om de foranstaltninger, de kan træffe for at beskytte deres enheder og kommunikation, f.eks. ved at anvende bestemte typer software eller krypteringsteknologier.

(105) En proaktiv tilgang til cybertrusler er et afgørende element i styring af cybersikkerhedsrisici, som bør sætte de kompetente myndigheder i stand til effektivt at forhindre cybertrusler i at blive til hændelser, der kan forårsage betydelige materiel eller immateriel skade. Med henblik herpå er underretning om cybertrusler af afgørende betydning. Enhederne opfordres med dette for øje til på frivillig basis at rapportere cybertrusler.

(106) For at forenkle rapporteringen af de oplysninger, der kræves i henhold til dette direktiv, og for at mindske den administrative byrde for enhederne bør medlemsstaterne stille tekniske midler til rådighed såsom et enkelt indgangspunkt, automatiserede systemer, onlineformularer, brugervenlige grænseflader, skabeloner og dedikerede platforme, som enheder, uanset om de falder ind under dette direktivs anvendelsesområde, til indgivelsen af de relevante oplysninger, der skal rapporteres. Unionens støtte til gennemførelsen af dette direktiv, navnlig inden for programmet for et digitalt Europa, der er oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/694 ([21]), vil kunne omfatte støtte til enkelte indgangspunkter. Endvidere befinder enheder sig ofte i en situation, hvor en bestemt hændelse på grund af dens karakteristika skal rapporteres til forskellige myndigheder som følge af underretningspligten i forskellige retsakter. Sådanne tilfælde medfører ekstra administrative byrder og kunne også føre til usikkerhed med hensyn til formatet af og procedurerne for sådanne underretninger. Hvor der er oprettet et enkelt indgangspunkt, opfordres medlemsstaterne til også at anvende dette til underretninger om sikkerhedshændelser, der kræves i henhold til anden EU-ret, såsom forordning (EU) 2016/679 og direktiv 2002/58/EF. Anvendelsen af et sådant enkelt indgangspunkt til rapportering af sikkerhedshændelser i henhold til forordning (EU) 2016/679 og direktiv 2002/58/EF bør ikke berøre anven-

delsen af bestemmelserne i forordning (EU) 2016/679 og direktiv 2002/58/EF, navnlig bestemmelserne vedrørende uafhængigheden af de deri omhandlede myndigheder. ENISA bør i samarbejde med samarbejdsgruppen udvikle fælles underretningsmodeller ved hjælp af retningslinjer, der kan forenkle og strømline de oplysninger, der skal rapporteres, i henhold til EU-retten, og mindske den administrative byrde for de underrettende enheder.

(107) Hvor der er mistanke om, at en hændelse har forbindelse til alvorlige kriminelle aktiviteter i henhold til EU-retten eller national ret, bør medlemsstaterne opfordre væsentlige og vigtige enheder til på grundlag af gældende strafferetsplejeregler i overensstemmelse med EU-retten at rapportere hændelser af formodet alvorlig kriminel karakter til de relevante retshåndhævende myndigheder. Hvor det er relevant, og uden at det berører de regler om beskyttelse af personoplysninger, der gælder for Europol, er det ønskeligt, at Det Europæiske Center for Bekæmpelse af Cyberkriminalitet (EC3) og ENISA letter koordineringen mellem de kompetente myndigheder og de retshåndhævende myndigheder i forskellige medlemsstater.

(108) Personoplysninger bliver i mange tilfælde kompromitteret som følge af hændelser. I den forbindelse bør de kompetente myndigheder samarbejde og udveksle oplysninger om alle relevante spørgsmål med de myndigheder, der er omhandlet i forordning (EU) 2016/679 og direktiv 2002/58/EF.

(109) Det er afgørende at opretholde nøjagtige og fuldstændige databaser over domænenavnsregistreringsdata (»WHOIS-data«) og give lovlig adgang til sådanne data for at sikre DNS'ens sikkerhed, stabilitet og modstandsdygtighed, hvilket igen bidrager til et højt fælles cybersikkerhedsniveau i hele Unionen. Med henblik herpå bør topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, være forpligtet til at behandle visse data, der er nødvendige for at opfylde dette formål. Denne behandling bør udgøre en retlig forpligtelse i den i artikel 6, stk. 1, litra c), i forordning (EU) 2016/679 anvendte betydning. Denne forpligtelse berører ikke muligheden for at indsamle domænenavnsregistreringsdata til andre formål, f.eks. på grundlag af kontraktlige arrangementer eller retlige krav, der er fastsat i anden EU-ret eller national ret. Denne forpligtelse har til formål at opnå et fuldstændigt og nøjagtigt sæt af registreringsdata og bør ikke medføre, at de samme data indsamles flere

gange. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør samarbejde med hinanden for at undgå dobbeltarbejde.

(110) Tilgængeligheden af og den rettidige adgang til domænenavnsregistreringsdata for legitime adgangssøgende er afgørende for at forebygge og bekæmpe DNS-misbrug samt for at forebygge, og opdage og reagere på, hændelser. Ved legitime adgangssøgende forstås enhver fysisk eller juridisk person, der fremsætter en anmodning i henhold til EU-retten eller national ret. De kan omfatte myndigheder, som er kompetente i henhold til dette direktiv, og myndigheder, som i henhold til EU-retten eller national ret er kompetente til at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, samt CERT'er eller CSIRT'er. Topdomæneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør være forpligtet til at give lovlig adgang til specifikke domænenavnsregistreringsdata, som er nødvendige for anmodningen om adgang, for legitime adgangssøgende i overensstemmelse med EU-retten og national ret. Anmodningen fra legitime adgangssøgende bør ledsages af en begrundelse, der gør det muligt at vurdere nødvendigheden af adgang til dataene.

(111) For at sikre, at nøjagtige og fuldstændige domænenavnsregistreringsdata er til rådighed, bør topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, indsamle og garantere integriteten og tilgængeligheden af domænenavnsregistreringsdata. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør navnlig fastlægge politikker og procedurer for indsamling og vedligeholdelse af nøjagtige og fuldstændige domænenavnsregistreringsdata samt for forebyggelse og rettelse af unøjagtige registreringsdata, i overensstemmelse med EU-databeskyttelsesretten. Disse politikker og procedurer bør så vidt muligt tage hensyn til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør fastlægge og indføre forholdsmæssige procedurer til verifikation af domænenavnsregistreringsdata. Disse procedurer bør afspejle den bedste praksis, der anvendes i industrien, og så vidt muligt de fremskridt, der er gjort inden for elektronisk identifikation. Verifikationsprocedurerne kan eksempelvis bestå i for-

udgående kontrol, der foretages på tidspunktet for registreringen, og efterfølgende kontrol, der foretages efter registreringen. Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør navnlig verificere mindst én kontaktmåde for registranten.

(112) Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør i overensstemmelse med præamblen til forordning (EU) 2016/679 forpligtes til at offentliggøre oplysninger om registrering af domænenavne, der ikke er omfattet af anvendelsesområdet for EU-databeskyttelsesretten, såsom data, der vedrører juridiske personer. For så vidt angår juridiske personer bør topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, mindst offentliggøre registrantens navn og kontakttelefonnummer. Kontaktmailadressen bør også offentliggøres, forudsat at den ikke indeholder personoplysninger, såsom ved brug af e-mail-aliasser or funktionsmailadresser. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør også give legitime adgangssøgende lovlig adgang til specifikke domænenavnsregistreringsdata om fysiske personer i overensstemmelse med EU-databeskyttelsesretten. Medlemsstaterne bør pålægger topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, uden unødigt ophold at besvare anmodninger om udlevering af domænenavnsregistreringsdata fra legitime adgangssøgende. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, bør fastlægge politikker og procedurer for offentliggørelse og udlevering af registreringsdata, herunder serviceleveranceaftaler til behandling af anmodninger om adgang fra legitime adgangssøgende. Disse politikker og procedurer bør så vidt muligt tage hensyn til eventuel vejledning og til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan. Adgangsproceduren vil også kunne omfatte brug af en grænseflade, en portal eller et andet teknisk værktøj til at tilvejebringe et effektivt system til anmodning om og adgang til registreringsdata. Med henblik på at fremme en harmoniseret praksis i hele det indre marked kan Kommissionen, uden at det berører Det Europæiske Databeskyttelsesråds beføjelser, fastlægge retningslinjer for sådanne procedurer, som så vidt muligt tager hensyn til de standarder, der er udviklet af multiinteres-

sentstyringsstrukturerne på internationalt plan. Medlemsstaterne bør sikre, at alle former for adgang til personlige og ikkepersonlige domænenavnsregistreringsdata er gratis.

(113) Enheder, der er omfattet af dette direktivs anvendelsesområde, bør anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret. Dog bør udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester. DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester til topdomæner, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester bør anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen. Offentlige forvaltningsenheder bør henhøre under jurisdiktionen i den medlemsstat, der har oprettet dem. Hvis enheden leverer tjenester eller er etableret i mere end én medlemsstat, bør den henhøre under hver af disse medlemsstaters særskilte og parallelle jurisdiktion. De kompetente myndigheder i disse medlemsstater bør samarbejde, yde hinanden gensidig bistand og, hvor det er hensigtsmæssigt, gennemføre fælles tilsynstiltag. Hvor medlemsstaterne udøver deres jurisdiktion, bør de ikke pålægge håndhævelsesforanstaltninger eller sanktioner mere end én gang for den samme adfærd i overensstemmelse med princippet ne bis in idem.

(114) For at tage hensyn til den grænseoverskridende karakter af de tjenester og operationer, der henholdsvis leveres og udføres af DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester, bør kun én medlemsstat have jurisdiktion over disse enheder. Jurisdiktionen bør tillægges den medlemsstat, hvor den pågældende enhed har sit hovedforretningssted i Unionen. For så vidt angår dette direktiv indebærer forretningsstedskriteriet i dette direktiv en faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende

ordningers juridiske form — hvorvidt der er tale om en filial eller et datterselskab med status som juridisk person — er ikke den afgørende faktor i denne forbindelse. Opfyldelsen af det nævnte kriterium bør ikke afhænge af, om net- og informationssystemerne fysisk befinder sig på et givent sted; tilstedeværelsen og anvendelsen af sådanne systemer udgør ikke i sig selv et sådant hovedforretningssted og er derfor ikke afgørende for fastlæggelsen af samme. Hovedforretningsstedet bør anses som værende i den medlemsstat, hvor beslutningerne vedrørende foranstaltninger til styring af cybersikkerhedsrisici overvejende træffes i Unionen. Det vil typisk være det sted, hvor enhedernes centrale administration i Unionen er placeret. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Unionen, bør hovedforretningsstedet anses for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Hvis en sådan medlemsstat ikke kan fastslås, bør hovedforretningsstedet anses for at være i den medlemsstat, hvor enhedens forretningssted med det største antal ansatte i Unionen er beliggende. Hvor tjenesterne udføres af en gruppe af virksomheder, bør den kontrollerende virksomheds hovedforretningssted anses for at være hele gruppens hovedforretningssted.

(115) Hvor en offentligt tilgængelig rekursiv DNS-tjeneste udbydes af en udbyder af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester kun som en del af dennes internetadgangstjeneste, bør enheden anses for at henhøre under jurisdiktionen i alle de medlemsstater, hvor dens tjenester udbydes.

(116) Hvor en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Unionen, udbyder tjenester i Unionen, bør denne udpege en repræsentant i Unionen. Med henblik på at afgøre, om en sådan enhed udbyder tjenester i Unionen, bør det fastslås, om enheden har til hensigt at udbyde tjenester til personer i en eller flere medlemsstater. Det blotte faktum, at der i Unionen er adgang til enhedens eller en formidlers websted eller til en e-mailadresse og andre kontaktoplysninger, eller at der

benyttes et sprog, som almindeligvis benyttes i det tredjeland, hvor enheden er etableret, bør anses for utilstrækkeligt til at fastslå en sådan hensigt. Imidlertid vil faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater, muligheden for at bestille tjenester på det pågældende sprog eller omtale af kunder eller brugere, der befinder sig i Unionen, kunne gøre det åbenbart, at enheden har til hensigt at udbyde tjenester i Unionen. Repræsentanten bør handle på vegne af enheden, og det bør være muligt for de kompetente myndigheder eller CSIRT'er at kontakte repræsentanten. Repræsentanten bør have et udtrykkeligt skriftligt mandat fra enheden til at handle på sidstnævntes vegne for så vidt angår sidstnævntes forpligtelser, der er fastsat i dette direktiv, herunder rapportering af hændelser.

(117) For at sikre et klart overblik over DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester, der leverer tjenester i hele Unionen, som er omfattet af dette direktivs anvendelsesområde, bør ENISA oprette og føre et register over sådanne enheder på grundlag af de oplysninger, som medlemsstaterne modtager, i givet fald gennem nationale mekanismer oprettet for, at enheder kan registrere dem selv. De centrale kontaktpunkter bør sende ENISA oplysningerne og eventuelle ændringer heraf. Med henblik på at sikre, at de oplysninger, som skal optages i dette register, er nøjagtige og fuldstændige, kan medlemsstaterne tilsende ENISA de oplysninger, der findes om de pågældende enheder i nationale registre. ENISA og medlemsstaterne bør træffe foranstaltninger til at fremme interoperabiliteten mellem sådanne registre, samtidig med at beskyttelsen af fortrolige eller klassificerede oplysninger sikres. ENISA bør fastsætte passende protokoller for klassificering og forvaltning af oplysninger for at sikre, at de udleverede oplysningers sikkerhed og fortrolighed bevares, og at adgangen til, lagringen af og overførsel af sådanne oplysninger begrænses til de tiltænkte brugere.

(118) Hvor oplysninger, der er klassificeret i overensstemmelse med EU-retten eller national ret udveksles, rapporteres eller på anden

måde deles i henhold til dette direktiv, bør de tilsvarende regler for håndtering af klassificerede oplysninger finde anvendelse. Endvidere bør ENISA have infrastruktur, procedurer og regler på plads til at håndtere følsomme og klassificerede oplysninger i overensstemmelse med de gældende regler for sikkerhedsbeskyttelse af EU's klassificerede informationer.

(119) I takt med at cybertrusler bliver mere komplekse og sofistikerede, er evnen til at opdage sådanne trusler og træffe effektive forebyggelsesforanstaltninger mod dem i høj grad afhængig af regelmæssig udveksling af trussels- og sårbarhedsefterretninger mellem enheder. Udveksling af oplysninger bidrager til øget bevidsthed om cybertrusler, hvilket igen styrker enhedernes evne til at forhindre trusler i at blive til hændelser og sætter dem i stand til bedre at inddæmme virkningerne af hændelser og reetablere sig mere effektivt. I mangel af vejledning på EU-plan synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, navnlig usikkerhed om foreneligheden med konkurrence- og ansvarsregler.

(120) Enhederne bør tilskyndes til, med bistand fra medlemsstaterne, i fællesskab at udnytte deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan med henblik på at styrke deres kapacitet til i tilstrækkeligt omfang at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger. Det er derfor nødvendigt at gøre det muligt på EU-plan at etablere frivillige ordninger for udveksling af cybersikkerhedsoplysninger. Med henblik herpå bør medlemsstaterne aktivt bistå og tilskynde enheder, såsom dem der leverer cybersikkerhedstjenester og -forskning, samt relevante enheder, der ikke er omfattet af dette direktivs anvendelsesområde til at deltage i sådanne ordninger for udveksling af cybersikkerhedsoplysninger. Disse ordninger bør etableres i overensstemmelse med EU-konkurrencereglerne og EU-databeskyttelsesretten.

(121) Væsentlige og vigtige enheders behandling af personoplysninger vil i det omfang, det er nødvendigt og står i et rimeligt forhold til målet om at sikre sikkerheden i net- og informationssystemer, kunne anses for at være lovlig, når en sådan behandling overholder en retlig forpligtelse, som påhviler den dataansvarlige, i overensstemmelse med betingelserne i artikel 6, stk. 1, litra c), og artikel 6, stk. 3, i forordning (EU) 2016/679. Behandling af personoplysninger vil også kunne være nødvendig for, at væsentlige

og vigtige enheder samt udbydere af sikkerhedsteknologier og -tjenester, der handler på de nævnte enheders vegne, kan forfølge legitime interesser i henhold til artikel 6, stk. 1, litra f), i forordning (EU) 2016/679, herunder når en sådan behandling er nødvendig for ordninger for udveksling af cybersikkerhedsoplysninger eller frivillig underretning om relevante oplysninger i overensstemmelse med dette direktiv. Foranstaltninger vedrørende forebyggelse, opdagelse, identifikation, inddæmning, analyse og reaktion på hændelser, foranstaltninger til at øge bevidstheden vedrørende specifikke cybertrusler, udveksling af oplysninger i forbindelse med afhjælpning af sårbarheder og koordineret offentliggørelse af sårbarheder, frivillig udveksling af oplysninger om disse hændelser samt cybertrusler og sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer vil kunne kræve behandling af visse kategorier af personoplysninger såsom IP-adresser, uniform resources locators (URL'er), domænenavne, e-mailadresser og, hvor disse afslører personlige oplysninger, tidsstempler. De kompetente myndigheders, de centrale kontaktpunkters og CSIRT'ernes behandling af personoplysninger vil kunne udgøre en retlig forpligtelse eller anses for at være nødvendig for udførelsen af en opgave i samfundets interesse eller henhørende under offentlig myndighedsudøvelse, som den ansvarlige har fået pålagt, i henhold til artikel 6, stk. 1, litra c) eller e), og artikel 6, stk. 3, i forordning (EU) 2016/679, eller for forfølgelsen af væsentlige og vigtige enheders legitime interesser, som omhandlet i artikel 6, stk. 1, litra f), i forordning (EU) 2016/679. Desuden vil der i national ret kunne fastsættes regler, der gør det muligt for de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne, i det omfang det er nødvendigt og forholdsmæssigt for at sikre sikkerheden i væsentlige og vigtige enheders net- og informationssystemer, at behandle særlige kategorier af personoplysninger i overensstemmelse med artikel 9 i forordning (EU) 2016/679, navnlig ved at fastsætte passende og specifikke foranstaltninger til beskyttelse af fysiske personers grundlæggende rettigheder og interesser, herunder tekniske begrænsninger for videreanvendelse af sådanne data og anvendelse af sikkerheds- og privatlivsbevarende foranstaltninger på det aktuelle teknologiske stade såsom pseudonymisering eller kryptering, hvor anonymisering i væsentlig grad kan påvirke det forfulgte formål.

(122) For at styrke de tilsynsbeføjelser og -foranstaltninger, der bidrager til at sikre effektiv overholdelse, bør dette direktiv indeholde en minimumsliste over tilsynsforanstaltninger og -midler, hvorigennem de kompetente myndigheder kan føre tilsyn med væsentlige og vigtige enheder. Desuden bør der ved dette direktiv indføres en differentiering af tilsynsordningen for henholdsvis væsentlige og vigtige enheder med henblik på at sikre en rimelig balance mellem forpligtelser for disse enheder og for de kompetente myndigheder. Væsentlige enheder bør derfor være underlagt en omfattende forudgående og efterfølgende tilsynsordning, mens vigtige enheder bør være underlagt en lettere, rent efterfølgende tilsynsordning. Vigtige enheder bør derfor ikke være forpligtet til systematisk at dokumentere overholdelsen af foranstaltninger til styring af cybersikkerhedsrisici, mens de kompetente myndigheder bør anvende en reaktiv efterfølgende tilgang til tilsyn og dermed ikke have en generel forpligtelse til at føre tilsyn med disse enheder. Det efterfølgende tilsyn med vigtige enheder kan udløses af dokumentation, tegn eller oplysninger, som de kompetente myndigheder gøres opmærksom på, og som efter deres opfattelse tyder på potentielle overtrædelser af dette direktiv. Sådan dokumentation, sådant tegn eller sådanne oplysninger kunne være af den type, som de kompetente myndigheder modtager fra andre myndigheder, enheder, borgere, medier eller andre kilder eller offentligt tilgængelige oplysninger, eller kunne hidrøre fra andre aktiviteter, der indgår i de kompetente myndigheders udførelse af deres opgaver.

(123) De kompetente myndigheders udførelse af tilsynsopgaver bør ikke unødigt hæmme den berørte enheds forretningsaktiviteter. Hvor de kompetente myndigheder udfører deres tilsynsopgaver vedrørende væsentlige enheder, herunder i form af kontrol på stedet og eksternt tilsyn, efterforskning overtrædelser af dette direktiv og udførelse af sikkerhedsaudits eller -scanninger, bør de minimere indvirkningen på den berørte enheds forretningsaktiviteter.

(124) Ved udøvelsen af efterfølgende tilsyn bør de kompetente myndigheder kunne træffe afgørelse om prioriteringen af de tilsynsforanstaltninger og -midler, som de har til rådighed, på en forholdsmæssig måde. Dette indebærer, at de kompetente myndigheder kan træffe afgørelse om en sådan prioritering på grundlag af tilsynsmetoder, som bør baseres på en risikobaseret tilgang.

Mere specifikt vil sådanne metoder kunne omfatte kriterier eller benchmarks for klassificering af væsentlige enheder i risikokategorier og tilsvarende anbefalede tilsynsforanstaltninger og -midler pr. risikokategori, som f.eks. brugen, hyppigheden eller typerne af kontrol på stedet, målrettede sikkerhedsaudits eller -scanninger, typen af oplysninger, der skal anmodes om, og detaljeringsgraden af disse oplysninger. Sådanne tilsynsmetoder vil også kunne ledsages af arbejdsprogrammer og vurderes og revideres regelmæssigt, herunder vedrørende aspekter såsom ressourcefordeling og -behov. For så vidt angår offentlige forvaltningsorganer bør tilsynsbeføjelserne udøves i overensstemmelse med de nationale lovgivningsmæssige og institutionelle rammer.

(125) De kompetente myndigheder bør sikre, at deres tilsynsopgaver i forbindelse med væsentlige og vigtige enheder udføres af uddannede fagfolk, som bør have de nødvendige færdigheder til at udføre disse opgaver, navnlig med hensyn til at udføre kontrol på stedet og eksternt tilsyn, herunder identifikation af svagheder i databaser, hardware, firewalls, kryptering og netværk. Denne kontrol og sådant tilsyn bør udføres på en objektiv måde.

(126) Den kompetente myndighed bør i behørigt begrundede tilfælde, hvor den er blevet bekendt med en væsentlig cybertrussel eller en overhængende risiko, omgående kunne træffe håndhævelsesafgørelser med henblik på at forebygge eller reagere på en hændelse.

(127) For at gøre håndhævelse effektiv bør der fastlægges en minimumsliste over håndhævelsesbeføjelser, der kan udøves for overtrædelse af foranstaltningerne til styring af cybersikkerhedsrisici og rapporteringskravene i dette direktiv, som opstiller en klar og konsekvent ramme for sådan håndhævelse i hele Unionen. Der bør tages behørigt hensyn til overtrædelsen af dette direktivs art, grovhed og varighed, den forvoldte materielle eller immaterielle skade, hvorvidt overtrædelsen var forsætlig eller uagtsom, tiltag truffet for at forebygge eller afbøde den materielle eller immaterielle skade, graden af ansvar eller eventuelle relevante tidligere overtrædelser, graden af samarbejde med den kompetente myndighed og enhver anden skærpende eller formildende omstændighed. Håndhævelsesforanstaltningerne, herunder administrative bøder, bør være forholdsmæssige, og pålæggelsen heraf bør være underlagt passende proceduremæssige ga-

rantier i overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder (chartret), herunder adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

(128) Dette direktiv forpligter ikke medlemsstaterne til at pålægge strafferetligt eller civilretligt ansvar for fysiske personer, der er ansvarlige for at sikre, at en enhed overholder dette direktiv, for skader, som tredjemand påføres som følge af en overtrædelse af dette direktiv.

(129) For at sikre en effektiv håndhævelse af de forpligtelser, der er fastsat i dette direktiv, bør hver kompetent myndighed have beføjelse til at pålægge eller anmode om pålæggelse af administrative bøder.

(130) Hvor en administrative bøde pålægges en væsentlig eller vigtig enhed, der er en virksomhed, bør der ved virksomhed i denne forbindelse forstås en virksomhed i overensstemmelse med artikel 101 og 102 i TEUF. Hvor en administrativ bøde pålægges en person, der ikke er en virksomhed, bør den kompetente myndighed ved fastsættelsen af en passende bødestørrelse tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske stilling. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder. Pålæggelse af en administrativ bøde berører ikke de kompetente myndigheders anvendelse af andre beføjelser eller andre sanktioner, der er fastsat i de nationale regler til gennemførelse af dette direktiv.

(131) Medlemsstaterne bør kunne fastsætte regler om strafferetlige sanktioner for overtrædelse af de nationale regler til gennemførelse af dette direktiv. Dog bør pålæggelse af strafferetlige sanktioner for overtrædelse af sådanne nationale regler og af tilknyttede administrative sanktioner ikke føre til et brud på princippet ne bis in idem som fortolket af Den Europæiske Unions Domstol.

(132) Hvor dette direktiv ikke harmoniserer administrative sanktioner eller hvor det i andre tilfælde er nødvendigt, f.eks. i tilfælde af en alvorlig overtrædelse af dette direktiv, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Sanktionernes art, herunder om de skal

være strafferetlige eller administrative, bør fastsættes ved national ret.

(133) For yderligere at styrke effektiviteten og den afskrækkende virkning af de håndhævelsesforanstaltninger, der finder anvendelse på overtrædelser af dette direktiv, bør de kompetente myndigheder have beføjelse til midlertidigt at suspendere eller anmode om en midlertidig suspension af en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, der leveres, eller aktiviteter, der udføres, af en væsentlig enhed, og kræve, at der indføres et midlertidigt forbud mod udøvelsen af ledelsesfunktioner for enhver fysisk person, der har ledelsesansvar på direktionsniveau eller som juridisk repræsentant. I betragtning af deres alvor og indvirkning på enhedernes aktiviteter og i sidste ende på brugerne bør sådanne midlertidige suspensioner eller forbud kun anvendes proportionalt med overtrædelsens alvor og under hensyntagen til omstændighederne i hver enkelttilfælde, herunder i lyset af, om overtrædelsen var forsætlig eller uagtsom, og ethvert tiltag, der er iværksat til at forebygge eller afbøde den materielle eller immaterielle skade. Sådanne midlertidige suspensioner eller forbud bør kun anvendes som en sidste udvej, dvs. først efter at de øvrige relevante håndhævelsesforanstaltninger, der er fastsat i dette direktiv, er udtømt, og kun indtil den pågældende enhed iværksætter de nødvendige tiltag for at afhjælpe manglerne eller opfylde kravene fra den kompetente myndighed, for hvilken sådanne midlertidige suspensioner eller forbud blev anvendt. Pålæggelse af sådanne midlertidige suspensioner eller forbud bør være underlagt passende proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og chartret, herunder adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar.

(134) For at sikre, at enhederne overholder deres forpligtelser fastsat i dette direktiv, bør medlemsstaterne samarbejde med og bistå hinanden med hensyn til tilsyns- og håndhævelsesforanstaltninger, navnlig hvor en enhed leverer tjenester i mere end én medlemsstat, eller hvor dens net- og informationssystemer er beliggende i en anden medlemsstat end den, hvori den leverer tjenesterne. Når den anmodede kompetente myndighed yder bistand, bør den træffe tilsyns- eller håndhævelsesforanstaltninger i overensstemmelse med national ret. For at sikre, at den gensidige bistand i

henhold til dette direktiv fungerer gnidningsløst, bør de kompetente myndigheder anvende samarbejdsgruppen som et forum til at drøfte sager og specifikke anmodninger om bistand.

(135) For at sikre effektivt tilsyn og effektiv håndhævelse, navnlig i en situation med en grænseoverskridende dimension, bør en medlemsstat, der har modtaget en anmodning om gensidig bistand, inden for rammerne af denne anmodning træffe passende tilsyns- og håndhævelsesforanstaltninger over for den enhed, der er genstand for denne anmodning, og som leverer tjenester eller har et net- og informationssystem på denne medlemsstats område.

(136) Dette direktiv bør fastlægge samarbejdsregler mellem de kompetente myndigheder og tilsynsmyndighederne i henhold til forordning (EU) 2016/679 med henblik på behandling af overtrædelser af dette direktiv vedrørende personoplysninger.

(137) Dette direktiv bør sigte mod at sikre et højt ansvarsniveau for de væsentlige og vigtige enheders foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser. Derfor bør de væsentlige og vigtige enheders ledelsesorganer godkende foranstaltningerne til styring af cybersikkerhedsrisici og føre tilsyn med deres gennemførelse.

(138) For at sikre et højt fælles cybersikkerhedsniveau i hele Unionen på grundlag af dette direktiv bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF for så vidt angår supplering af dette direktiv ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning ([22]). For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(139) For at sikre ensartede betingelser for gennemførelsen af dette direktiv bør Kommissionen tillægges gennemførelsesbeføjelser til at fastlægge de proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion og de tekniske og metodologiske samt sektorspecifikke krav vedrørende foranstaltninger til styring af cybersikkerhedsrisici og til yderligere at præcisere typen af oplysninger, formatet og proceduren for underretning om hændelser, cybertrusler og nærvedhændelser og for kommunikation om væsentlige cybertrusler samt de tilfælde, hvor en hændelse skal anses for at være væsentlig. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 ([23]).

(140) Kommissionen bør regelmæssigt evaluere dette direktiv efter høring af interessenter, navnlig med henblik på at afgøre, om det er hensigtsmæssigt at foreslå ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår. Som led i disse evalueringer bør Kommissionen vurdere relevansen af størrelsen af de berørte enheder, sektorerne, delsektorerne og typerne af enheder omhandlet i dette direktivs bilag for, hvordan økonomien og samfundet fungerer i relation til cybersikkerhed. Kommissionen bør bl.a. vurdere, hvorvidt udbydere, der er omfattet af dette direktivs anvendelsesområde og er udpeget som meget store onlineplatforme i den i artikel 33 i Europa-Parlamentets og Rådets forordning (EU) 2022/2065 ([24]) anvendte betydning, vil kunne identificeres som væsentlige enheder i henhold til dette direktiv.

(141) Dette direktiv tildeler ENISA nye opgaver og styrker derved dets rolle og vil også kunne resultere i, at ENISA vil skulle udføre sine eksisterende opgaver i henhold til forordning (EU) 2019/881 på et højere niveau end tidligere. For at sikre, at ENISA har de nødvendige finansielle og menneskelige ressourcer til at udføre eksisterende og nye opgaver samt til at opnå et højere gennemførelsesniveau for disse opgaver som følge af sin styrkede rolle, bør dets budget forhøjes tilsvarende. For at sikre en effektiv anvendelse af ressourcerne bør ENISA desuden gives større handlefrihed i sin interne ressourcefordeling for at sætte det i stand til at udføre sine opgaver effektivt og indfri forventningerne.

(142)Målene for dette direktiv, nemlig at opnå et højt, fælles cybersikkerhedsniveau i hele Unionen, kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af handlingens virkninger bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(143)Dette direktiv respekterer de grundlæggende rettigheder og overholder de principper, som anerkendes i chartret, navnlig retten til respekt for privatliv og kommunikation og retten til beskyttelse af personoplysninger, friheden til at oprette og drive egen virksomhed, ejendomsretten, adgangen til effektive retsmidler og retten til en retfærdig rettergang, uskyldsformodningen og retten til et forsvar. Adgangen til effektive retsmidler gælder også modtagere af tjenester, der leveres af væsentlige og vigtige enheder. Direktivet bør gennemføres i overensstemmelse med disse rettigheder og principper.

(144)Den Europæiske Tilsynsførende for Databeskyttelse er blevet hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([25]) og afgav en udtalelse den 11. marts 2021 ([26]) —

VEDTAGET DETTE DIREKTIV:

KAPITEL I
GENERELLE BESTEMMELSER

Artikel 1

Genstand

1. Dette direktiv fastlægger foranstaltninger, der sigter på at opnå et højt fælles cybersikkerhedsniveau i hele Unionen med henblik på at forbedre det indre markeds funktion.

2. Med henblik herpå fastlægger dette direktiv:

a) forpligtelser, der kræver, at medlemsstaterne vedtager nationale cybersikkerhedsstrategier og udpeger eller opretter kompetente myndigheder, cyberkrisestyringsmyndigheder, centrale kontaktpunkter

for cybersikkerhed (centrale kontaktpunkter) og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

b) foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser for enheder af den type, der er omhandlet i bilag I eller II, samt for enheder, der er udpeget som kritiske enheder i henhold til direktiv (EU) 2022/2557

c) regler og forpligtelser vedrørende udveksling af cybersikkerhedsoplysninger

d)tilsyns- og håndhævelsesforpligtelser for medlemsstaterne.

Artikel 2

Anvendelsesområde

1. Dette direktiv finder anvendelse på offentlige eller private enheder af den type, der er omhandlet i bilag I eller II, som udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til henstilling 2003/361/EF, eller overskrider tærsklerne for mellemstore virksomheder fastsat i nævnte artikels stk. 1, og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen.

Artikel 3, stk. 4, i bilaget til nævnte henstilling finder ikke anvendelse for så vidt angår dette direktiv.

2. Uanset deres størrelse finder dette direktiv også anvendelse på enheder af den type, der er omhandlet i bilag I eller II, hvor:

a) tjenester leveres af:

i) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester

ii) tillidstjenesteudbydere

iii) topdomænenavneadministratorer og udbydere af domænenavnesystemer

b) enheden er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter

c) en forstyrrelse af den tjeneste, enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden

d) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning

e) enheden er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i medlemsstaten

f) enheden er en offentlig forvaltningsenhed:

i) under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret eller

ii) på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret, som efter en risikobaseret vurdering leverer tjenester, hvis forstyrrelse vil kunne have væsentlig indvirkning på kritiske samfundsmæssige eller økonomiske aktiviteter.

3. Uanset deres størrelse, finder dette direktiv anvendelse på enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557.

4. Uanset deres størrelse, finder dette direktiv anvendelse på enheder, der leverer domænenavnsregistreringstjenester.

5. Medlemsstater kan fastsætte, at dette direktiv finder anvendelse på:

a) offentlige forvaltningsenheder på lokalt plan

b) uddannelsesinstitutioner, navnlig hvor de udfører kritiske forskningsaktiviteter.

6. Dette direktiv berører ikke medlemsstaternes ansvar for at beskytte national sikkerhed og deres beføjelse til at beskytte andre væsentlige statslige funktioner, herunder sikring af statens territoriale integritet og opretholdelse af lov og orden.

7. Dette direktiv finder ikke anvendelse på offentlige forvaltningsenheder, der udfører deres aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger.

8. Medlemsstater kan undtage specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse, herunder forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, eller som udelukkende leverer tjenester til de offentlige forvaltningsenheder, der er omhandlet i denne artikels stk. 7, fra forpligtelserne i artikel 21 eller 23 for så vidt angår disse aktiviteter eller tjenester. I så fald finder de i kapitel VII omhandlede tilsyns- og håndhævelsesforanstaltninger ikke anven-

delse i forbindelse med disse specifikke aktiviteter eller tjenester. Hvor enhederne udelukkende udfører aktiviteter eller leverer tjenester af den type, der er omhandlet i dette stykke, kan medlemsstater beslutte også at fritage disse enheder for forpligtelserne i artikel 3 og 27.

9. Stk. 7 og 8 finder ikke anvendelse, hvor en enhed fungerer som tillidstjenesteudbyder.

10. Dette direktiv finder ikke anvendelse på enheder, som medlemsstaterne har undtaget fra anvendelsesområdet for forordning (EU) 2022/2554 i overensstemmelse med artikel 2, stk. 4, i nævnte forordning.

11. De forpligtelser, der er fastsat i dette direktiv, omfatter ikke meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar.

12. Dette direktiv berører ikke forordning (EU) 2016/679, direktiv 2002/58/EF, Europa-Parlamentets og Rådets direktiv 2011/93/EU ([27]) og 2013/40/EU ([28]) samt direktiv (EU) 2022/2557.

13. Uden at det berører artikel 346 i TEUF, udveksles oplysninger, der er fortrolige i henhold til EU-regler eller nationale regler, såsom regler om forretningshemmeligheder, kun med Kommissionen og andre relevante myndigheder i overensstemmelse med dette direktiv, hvor denne udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger begrænses til, hvad der er relevant og forholdsmæssigt under hensyn til formålet med udvekslingen. Udvekslingen af oplysninger skal bevare de pågældende oplysningers fortrolighed og beskytte de berørte enheders sikkerhed og kommercielle interesser.

14. Enheder, de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne behandler personoplysninger i det omfang, det er nødvendigt med henblik på dette direktiv og i overensstemmelse med forordning (EU) 2016/679, navnlig på grundlag af artikel 6 deri.

Når udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester behandler personoplysninger i medfør af dette direktiv, skal det ske i overensstemmelse med EU-databeskyttelsesret og EU-retten om privatlivets fred, navnlig direktiv 2002/58/EF.

Artikel 3

Væsentlige og vigtige enheder

1. Med henblik på dette direktiv anses følgende enheder for at være væsentlige enheder:

a) enheder af en type, som er omhandlet i bilag I og som overskrider tærsklerne for mellemstore virksomheder, der er fastsat i artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF

b) kvalificerede tillidstjenesteudbydere og topdomænenavneadministratorer samt DNS-tjenesteudbydere, uanset deres størrelse

c) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, der udgør mellemstore virksomheder i henhold til artikel 2, i bilaget til henstilling 2003/361/EF

d) offentlige forvaltningsenheder omhandlet i artikel 2, stk. 2, litra f), nr. i)

e) alle andre enheder af en type omhandlet i bilag I eller II, som en medlemsstat har identificeret som væsentlige enheder i medfør af artikel 2, stk. 2, litra b)-e)

f) enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557, jf. artikel 2, stk. 3, i nærværende direktiv

g) hvis medlemsstaten træffer afgørelse herom, enheder, som den pågældende medlemsstat inden den 16. januar 2023 har identificeret som operatører af væsentlige tjenester i overensstemmelse med direktiv (EU) 2016/1148 eller national ret.

2. Med henblik på dette direktiv anses enheder af en type omhandlet i bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til denne artikels stk. 1, for at være vigtige enheder. Dette indbefatter enheder, som medlemsstaterne har identificeret som vigtige enheder i medfør af artikel 2, stk. 2, litra b)-e).

3. Senest den 17. april 2025 udarbejder medlemsstaterne en liste over væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester. Medlemsstaterne reviderer og, hvor det er relevant, ajourfører derefter listen med jævne mellemrum, mindst hvert andet år.

4. Med henblik på udarbejdelsen af den i stk. 3 omhandlede liste pålægger medlemsstaterne de enheder, der er omhandlet i nævnte stykke,

at indgive mindst følgende oplysninger til de kompetente myndigheder:

a) enhedens navn

b) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre

c) i givet fald den relevante sektor og delsektor i bilag I eller II, samt

d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af dette direktivs anvendelsesområde.

De i stk. 3 omhandlede enheder skal i tilfælde af ændringer af de oplysninger, de har indgivet i henhold til nærværende stykkes første afsnit, straks give underretning herom og under alle omstændigheder senest to uger efter datoen for ændringen.

Kommissionen fastlægger med bistand fra Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) uden unødigt ophold retningslinjer og skabeloner vedrørende de forpligtelser, der er fastsat i dette stykke.

Medlemsstaterne kan indføre nationale mekanismer, hvorigennem enheder kan registrere sig selv.

5. Senest den 17. april 2025 og derefter hvert andet år underretter de kompetente myndigheder:

a) Kommissionen og samarbejdsgruppen om antallet af væsentlige og vigtige enheder, der er opført på den i stk. 3 omhandlede liste for hver af de sektorer og delsektorer, der er omhandlet i bilag I eller II, samt

b) Kommissionen om relevante oplysninger med hensyn til antallet af væsentlige og vigtige enheder, der er identificeret i medfør af artikel 2, stk. 2, litra b)-e), hvilke af sektorerne og delsektorerne i bilag I eller II, som de tilhører, hvilken type tjeneste de leverer, og hvilken af bestemmelserne i artikel 2, stk. 2, litra b)-e), i medfør af hvilken de blev identificeret.

6. Indtil til den 17. april 2025 og efter anmodning fra Kommissionen kan medlemsstaterne underrette Kommissionen om navnene på de væsentlige og vigtige enheder, der er omhandlet i stk. 5, litra b).

Artikel 4

Sektorspecifikke EU-retsakter

1. I tilfælde, hvor sektorspecifikke EU-retsakter kræver, at væsentlige eller vigtige enheder træffer foranstaltninger til styring af cybersikkerhedsrisici eller underretter om væsentlige hændelser, og hvor disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, finder de relevante bestemmelser i dette direktiv, herunder bestemmelserne om tilsyn og håndhævelse, der er fastsat i kapitel VII, ikke finde anvendelse på sådanne enheder. I tilfælde, hvor sektorspecifikke EU-retsakter ikke omfatter alle enheder i en specifik sektor, der er omfattet af dette direktivs anvendelsesområde, finder de relevante bestemmelser i dette direktiv fortsat anvendelse på de enheder, der ikke er omfattet af de nævnte sektorspecifikke EU-retsakter.

2. De i denne artikels stk. 1 omhandlede krav anses for at have samme virkning som de forpligtelser, der er fastsat i dette direktiv, hvor:

a) foranstaltningerne til styring af cybersikkerhedsrisici har mindst samme virkning som dem, der er fastsat i artikel 21, stk. 1 og 2, eller

b) den sektorspecifikke EU-retsakt giver CSIRT'erne, de kompetente myndigheder eller de centrale kontaktpunkter i henhold til dette direktiv øjeblikkelig, hvor relevant automatisk og direkte, adgang til underretninger om hændelser, og hvor kravene om at give underretning om væsentlige hændelser mindst har samme virkning som kravene fastsat i dette direktivs artikel 23, stk. 1-6.

3. Kommissionen fastlægger senest den 17. juli 2023 retningslinjer, der præciserer anvendelsen af stk. 1 og 2. Kommissionen reviderer regelmæssigt disse retningslinjer. Ved udarbejdelsen af disse retningslinjer tager Kommissionen hensyn til eventuelle bemærkninger fra samarbejdsgruppen og ENISA.

Artikel 5

Minimumsharmonisering

Dette direktiv er ikke til hinder for, at medlemsstaterne vedtager eller opretholder bestemmelser, der sikrer et højere cybersikkerhedsniveau, forudsat at sådanne bestemmelser er i overensstemmelse med medlemsstaternes forpligtelser, der er fastsat i EU-retten.

Artikel 6

Definitioner

I dette direktiv forstås ved:

1) »net- og informationssystem«:

   a) et elektronisk kommunikationsnet som defineret i artikel 2, nr. 1), i direktiv (EU) 2018/1972

   b) enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, eller

   c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse

2) »sikkerhed i net- og informationssystemer«: net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer

3) »cybersikkerhed«: cybersikkerhed som defineret i artikel 2, nr. 1), i forordning (EU) 2019/881

4) »national cybersikkerhedsstrategi«: en medlemsstats sammenhængende ramme, der opstiller strategiske mål og prioriteter på cybersikkerhedsområdet og styringen for at nå dem i den pågældende medlemsstat

5) »nærvedhændelse«: en begivenhed, der kunne have bragt tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre i at materialisere sig, eller som ikke materialiserede sig

6) »hændelse«: en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare

7) »omfattende cybersikkerhedshændelse«: en hændelse, der forårsager en forstyrrelse på et niveau, som overstiger en medlemsstats kapacitet til at reagere på den, eller som har en betydelig indvirkning på mindst to medlemsstater

8) »håndtering af hændelser«: enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse

9) »risiko«: potentialet for tab eller forstyrrelse som følge af en hændelse, udtrykt som en kombination af størrelsen af et sådant tab eller en sådan forstyrrelse og sandsynligheden for, at hændelsen indtræffer

10) »cybertrussel«: en cybertrussel som defineret i artikel 2, nr. 8), i forordning (EU) 2019/881

11) »væsentlig cybertrussel«: en cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en enheds net- og informationssystemer eller på brugerne af enhedens tjenester ved at forårsage betydelig materiel eller immateriel skade

12) »IKT-produkt«: et IKT-produkt som defineret i artikel 2, nr. 12), i forordning (EU) 2019/881

13) »IKT-tjeneste«: en IKT-tjeneste som defineret i artikel 2, nr. 13), i forordning (EU) 2019/881

14) »IKT-proces«: en IKT-proces som defineret i artikel 2, nr. 14), i forordning (EU) 2019/881

15) »sårbarhed«: en svaghed, modtagelighed eller fejl ved IKT-produkter eller -tjenester, som kan udnyttes af en cybertrussel

16) »standard«: standard som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([29])

17) »teknisk specifikation«: en teknisk specifikation som defineret i artikel 2, nr. 4), i forordning (EU) nr. 1025/2012

18) »internetudvekslingspunkt« en netfacilitet, som muliggør sammenkobling af mere end to uafhængige net (autonome systemer), hovedsageligt med henblik på at lette udvekslingen af internettrafik, som kun leverer sammenkobling til autonome systemer og som hverken kræver, at internettrafik, som bevæger sig mellem et givent par af deltagende autonome systemer, passerer gennem et eventuelt tredje autonomt system, eller ændrer eller på anden måde griber ind i en sådan trafik

19) »domænenavnesystem« eller »DNS«: et hierarkisk distribueret navngivningssystem, der gør det muligt at identificere internettjenester og -ressourcer, således at slutbrugerudstyr kan benytte inter-

netrouting- og konnektivitetstjenester til at nå disse tjenester og ressourcer

20) »DNS-tjenesteudbyder«: en enhed, der leverer:

a) offentligt tilgængelige rekursive domænenavnsoversættelsestjenester til internetslutbrugere, eller

b) autoritative domænenavnsoversættelsestjenester til tredjepartsbrug, med undtagelse af rodnavneservere

21) »topdomænenavneadministrator«: en enhed, der har fået uddelegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, hvilket inkluderer driften af dets navneservere, vedligeholdelsen af dets databaser og distributionen af topdomænezonefiler til navneservere, uanset om hvorvidt nogen af disse operationer udføres af enheden selv eller outsources, men ikke situationer, hvor topdomænenavne kun anvendes af en administrator til eget brug

22) »enhed, der leverer domænenavnsregistreringstjenester«: en registrator eller en agent, der handler på vegne af registratorer, såsom en udbyder eller videresælger af privatlivs- eller proxyregistreringstjenester

23) »digital tjeneste«: en tjeneste som defineret i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 ([30])

24) »tillidstjeneste«: en tillidstjeneste som defineret i artikel 3, nr. 16), i forordning (EU) nr. 910/2014

25) »tillidstjenesteudbyder«: en tillidstjenesteudbyder som defineret i artikel 3, nr. 19), i forordning (EU) nr. 910/2014

26) »kvalificeret tillidstjeneste«: en kvalificeret tillidstjeneste som defineret i artikel 3, nr. 17), i forordning (EU) nr. 910/2014

27) »kvalificeret tillidstjenesteudbyder«: en kvalificeret tillidstjenesteudbyder som defineret i artikel 3, nr. 20), i forordning (EU) nr. 910/2014

28) »onlinemarkedsplads«: en onlinemarkedsplads som defineret i artikel 2, litra n), i Europa-Parlamentets og Rådets direktiv 2005/29/EF ([31])

29) »onlinesøgemaskine«: en onlinesøgemaskine som defineret i artikel 2, nr. 5), i Europa-Parlamentets og Rådets forordning (EU) 2019/1150 ([32])

30) »cloudcomputingtjeneste«: en digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og elastisk pulje af delbare computerressourcer, herunder hvor disse ressourcer er fordelt mellem flere lokaliteter

31) »datacentertjeneste«: en tjeneste, der omfatter strukturer eller grupper af strukturer, der er beregnet til central opbevaring, sammenkobling og drift af IT- og netværksudstyr, der leverer datalagrings-, -behandlings- og -transporttjenester samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol

32) »indholdsleveringsnetværk«: et net af geografisk distribuerede servere med det formål at sikre høj tilgængelighed af, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere

33) »platform for sociale netværkstjenester«: en platform, der sætter slutbrugere i stand til at komme i forbindelse, dele, opdage og kommunikere med hinanden på tværs af forskellige anordninger, navnlig via chats, opslag, videoer og anbefalinger

34) »repræsentant«: en fysisk eller juridisk person, der er etableret i Unionen, som udtrykkeligt er udpeget til at handle på vegne af en DNS-tjenesteudbyder, en topdomænenavneadministrator, en enhed, der leverer domænenavnsregistreringstjenester eller en udbyder af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som ikke er etableret i Unionen, og som kan kontaktes af en kompetent myndighed eller en CSIRT på enhedens sted for så vidt angår denne enheds forpligtelser i henhold til dette direktiv

35) »offentlig forvaltningsenhed«: en enhed, der er anerkendt som sådan i en medlemsstat i overensstemmelse med national ret, med undtagelse af retsvæsenet, parlamenter og centralbanker, som opfylder følgende kriterier:

   a) den er oprettet med henblik på at opfylde almennyttige formål og har ikke industriel eller kommerciel karakter

   b) den har status som juridisk person, eller den er ved lov berettiget til at handle på vegne af en anden enhed med status som juridisk person

c) den finansieres overvejende af staten, regionale myndigheder eller af andre offentligretlige organer, er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale myndigheder eller andre offentligretlige organer

d) den har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelighed for personer, varer, tjenester eller kapital

36) »offentligt elektronisk kommunikationsnet«: et offentligt elektronisk kommunikationsnet som defineret i artikel 2, nr. 8), i direktiv (EU) 2018/1972

37) »elektronisk kommunikationstjeneste«: en elektronisk kommunikationstjeneste som defineret i artikel 2, nr. 4), i direktiv (EU) 2018/1972

38) »enhed«: en fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale ret på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser

39) »udbyder af administrerede tjenester«: en enhed, der leverer tjenester i forbindelse med installation, administration, drift eller vedligeholdelse af IKT-produkter, -net, -infrastruktur, -applikationer eller andre net- og informationssystemer via assistance eller aktiv administration, der udføres enten i kundernes lokaler eller på afstand

40) »udbyder af administrerede sikkerhedstjenester«: en udbyder af administrerede tjenester, der udfører eller yder assistance til aktiviteter vedrørende styring af cybersikkerhedsrisici

41) »forskningsorganisation«: en enhed, hvis primære mål er at udføre anvendt forskning eller udvikling med henblik på at udnytte resultaterne af denne forskning til kommercielle formål, men som ikke indbefatter uddannelsesinstitutioner.

KAPITEL II

KOORDINEREDE RAMMER FOR CYBERSIKKERHED

Artikel 7

National cybersikkerhedsstrategi

1. Hver medlemsstat vedtager en national cybersikkerhedsstrategi, der fastlægger de strategiske mål, de nødvendige ressourcer til at nå disse mål, og passende politiske og lovgivningsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau. Den nationale cybersikkerhedsstrategi skal omfatte:

a) mål og prioriteter for medlemsstatens cybersikkerhedsstrategi, navnlig for de sektorer, der er omhandlet i bilag I og II

b) en styringsramme med henblik på at nå de i dette stykkes litra a) omhandlede mål og prioriteter, herunder de politikker, der er omhandlet i stk. 2

c) en styringsramme, der præciserer de relevante interessenters roller og ansvarsområder på nationalt plan og understøtter samarbejdet og koordineringen på nationalt plan mellem de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne i henhold til dette direktiv samt koordinering og samarbejde mellem disse organer og kompetente myndigheder i henhold til sektorspecifikke EU-retsakter

d) en mekanisme til at identificere relevante aktiver og en vurdering af risiciene i den pågældende medlemsstat

e) en identifikation af de foranstaltninger, der sikrer beredskabet for og evnen til at reagere på og reetablere sig efter hændelser, herunder samarbejde mellem den offentlige og den private sektor

f) en liste over de forskellige myndigheder og interessenter, der er involveret i gennemførelsen af den nationale cybersikkerhedsstrategi

g) en politisk ramme for øget koordinering mellem de kompetente myndigheder i henhold til dette direktiv og de kompetente myndigheder i henhold til direktiv (EU) 2022/2557 med henblik på udveksling af oplysninger om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser og udøvelse af tilsynsopgaver, alt efter hvad der er relevant.

h) en plan, herunder med de nødvendige foranstaltninger, for højnelse af borgernes generelle bevidsthed om cybersikkerhed.

2. Som led i den nationale cybersikkerhedsstrategi skal medlemsstaterne navnlig vedtage politikker for:

a) håndtering af cybersikkerhed i forsyningskæden for IKT-produkter og -tjenester, der anvendes af enheder til levering af deres tjenester

b) inklusion og specificering af cybersikkerhedsrelaterede krav til IKT-produkter og -tjenester i forbindelse med offentlige indkøb, herunder vedrørende cybersikkerhedscertificering, kryptering og brugen af open source-cybersikkerhedsprodukter

c) håndtering af sårbarheder, der omfatter fremme og facilitering af koordineret offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1

d) opretholdelse af den generelle tilgængelighed, integritet og fortrolighed af den offentlige centrale del af det åbne internet, herunder, hvor det er relevant, undersøiske kommunikationskablers cybersikkerhed

e) fremme af udviklingen og integrationen af relevante avancerede teknologier, der har til formål at gennemføre foranstaltninger på det aktuelle teknologiske stade til styring af cybersikkerhedsrisici

f) fremme og udvikling af uddannelse i cybersikkerhed, cybersikkerhedsfærdigheder, -bevidstgørelse og -forskning og -udviklingsinitiativer samt vejledning om god praksis for og kontrol med cyberhygiejne rettet mod borgere, interessenter og enheder

g) støtte til akademiske institutioner og forskningsinstitutioner med henblik på at udvikle, forbedre og fremme udbredelsen af cybersikkerhedsværktøjer og sikker netinfrastruktur

h) indførelse af relevante procedurer og passende informationsdelingsværktøjer til støtte for frivillig udveksling af cybersikkerhedsoplysninger mellem enheder i overensstemmelse med EU-retten

i) styrkelse af den grundlæggende cyberrobusthed og cyberhygiejne i små og mellemstore virksomheder, navnlig dem, der er udelukket fra dette direktivs anvendelsesområde, ved at yde let tilgængelig vejledning og bistand til opfyldelse af deres specifikke behov

j) fremme af aktiv cyberbeskyttelse.

3. Medlemsstaterne underretter Kommissionen om deres nationale cybersikkerhedsstrategier senest tre måneder efter vedtagelsen deraf. Medlemsstaterne kan udelade oplysninger, der vedrører deres nationale sikkerhed, fra sådanne underretninger.

4. Regelmæssigt og mindst hvert femte år vurderer og om fornødent ajourfører medlemsstaterne deres nationale cybersikkerhedsstrategier

på grundlag af centrale præstationsindikatorer. ENISA bistår på anmodning medlemsstaterne med at udvikle eller ajourføre en national strategi og nøgleresultatindikatorer til vurdering af denne strategi med henblik på at bringe den i overensstemmelse med de krav og forpligtelser, der er fastsat i dette direktiv.

Artikel 8

Kompetente myndigheder og centrale kontaktpunkter

1. Hver medlemsstat udpeger eller opretter en eller flere kompetente myndigheder med ansvar for cybersikkerhed og for de tilsynsopgaver, der er omhandlet i kapitel VII (kompetente myndigheder).

2. De i stk. 1 omhandlede kompetente myndigheder fører tilsyn med gennemførelsen af dette direktiv på nationalt plan.

3. Hver medlemsstat udpeger eller opretter et centralt kontaktpunkt. Hvor en medlemsstat kun udpeger eller opretter én kompetent myndighed i henhold til stk. 1, skal denne kompetente myndighed også være det centrale kontaktpunkt i den pågældende medlemsstat.

4. Hvert enkelt centrale kontaktpunkt udøver en forbindelsesfunktion for at sikre grænseoverskridende samarbejde mellem dets medlemsstats myndigheder og andre medlemsstaters relevante myndigheder og, hvor det er relevant, Kommissionen og ENISA, samt for at sikre tværsektorielt samarbejde med andre kompetente myndigheder i dets medlemsstat.

5. Medlemsstaterne sikrer, at deres kompetente myndigheder og centrale kontaktpunkter har tilstrækkelige ressourcer til på en effektiv måde at udføre de opgaver, som de pålægges, og dermed opfylde dette direktivs mål.

6. Hver medlemsstat underretter uden unødigt ophold Kommissionen om identiteten af den i stk. 1 omhandlede kompetente myndighed og af det i stk. 3 omhandlede centrale kontaktpunkt, om disse myndigheders opgaver og om enhver senere ændring heraf. Hver medlemsstat offentliggør sin kompetente myndigheds identitet. Kommissionen gør en liste over de centrale kontaktpunkter offentligt tilgængelig.

Artikel 9

Nationale rammer for cyberkrisestyring

1. Hver medlemsstat udpeger eller opretter en eller flere kompetente myndigheder med ansvar for styring af omfattende cybersikkerheds-

hændelser og kriser (cyberkrisestyringsmyndigheder). Medlemsstaterne sikrer, at disse myndigheder har tilstrækkelige ressourcer til at udføre de opgaver, de pålægges, på en virkningsfuld og effektiv måde. Medlemsstaterne sikrer sammenhængen med de eksisterende rammer for generel national krisestyring.

2. Hvor en medlemsstat udpeger eller opretter mere end én cyberkrisestyringsmyndighed i henhold til stk. 1, skal den klart angive, hvilken af disse myndigheder der skal fungere som koordinator for styringen af omfattende cybersikkerhedshændelser og kriser.

3. Hver medlemsstat identificerer kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise inden for rammerne af dette direktiv.

4. Hver medlemsstat vedtager en national beredskabsplan for omfattende cybersikkerhedshændelser og kriser, hvor målene og ordningerne for håndtering af omfattende cybersikkerhedshændelser og kriser er fastsat. Denne plan skal navnlig fastlægge:

a)målene for de nationale beredskabsforanstaltninger og –aktiviteter

b)cyberkrisestyringsmyndighedernes opgaver og ansvarsområder

c) cyberkrisestyringsprocedurerne, herunder deres integration i den generelle nationale krisestyringsramme, og kanalerne for udveksling af oplysninger

d) nationale beredskabsforanstaltninger, herunder øvelses- og uddannelsesaktiviteter

e) de relevante involverede offentlige og private interessenter og infrastrukturer

f) nationale procedurer og ordninger mellem relevante nationale myndigheder og organer for at sikre medlemsstatens effektive deltagelse i og støtte til den koordinerede håndtering af omfattende cybersikkerhedshændelser og kriser på EU-plan.

5. Senest tre måneder efter udpegelsen eller oprettelsen af den i stk. 1 omhandlede cyberkrisestyringsmyndighed underretter hver medlemsstat Kommissionen om sin myndigheds identitet og om eventuelle senere ændringer heraf. Medlemsstaterne forelægger senest tre måneder efter vedtagelsen af deres nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser Kommissionen og det europæiske netværk af cybersikkerhedsforbindelsesorganisationer (EU-CyCLONe) relevante oplysninger vedrørende de i stk. 4 indeholdte

krav til disse planer. Medlemsstaterne kan udelade oplysninger, hvor og i det omfang en sådan udeladelse er nødvendig for deres nationale sikkerhed.

Artikel 10

Enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

1. Hver medlemsstat udpeger eller opretter en eller flere CSIRT'er. CSIRT'erne kan udpeges eller oprettes inden for en kompetent myndighed. CSIRT'erne skal opfylde kravene i artikel 11, stk. 1, mindst dække de sektorer, delsektorer og typer af enheder, der er omhandlet i bilag I og II, og være ansvarlige for håndtering af hændelser i overensstemmelse med en nøje fastlagt proces.

2. Medlemsstaterne sikrer, at hver CSIRT har tilstrækkelige ressourcer til effektivt at udføre sine opgaver som fastsat i artikel 11, stk. 3.

3. Medlemsstaterne sikrer, at hver CSIRT råder over en passende, sikker og modstandsdygtig kommunikations- og informationsinfrastruktur til udveksling af oplysninger med væsentlige og vigtige enheder og andre relevante interessenter. Med henblik herpå sikrer medlemsstaterne, at hver CSIRT bidrager til udbredelsen af sikre værktøjer til udveksling af oplysninger.

4. CSIRT'erne samarbejder og, hvor det er relevant, udveksler relevante oplysninger i overensstemmelse med artikel 29 med sektorielle eller tværsektorielle fællesskaber af væsentlige og vigtige enheder.

5. CSIRT'erne deltager i peerevalueringer, der tilrettelægges i overensstemmelse med artikel 19.

6. Medlemsstaterne sikrer et effektivt og sikkert samarbejde mellem deres CSIRT'er i CSIRT-netværket.

7. CSIRT'erne kan etablere samarbejdsrelationer med tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser. Som led i sådanne samarbejdsrelationer skal medlemsstaterne lette effektiv og sikker udveksling af oplysninger med disse tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser, ved hjælp af relevante protokoller for udveksling af oplysninger, herunder Traffic Light Protocol. CSIRT'erne kan udveksle relevante oplysninger med tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser, herunder personoplysninger i overensstemmelse med EU-databeskyttelsesret.

8. CSIRT'erne kan samarbejde med tredjelandes nationale enheder, der håndterer IT-sikkerhedshændelser, eller tilsvarende organer i tredjelande, navnlig med henblik på at yde dem cybersikkerhedsbistand.

9. Hver medlemsstat underretter uden unødigt ophold Kommissionen om identiteten af den eller de i denne artikels stk. 1 omhandlede CSIRT'er og den CSIRT, der er udpeget som koordinator i henhold til artikel 12, stk. 1, om deres respektive opgaver i relation til væsentlige og vigtige enheder og om eventuelle efterfølgende ændringer heraf.

10. Medlemsstaterne kan anmode ENISA om bistand til at udvikle deres CSIRT'er.

Artikel 11

Krav til CSIRT'er og deres tekniske kapaciteter og opgaver

1. CSIRT'erne skal opfylde nedenstående krav:

a) CSIRT'erne skal sikre et højt tilgængelighedsniveau for deres kommunikationskanaler ved at undgå enkelte fejlpunkter og ved til enhver tid at have flere muligheder for at blive kontaktet og for at kontakte andre; de skal tydeligt angive kommunikationskanalerne og bringe dem til brugergruppers og samarbejdspartneres kundskab

b) CSIRT'ernes lokaler og de underliggende informationssystemer skal være placeret i sikrede lokaliteter

c) CSIRT'erne skal være udstyret med et passende system til at administrere og videresende anmodninger, navnlig med henblik på at lette effektive overdragelser

d) CSIRT'erne skal sikre fortroligheden og troværdigheden af deres operationer

e) CSIRT'erne skal have tilstrækkeligt personale til at sikre, at deres tjenester er tilgængelige på alle tidspunkter, og de skal sikre, at deres personale er behørigt uddannet

f) CSIRT'erne skal være udstyret med redundante systemer og backup-arbejdsplads for at sikre kontinuiteten af deres tjenester.

CSIRT'erne kan deltage i internationale samarbejdsnetværk.

2. Medlemsstaterne sikrer, at deres CSIRT'er i fællesskab har den tekniske kapacitet, der er nødvendig for at udføre de opgaver, der er omhandlet i stk. 3. Medlemsstaterne sikrer, at deres CSIRT'er har de fornødne ressourcer til at sikre et tilstrækkeligt personaleniveau, med

henblik på at gøre det muligt, at CSIRT'erne kan udvikle deres tekniske kapacitet.

3. CSIRT'erne har følgende opgaver:

a) overvågning og analyse af cybertrusler, sårbarheder og hændelser på nationalt plan og, efter anmodning, ydelse af bistand til væsentlige og vigtige enheder vedrørende realtids- eller nærrealtidsovervågning af deres net- og informationssystemer

b) tidlig varsling, alarmer, meddelelser og formidling af oplysninger til berørte væsentlige og vigtige enheder samt til de kompetente myndigheder og andre relevante interessenter om cybertrusler, sårbarheder og hændelser, om muligt i nærrealtid

c) at reagere på hændelser og i givet fald yde bistand til de berørte væsentlige og vigtige enheder

d) at indsamle og analysere kriminaltekniske data og udarbejde dynamiske risiko- og hændelsesanalyser og samt skabe situationsbevidsthed vedrørende cybersikkerhed

e) på anmodning af en væsentlig eller vigtig enhed at foretage en proaktiv scanning af den pågældende enheds net- og informationssystemer for at opdage sårbarheder med en potentielt væsentlig indvirkning

f) at deltage i CSIRT-netværket og yde gensidig bistand i overensstemmelse med deres kapacitet og kompetencer til andre medlemmer af CSIRT-netværket efter anmodning fra disse

g) i givet fald at fungere som koordinator med henblik på den koordinerede offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1

h) at bidrage til udbredelsen af sikre værktøjer til udveksling af oplysninger i henhold til artikel 10, stk. 3.

CSIRT'erne kan foretage proaktiv ikkeindgribende scanning af væsentlige og vigtige enheders offentligt tilgængelige net- og informationssystemer. En sådan scanning skal foretages for at opdage sårbare eller usikkert konfigurerede net- og informationssystemer og informere de berørte enheder. En sådan scanning må ikke have nogen negativ indvirkning på enhedernes tjenester.

Ved udførelsen af de opgaver, der er omhandlet i første afsnit, kan CSIRT'erne prioritere særlige opgaver på grundlag af en risikobaseret tilgang.

4. CSIRT'erne etablerer samarbejdsrelationer med relevante interessenter i den private sektor med henblik på at nå dette direktivs mål.

5. For at lette det i stk. 4 omhandlede samarbejde fremmer CSIRT'erne vedtagelsen og anvendelsen af fælles eller standardiserede praksisser, klassificeringsordninger og taksonomier i forbindelse med:

a) procedurer for håndtering af hændelser

b) krisestyring og

c) koordineret offentliggørelse af sårbarheder i henhold til artikel 12, stk. 1.

Artikel 12

Koordineret offentliggørelse af sårbarheder og en europæisk sårbarhedsdatabase

1. Hver medlemsstat udpeger en af sine CSIRT'er som koordinator med henblik på koordineret offentliggørelse af sårbarheder. Den CSIRT, der er udpeget som koordinator, fungerer som betroet formidler, der, hvor det er nødvendigt, letter interaktionen mellem den fysiske eller juridiske person, der rapporterer en sårbarhed, og producenten eller udbyderen af de potentielt sårbare IKT-produkter eller -tjenester på anmodning fra en af parterne. Opgaverne for den CSIRT, der er udpeget som koordinator, omfatter:

a) identifikation af og kontakt til de berørte enheder

b) bistand til de fysiske eller juridiske personer, der rapporterer en sårbarhed og

c) forhandling af tidsfrister for offentliggørelse og håndtering af sårbarheder, der berører flere enheder.

Medlemsstaterne sikrer, at fysiske eller juridiske personer er i stand til at rapportere en sårbarhed, anonymt hvor de anmoder herom, til den CSIRT, der er udpeget som koordinator. Den CSIRT, der er udpeget som koordinator, sørger for omhyggelig opfølgning med hensyn til den rapporterede sårbarhed, og sikrer anonymiteten for den fysiske eller juridiske person, der rapporterer sårbarheden. Hvor en rapporteret sårbarhed vil kunne have en væsentlig indvirkning på enheder i mere end én medlemsstat, samarbejder den CSIRT, der er udpeget som koordinator for hver berørt medlemsstat, om nødvendigt med andre

CSIRT'er, der er udpeget som koordinatorer, inden for CSIRT-netværket.

2. ENISA udvikler og vedligeholder efter høring af samarbejdsgruppen en europæisk sårbarhedsdatabase. Med henblik herpå opretter og vedligeholder ENISA passende informationssystemer, -politikker og -procedurer og træffer de nødvendige tekniske og organisatoriske foranstaltninger til at garantere den europæiske sårbarhedsdatabases sikkerhed og integritet, navnlig med det formål at sætte enheder, uanset om de er omfattet af dettes direktivs anvendelsesområde, og deres leverandører af net- og informationssystemer, i stand til på frivillig basis at oplyse om og registrere offentligt kendte sårbarheder i IKT-produkter eller -tjenester. Alle interessenter skal have adgang til oplysningerne om sårbarhederne i den europæiske sårbarhedsdatabase. Denne database indeholder:

a) oplysninger, der beskriver sårbarheden

b) de berørte IKT-produkter eller -tjenester og sårbarhedens alvor med hensyn til de omstændigheder, hvorunder den kan udnyttes

c) tilgængeligheden af relaterede patches og, i mangel af tilgængelige patches, vejledning fastlagt af de kompetente myndigheder eller CSIRT'erne til brugere af sårbare IKT-produkter og -tjenester om, hvordan risiciene som følge af afslørede sårbarheder kan afbødes.

Artikel 13

Samarbejde på nationalt plan

1. Hvor de kompetente myndigheder, det centrale kontaktpunkt og CSIRT'erne i samme medlemsstat er adskilt fra hinanden, samarbejder de med hensyn til opfyldelsen af forpligtelserne, der er fastsat i dette direktiv.

2. Medlemsstaterne sikrer, at deres CSIRT'er eller i givet fald deres kompetente myndigheder modtager underretninger om væsentlige hændelser i henhold til artikel 23 og om hændelser, cybertrusler og nærvedhændelser i henhold til artikel 30.

3. Medlemsstaterne sikrer, at deres CSIRT'er eller i givet fald deres kompetente myndigheder oplyser deres centrale kontaktpunkter om underretninger om hændelser, cybertrusler og nærvedhændelser indgivet i henhold til dette direktiv.

4. For at sikre, at de kompetente myndigheders, de centrale kontaktpunkters og CSIRT'ernes opgaver og forpligtelser udføres effektivt,

sikrer medlemsstaterne i muligt omfang et passende samarbejde mellem disse organer og retshåndhævende myndigheder, databeskyttelsesmyndigheder, de nationale myndigheder i henhold til forordning (EF) nr. 300/2008 og (EU) 2018/1139, tilsynsorganerne i henhold til forordning (EU) nr. 910/2014, de kompetente myndigheder i henhold til forordning (EU) 2022/2554, de nationale tilsynsmyndigheder i henhold til direktiv (EU) 2018/1972, de kompetente myndigheder i henhold til direktiv (EU) 2022/2557, samt de kompetente myndigheder i henhold til andre sektorspecifikke EU-retsakter, i den pågældende medlemsstat.

5. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv og deres kompetente myndigheder i henhold til direktiv (EU) 2022/2557 regelmæssigt samarbejder og udveksler oplysninger vedrørende identifikation af kritiske enheder, om risici, cybertrusler og hændelser samt om ikke-cyberrelaterede risici, trusler og hændelser, som påvirker væsentlige enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557, og de foranstaltninger, der træffes som reaktion på sådanne risici, trusler og hændelser. Medlemsstaterne sikrer endvidere, at deres kompetente myndigheder i henhold til nærværende direktiv og deres kompetente myndigheder i henhold til forordning (EU) nr. 910/2014, forordning (EU) 2022/2554 og direktiv (EU) 2018/1972 regelmæssigt udveksler relevante oplysninger, herunder om relevante hændelser og cybertrusler.

6. Medlemsstaterne forenkler rapporteringen ved hjælp af tekniske midler for underretninger omhandlet i artikel 23 og 30.

KAPITEL III
SAMARBEJDE PÅ EU-PLAN OG INTERNATIONALT PLAN

Artikel 14

Samarbejdsgruppe

1. For at støtte og lette strategisk samarbejde og udvekslingen af oplysninger mellem medlemsstaterne samt for at styrke tillid og fortrolighed nedsættes der en samarbejdsgruppe.

2. Samarbejdsgruppen udfører sine opgaver på grundlag af toårige arbejdsprogrammer omhandlet i stk. 7.

3. Samarbejdsgruppen består af repræsentanter fra medlemsstaterne, Kommissionen og ENISA. Tjenesten for EU's Optræden Udadtil del-

tager som observatør i samarbejdsgruppens aktiviteter. De europæiske tilsynsmyndigheder (ESA'er) og de kompetente myndigheder i henhold til forordning (EU) 2022/2554 kan deltage i samarbejdsgruppens aktiviteter i overensstemmelse med artikel 47, stk. 1, i nævnte forordning.

Samarbejdsgruppen kan, hvor det er relevant, indbyde Europa-Parlamentet og repræsentanter for relevante interessenter til at deltage i dens arbejde.

Sekretariatsopgaverne varetages af Kommissionen.

4. Samarbejdsgruppen har følgende opgaver:

a) at vejlede de kompetente myndigheder vedrørende omsætningen og gennemførelsen af dette direktiv

b) at vejlede de kompetente myndigheder vedrørende udviklingen og gennemførelsen af politikker for koordineret offentliggørelse af sårbarheder som omhandlet i artikel 7, stk. 2, litra c)

c) at udveksle bedste praksis og oplysninger vedrørende gennemførelsen af dette direktiv, herunder vedrørende cybertrusler, hændelser og sårbarheder, nærvedhændelser, bevidstgørelsesinitiativer, uddannelse, øvelser og færdigheder, kapacitetsopbygning, standarder og tekniske specifikationer samt identifikation af væsentlige og vigtige enheder i medfør af artikel 2, stk. 2, litra b)-e)

d) at udveksle rådgivning og samarbejde med Kommissionen om nye politiske initiativer inden for cybersikkerhed og den overordnede sammenhæng mellem sektorspecifikke cybersikkerhedskrav

e) at udveksle rådgivning og samarbejde med Kommissionen om udkast til delegerede retsakter eller gennemførelsesretsakter vedtaget i henhold til dette direktiv

f) at udveksle bedste praksis og oplysninger med relevante EU-institutioner, -organer, -kontorer og -agenturer

g) at drøfte gennemførelsen af sektorspecifikke EU-retsakter, der indeholder bestemmelser om cybersikkerhed

h) hvor det er relevant, at drøfte rapporter om den i artikel 19, stk. 9, omhandlede peerevaluering og udarbejde konklusioner og henstillinger

i) at foretage koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder i overensstemmelse med artikel 22, stk. 1

j) at drøfte tilfælde af gensidig bistand, herunder erfaringer fra og resultater af grænseoverskridende fælles tilsynstiltag som omhandlet i artikel 37

k) på anmodning af en eller flere berørte medlemsstater at drøfte specifikke anmodninger om gensidig bistand som omhandlet i artikel 37

l) at yde strategisk vejledning til CSIRT-netværket og EU–CyCLONe om specifikke nye spørgsmål

m) at drøfte politikken for opfølgende foranstaltninger efter omfattende cybersikkerhedshændelser og kriser på grundlag af erfaringer fra CSIRT-netværket og EU-CyCLONe

n) at bidrage til cybersikkerhedskapaciteter i hele Unionen ved at lette udvekslingen af nationale embedsmænd gennem et kapacitetsopbygningsprogram, der omfatter personale fra kompetente myndigheder eller CSIRT'erne

o) at tilrettelægge regelmæssige fælles møder med relevante private interessenter fra hele Unionen for at drøfte samarbejdsgruppens aktiviteter og indsamle input om nye politiske udfordringer

p) at drøfte det arbejde, der udføres i forbindelse med cybersikkerhedsøvelser, herunder det arbejder, der udføres af ENISA

q) at fastlægge metodologien og de organisatoriske aspekter af de peerevalueringer, der er omhandlet i artikel 19, stk. 1, samt at fastlægge selvevalueringsmetoden for medlemsstaterne i overensstemmelse med artikel 19, stk. 5, med bistand fra Kommissionen og ENISA samt, i samarbejde med Kommissionen og ENISA, at udvikle adfærdskodekser, der understøtter de udpegede cybersikkerhedseksperters arbejdsmetoder, i overensstemmelse med artikel 19, stk. 6

r) at udarbejde rapporter med henblik på den evaluering, der er omhandlet i artikel 40, om de erfaringer, der er indhøstet på strategisk plan og fra peerevalueringer

s) regelmæssigt at drøfte og foretage en vurdering af situationen med hensyn til cybertrusler eller hændelser såsom ransomware.

Samarbejdsgruppen forelægger de i første afsnit, litra r), omhandlede rapporter for Kommissionen, Europa-Parlamentet og Rådet.

5. Medlemsstaterne sikrer effektivt og sikkert samarbejde mellem deres repræsentanter i samarbejdsgruppen.

6. Samarbejdsgruppen kan anmode CSIRT-netværket om en teknisk rapport om udvalgte emner.

7. Senest den 1. februar 2024 og derefter hvert andet år udarbejder samarbejdsgruppen et arbejdsprogram vedrørende tiltag, der skal iværksættes for at gennemføre dens mål og opgaver.

8. Kommissionen kan vedtage gennemførelsesretsakter, hvori der fastlægges proceduremæssige ordninger, som er nødvendige for samarbejdsgruppens funktion.

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 39, stk. 2.

Kommissionen udveksler rådgivning og samarbejder med samarbejdsgruppen om de udkast til gennemførelsesretsakter, der er omhandlet i dette stykkes første afsnit, i overensstemmelse med stk. 4, litra e).

9. Samarbejdsgruppen mødes regelmæssigt og i hvert fald mindst en gang om året med gruppen for kritiske enheders modstandsdygtighed, der er nedsat i henhold til direktiv (EU) 2022/2557, for at fremme og lette strategisk samarbejde og udvekslingen af oplysninger.

Artikel 15

CSIRT-netværket

1. Med henblik på at bidrage til skabelsen af tillid mellem medlemsstaterne og fremme hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne oprettes der et netværk af nationale CSIRT'er.

2. CSIRT-netværket består af repræsentanter for de CSIRT'er, der er udpeget eller oprettet i henhold til artikel 10, og IT-Beredskabsenheden for Unionens institutioner, organer og agenturer (CERT-EU). Kommissionen deltager i CSIRT-netværket som observatør. ENISA varetager sekretariatsopgaverne og bistår aktivt samarbejdet mellem CSIRT'erne.

3. CSIRT-netværket har følgende opgaver:

a) at udveksle oplysninger om CSIRT'ernes kapaciteter

b) at lette deling, overførsel og udveksling af teknologi og relevante foranstaltninger, politikker, værktøjer, processer, bedste praksisser og rammer mellem CSIRT'erne

c) at udveksle relevant information om hændelser, nærvedhændelser, cybertrusler, risici og sårbarheder

d) at udveksle information vedrørende cybersikkerhedspublikationer og –anbefalinger

e) at sikre interoperabilitet med hensyn til specifikationer og protokoller for informationsdeling

f) på anmodning af et medlem af CSIRT-netværket, der potentielt er berørt af en hændelse, at udveksle og drøfte oplysninger i forbindelse med denne hændelse og tilknyttede cybertrusler, risici og sårbarheder

g) på anmodning af et medlem af CSIRT-netværket at drøfte og, hvor det er muligt, gennemføre en samordnet reaktion på en hændelse, som er identificeret inden for den pågældende medlemsstats jurisdiktion

h) at yde medlemsstaterne bistand til håndtering af grænseoverskridende hændelser i henhold til dette direktiv

i) at samarbejde, udveksle bedste praksis og yde bistand til de CSIRT'er, der er udpeget som koordinatorer i henhold til artikel 12, stk. 1, med hensyn til forvaltningen af den koordinerede offentliggørelse af sårbarheder, som vil kunne have en væsentlig indvirkning på enheder i mere end én medlemsstat

j) at drøfte og identificere yderligere former for operationelt samarbejde, herunder i forhold til:

i) kategorier af cybertrusler og hændelser

ii) tidlig varsling

iii) gensidig bistand

iv) principper og ordninger for koordination som reaktion på grænseoverskridende risici og hændelser

v) bidrag til den nationale beredskabsplan for omfattende cybersikkerhedshændelser og kriser, der er omhandlet i artikel 9, stk. 4, efter anmodning fra en medlemsstat

k) at oplyse samarbejdsgruppen om sine aktiviteter og om yderligere former for operationelt samarbejde, som drøftes i henhold til litra j), og, hvor det er nødvendigt, anmode om vejledning i forbindelse hermed

l) at gøre status over cybersikkerhedsøvelser, herunder dem, der organiseres af ENISA

m) på anmodning af en individuel CSIRT at drøfte denne CSIRT's kapaciteter og beredskab

n) at samarbejde og udveksle information med regionale og EU-dækkende sikkerhedsoperationscentre (SOC'er) for at forbedre den fælles situationsbevidsthed om hændelser og cybertrusler i hele Unionen

o) hvor det er relevant, at drøfte de i artikel 19, stk. 9, omhandlede peerevalueringsrapporter

p) at fastlægge retningslinjer for at lette konvergensen mellem operationel praksis med hensyn til anvendelsen af bestemmelserne i denne artikel vedrørende operationelt samarbejde.

4. Med henblik på den i artikel 40 omhandlede evaluering vurderer CSIRT-netværket senest den 17. januar 2025 og derefter hvert andet år de fremskridt, der er gjort med hensyn til det operationelle samarbejde, og udarbejde en rapport. Rapporten indeholder navnlig konklusioner og henstillinger baseret på resultaterne af de i artikel 19 omhandlede peerevalueringer, der foretages vedrørende de nationale CSIRT'er. Rapporten skal forelægges for samarbejdsgruppen.

5. CSIRT-netværket vedtager sin forretningsorden.

6. CSIRT-netværket og EU-CyCLONe aftaler proceduremæssige ordninger og samarbejder på grundlag heraf.

Artikel 16

Det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe)

1. EU-CyCLONe oprettes for at støtte den koordinerede forvaltning af omfattende cybersikkerhedshændelser og kriser på operationelt plan og for at sikre regelmæssig udveksling af relevant information mellem medlemsstaterne og EU-institutioner, -organer, -kontorer og -agenturer.

2. EU-CyCLONe består af repræsentanter for medlemsstaternes cyberkrisestyringsmyndigheder samt, i tilfælde hvor en potentiel eller igangværende omfattende cybersikkerhedshændelse har eller sandsynligvis vil have en betydelig indvirkning på tjenester og aktiviteter, der er omfattet af dette direktivs anvendelsesområde, Kommissionen. I andre tilfælde deltager Kommissionen i EU-CyCLONe's aktiviteter som observatør.

ENISA varetager sekretariatsfunktionen for EU-CyCLONe og støtter sikker udveksling af oplysninger samt stiller de nødvendige værktøjer til rådighed for samarbejdet mellem medlemsstaterne med henblik på sikker udveksling af oplysninger.

EU-CyCLONe kan, hvor det er hensigtsmæssigt, indbyde repræsentanter for relevante interessenter til at deltage i dets arbejde som observatører.

3. EU-CyCLONe har følgende opgaver:

a) at øge beredskabsniveauet i forbindelse med håndtering af omfattende cybersikkerhedshændelser og kriser

b) at udvikle en fælles situationsbevidsthed om omfattende cybersikkerhedshændelser og kriser

c) at vurdere konsekvenserne og indvirkningen af relevante omfattende cybersikkerhedshændelser og kriser og foreslå mulige afbødende foranstaltninger

d) at koordinere håndteringen af omfattende cybersikkerhedshændelser og kriser og støtte beslutningstagningen på politisk plan i forbindelse med sådanne hændelser og kriser

e) på anmodning af en berørt medlemsstat at drøfte nationale beredskabsplaner for omfattende cybersikkerhedshændelser og kriser, der er omhandlet i artikel 9, stk. 4.

4. EU-CyCLONe vedtager sin forretningsorden.

5. EU-CyCLONe aflægger regelmæssigt rapport til samarbejdsgruppen om håndteringen af omfattende cybersikkerhedshændelser og kriser samt tendenser med særlig fokus på deres indvirkning på væsentlige og vigtige enheder.

6. EU-CyCLONe samarbejder med CSIRT-netværket på grundlag af aftalte proceduremæssige ordninger, jf. artikel 15, stk. 6.

7. Senest den 17. juli 2024 og derefter hver 18. måned forelægger EU-CyCLONe Europa-Parlamentet og Rådet en rapport med en vurdering af sit arbejde.

Artikel 17

Internationalt samarbejde

Unionen kan, hvor det er hensigtsmæssigt, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller

internationale organisationer, der giver mulighed for og tilrettelægger disses deltagelse i bestemte aktiviteter, der foretages af samarbejdsgruppen, CSIRT-netværket og EU-CyCLONe. Sådanne aftaler skal overholde EU-databeskyttelsesretten.

Artikel 18

Rapport om cybersikkerhedssituationen i Unionen

1. ENISA udarbejder i samarbejde med Kommissionen og samarbejdsgruppen hvert andet år en rapport om cybersikkerhedssituationen i Unionen, som fremsendes til og fremlægges for Europa-Parlamentet. Rapporten skal bl.a. gøres tilgængelig i et maskinlæsbart format og indeholde følgende:

a) en cybersikkerhedsrisikovurdering på EU-plan, der tager cybertrusselsbilledet i betragtning

b) en vurdering af udviklingen af cybersikkerhedskapaciteter i den offentlige og den private sektor i hele Unionen

c) en vurdering af det generelle niveau af cybersikkerhedsbevidsthed og cyberhygiejne hos borgere og enheder, herunder små og mellemstore virksomheder

d) en samlet vurdering af resultaterne af de peerevalueringer, der er omhandlet i artikel 19

e) en samlet vurdering af modenhedsniveauet for cybersikkerhedskapaciteter og -ressourcer i hele Unionen, herunder på sektorniveau, samt af i hvilket omfang medlemsstaternes nationale cybersikkerhedsstrategier er afstemt med hinanden.

2. Rapporten skal indeholde særlige politiske anbefalinger med henblik på at afhjælpe mangler og øge cybersikkerhedsniveauet i hele Unionen og et sammendrag af resultaterne for den pågældende periode fra de tekniske EU-cybersikkerhedsrapporter om hændelser og cybertrusler, som udarbejdes af ENISA i overensstemmelse med artikel 7, stk. 6, i forordning (EU) 2019/881.

3. ENISA udformer i samarbejde med Kommissionen, samarbejdsgruppen og CSIRT-netværket metodologien, herunder de relevante variabler, såsom kvantitative og kvalitative indikatorer, for den samlede vurdering, der er omhandlet i stk. 1, litra e).

Artikel 19

Peerevalueringer

1. Samarbejdsgruppen fastlægger senest den 17. januar 2025 med bistand fra Kommissionen og ENISA samt, hvor det er relevant, CSIRT-netværket metodologien og de organisatoriske aspekter af peerevalueringerne med henblik på at lære af fælles erfaringer, styrke gensidig tillid, opnå et højt fælles cybersikkerhedsniveau samt styrke medlemsstaternes cybersikkerhedskapaciteter og -politikker, der er nødvendige for at gennemføre dette direktiv. Deltagelse i peerevalueringer er frivillig. Peerevalueringerne foretages af cybersikkerhedseksperter. Cybersikkerhedseksperterne udpeges af mindst to medlemsstater, som skal være forskellige fra den medlemsstat, der evalueres.

Peerevalueringerne skal mindst omfatte et af følgende aspekter:

a) gennemførelsesniveauet for de foranstaltninger til styring af cybersikkerhedsrisici og de rapporteringsforpligtelser, der er fastsat i artikel 21 og 23

b) kapacitetsniveauet, herunder de finansielle, tekniske og menneskelige ressourcer, der er til rådighed, og effektiviteten af de kompetente myndigheders varetagelse af deres opgaver

c) CSIRT'ernes operationelle kapacitet

d) gennemførelsesniveauet for den gensidige bistand, der er omhandlet i artikel 37

e) gennemførelsesniveauet for de ordninger for udveksling af cybersikkerhedsoplysninger, der er omhandlet i artikel 29

f) specifikke spørgsmål af grænseoverskridende eller tværsektoriel karakter.

2. Den i stk. 1 omhandlede metodologi skal omfatte objektive, ikkediskriminerende, retfærdige og gennemsigtige kriterier, på grundlag af hvilke medlemsstaterne udpeger cybersikkerhedseksperter, der kan udføre peerevalueringerne. Kommissionen og ENISA deltager som observatører i peerevalueringerne.

3. Medlemsstaterne kan udvælge specifikke spørgsmål som omhandlet i stk. 1, litra f), med henblik på en peerevaluering.

4. Forud for indledningen af en peerevaluering som omhandlet i stk. 1 underretter medlemsstater de deltagende medlemsstater om dens omfang, herunder de specifikke spørgsmål, der er udvalgt i medfør af stk. 3.

5. Forud for indledningen af peerevalueringen kan medlemsstaterne foretage en selvevaluering af de pågældende aspekter og stille denne selvevaluering til rådighed for de udpegede cybersikkerhedseksperter. Samarbejdsgruppen fastlægger med bistand fra Kommissionen og ENISA metoden for medlemsstaternes selvevaluering.

6. Peerevalueringer omfatter fysiske eller virtuelle besøg på stedet og ekstern udveksling af oplysninger. I overensstemmelse med princippet om godt samarbejde giver den medlemsstat, der er genstand for peerevalueringen, de udpegede cybersikkerhedseksperter de oplysninger, der er nødvendige for vurderingen, uden at det berører national ret eller EU-retten vedrørende beskyttelse af fortrolige eller klassificerede informationer og varetagelsen af væsentlige statslige funktioner såsom den nationale sikkerhed. Samarbejdsgruppen udarbejder i samarbejde med Kommissionen og ENISA passende adfærdskodekser, der understøtter de udpegede cybersikkerhedseksperters arbejdsmetoder. Alle oplysninger, der indhentes ved peerevalueringen, må kun anvendes til dette formål. De cybersikkerhedseksperter, der deltager i peerevalueringen, må ikke videregive følsomme eller fortrolige oplysninger, som er indhentet som led i denne peerevaluering, til tredjemand.

7. Aspekter, der været genstand for en peerevaluering i en medlemsstat, må ikke underkastes en yderligere peerevaluering i den pågældende medlemsstat i to år efter afslutningen af peerevalueringen, medmindre medlemsstaten anmoder om andet, eller der aftales andet på forslag af samarbejdsgruppen.

8. Medlemsstaterne sikrer, at enhver risiko for interessekonflikter vedrørende de udpegede cybersikkerhedseksperter meddeles de øvrige medlemsstater, samarbejdsgruppen, Kommissionen og ENISA, inden peerevalueringen indledes. Den medlemsstat, der er genstand for peerevalueringen, kan gøre indsigelse mod udpegelsen af bestemte cybersikkerhedseksperter af behørigt begrundede årsager, som meddeles den udpegende medlemsstat.

9. Cybersikkerhedseksperter, der deltager i peerevalueringer, udarbejder rapporter om resultaterne og konklusionerne af peerevalueringerne. Medlemsstater, der er genstand for en peerevaluering, kan fremsætte bemærkninger til udkast til rapporter, der vedrører dem, og sådanne bemærkninger vedføjes rapporterne. Rapporterne skal indeholde anbefalinger, der kan gøre det muligt at forbedre de aspekter, peerevalueringen vedrører. Rapporterne forelægges for samarbejdsgruppen og CSIRT-netværket, hvor det er relevant. En medlemsstat,

der er genstand for peerevalueringen, kan beslutte at gøre sin rapport, eller en redigeret udgave heraf, offentligt tilgængelig.

KAPITEL IV
FORANSTALTNINGER TIL STYRING AF CYBERSIKKERHEDSRISICI OG RAPPORTERINGSFORPLIGTELSER

Artikel 20

Styring

1. Medlemsstaterne sikrer, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.

Anvendelsen af dette stykke berører ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

2. Medlemsstaterne sikrer, at medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.

Artikel 21

Foranstaltninger til styring af cybersikkerhedsrisici

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne skal de i første afsnit omhandlede foranstaltninger tilvejebringe et sikkerhedsniveau i net- og informationssystemer,

der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

2. De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende:

a)politikker for risikoanalyse og informationssystemsikkerhed

b) håndtering af hændelser

c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring

d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere

e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse

h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering

i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver

j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

3. Medlemsstaterne sikrer, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet i denne artikels stk. 2, litra d), der er passende, tager 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 deres sikre udviklingsprocedurer. Medlemsstaterne

sikrer også, at enhederne, når de overvejer, hvilke foranstaltninger omhandlet i nævnte litra, der er passende, er forpligtet til at tage hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der foretages i overensstemmelse med artikel 22, stk. 1.

4. Medlemsstaterne sikrer, at en enhed, der finder, at den ikke overholder foranstaltningerne i stk. 2, uden unødigt ophold træffer alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

5. Senest 17. oktober 2024 vedtager Kommissionen gennemførelsesretsakter, der fastsætter de tekniske og metodologiske krav til de foranstaltninger, der er omhandlet i stk. 2, for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester og af tillidstjenester.

Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter de tekniske og metodologiske, samt om nødvendigt sektorspecifikke, krav til de i stk. 2 omhandlede foranstaltninger for så vidt angår andre væsentlige og vigtige enheder end dem, der er omhandlet i nærværende stykkes første afsnit.

Ved udarbejdelsen af de gennemførelsesretsakter, der er omhandlet i nærværende stykkes første og andet afsnit, følger Kommissionen i videst muligt omfang europæiske og internationale standarder samt relevante tekniske specifikationer. Kommissionen udveksler rådgivning og samarbejder med samarbejdsgruppen og ENISA om udkastene til gennemførelsesretsakter i overensstemmelse med artikel 14, stk. 4, litra e).

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 39, stk. 2.

Artikel 22

Koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan

1. Samarbejdsgruppen kan i samarbejde med Kommissionen og ENISA foretage koordinerede sikkerhedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder

under hensyntagen til tekniske og, hvor det er relevant, ikketekniske risikofaktorer.

2. Kommissionen identificerer efter høring af samarbejdsgruppen og ENISA og, hvor det er nødvendigt, relevante interessenter de specifikke kritiske IKT-tjenester, -systemer eller -produkter, der kan være genstand for den i stk. 1 omhandlede koordinerede sikkerhedsrisikovurdering.

Artikel 23

Rapporteringsforpligtelser

1. Hver medlemsstat sikrer, at væsentlige og vigtige enheder uden unødigt ophold underretter dens CSIRT eller i givet fald dens kompetente myndighed i overensstemmelse med stk. 4 om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester som omhandlet i stk. 3 (væsentlig hændelse). Hvor det er relevant, underretter de pågældende enheder uden unødigt ophold modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt. Hver medlemsstat sikrer, at disse enheder indberetter bl.a. alle oplysninger, der gør det muligt for CSIRT'en, eller i givet fald den kompetente myndighed, at fastslå eventuelle grænseoverskridende virkninger af hændelsen. Underretningen i sig selv medfører ikke et øget ansvar for den underrettende enhed.

Hvor de berørte enheder underretter den kompetente myndighed om en væsentlig hændelse i henhold til første afsnit, sikrer medlemsstaten, at den pågældende kompetente myndighed videresender underretningen til CSIRT'en på tidspunktet for modtagelsen.

I tilfælde af en grænseoverskridende eller tværsektoriel væsentlig hændelse sikrer medlemsstaterne, at deres centrale kontaktpunkter rettidigt forsynes med relevante oplysninger, som der er givet underretning om i overensstemmelse med stk. 4.

2. I givet fald sikrer medlemsstaterne, at væsentlige og vigtige enheder uden unødigt ophold meddeler 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. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige cybertrussel.

3. En hændelse anses for at være væsentlig, hvis:

a) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed

b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

4. Medlemsstaterne sikrer, at de berørte enheder med henblik på den i stk. 1 omhandlede underretning fremsender følgende til CSIRT'en eller i givet fald den kompetente myndighed:

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

b) uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse, en hændelsesunderretning, som i givet fald skal ajourføre de oplysninger, der er omhandlet under litra a), og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger

c) efter anmodning fra en CSIRT eller i givet fald den kompetente myndighed en foreløbig rapport om relevante statusopdateringer

d) en endelig rapport senest en måned efter forelæggelsen af den i litra b) omhandlede hændelsesunderretning, der skal omfatte følgende:

   i) en detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning

   ii) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen

   iii) anvendte og igangværende afbødende foranstaltninger

   iv) i givet fald de grænseoverskridende virkninger af hændelsen.

e) i tilfælde af at en hændelse pågår på tidspunktet for indgivelsen af den i litra d), omhandlede endelige rapport, sikrer medlemsstaterne, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af hændelsen.

Uanset første afsnit, litra b), skal tillidstjenesteudbyderen for så vidt angår væsentlige hændelser, der har en virkning på leveringen af dens tillidstjenester, underrette CSIRT'en eller i givet fald den kompetente myndighed uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at være blevet bekendt med den væsentlige hændelse.

5. CSIRT'en eller den kompetente myndighed giver uden unødigt ophold og, hvor det er muligt, inden for 24 timer efter modtagelsen af den i stk. 4, litra a), omhandlede tidlige varsling den underrettende enhed et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse og, efter anmodning fra enheden, vejledning eller operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger. Hvor CSIRT'en ikke er den oprindelige modtager af den i stk. 1 omhandlede underretning, gives vejledningen af den kompetente myndighed i samarbejde med CSIRT'en. CSIRT'en yder supplerende teknisk bistand, hvis den berørte enhed anmoder herom. Hvor den væsentlige hændelse mistænkes for at være af strafferetlig karakter, giver CSIRT'en eller den kompetente myndighed også vejledning om underretning om den væsentlige hændelse til retshåndhævende myndigheder.

6. Hvor det er relevant, og navnlig hvor den væsentlige hændelse berører to eller flere medlemsstater, informerer CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt uden unødigt ophold de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse. Sådan information omfatter den type af oplysninger, der er modtaget i overensstemmelse med stk. 4. CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt sikrer i den forbindelse i overensstemmelse med EU-retten eller national ret enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

7. Hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende væsentlig hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed og, hvor det er relevant, CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

8. På CSIRT'ens eller den kompetente myndigheds anmodning videresender det centrale kontaktpunkt de underretninger, der er modtaget i henhold til stk. 1, til de centrale kontaktpunkter i andre berørte medlemsstater.

9. Det centrale kontaktpunkt forelægger en gang hver tredje måned en sammenfattende rapport for ENISA, herunder anonymiserede og aggregerede data om væsentlige hændelser, hændelser, cybertrusler og nærvedhændelser, der er indberettet i overensstemmelse med denne artikels stk. 1 og med artikel 30. For at bidrage til tilvejebringelsen af sammenlignelige oplysninger kan ENISA vedtage teknisk vejledning om parametrene for de oplysninger, der skal inkluderes i den sammenfattende rapport. ENISA underretter samarbejdsgruppen og CSIRT-netværket om sine resultater vedrørende modtagne underretninger hver sjette måned.

10. CSIRT'erne eller i givet fald de kompetente myndigheder giver de kompetente myndigheder i henhold til direktiv (EU) 2022/2557, oplysninger om væsentlige hændelser, hændelser, cybertrusler og nærvedhændelser, der er indberettet i overensstemmelse med denne artikels stk. 1 og med artikel 30 af enheder, der er identificeret som kritiske enheder i henhold til direktiv (EU) 2022/2557.

11. Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer typen af oplysninger, formatet og proceduren for en underretning indgivet i henhold til denne artikels stk. 1 og til artikel 30 og for en meddelelse, der er indgivet i henhold til nærværende artikels stk. 2.

Senest den 17. oktober 2024 vedtager Kommissionen for så vidt angår DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester gennemførelsesretsakter, der yderligere præciserer de tilfælde, hvor en hændelse anses for at være væsentlig som omhandlet i stk. 3. Kommissionen kan vedtage sådanne gennemførelsesretsakter for så vidt angår andre væsentlige og vigtige enheder.

Kommissionen udveksler rådgivning og samarbejder med samarbejdsgruppen om de udkast til gennemførelsesretsakter, der er om-

handlet i dette stykkes første og andet afsnit, i overensstemmelse med artikel 14, stk. 4, litra e).

Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 39, stk. 2.

Artikel 24

Brug af europæiske cybersikkerhedscertificeringsordninger

1. For at påvise overensstemmelse med bestemte krav i artikel 21 kan medlemsstaterne kræve, at væsentlige og vigtige enheder bruger særlige IKT-produkter, -tjenester og -processer, der er udviklet af den væsentlige eller vigtige enhed eller indkøbt fra tredjeparter, og som er certificeret i henhold til europæiske cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. Endvidere skal medlemsstaterne tilskynde væsentlige og vigtige enheder til at anvende kvalificerede tillidstjenester.

2. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 38 for at supplere dette direktiv ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. Disse delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer, og skal indeholde en gennemførelsesperiode.

Inden vedtagelsen af sådanne delegerede retsakter foretager Kommissionen en konsekvensanalyse og gennemfører høringer i overensstemmelse med artikel 56 i forordning (EU) 2019/881.

3. I tilfælde, hvor der ikke findes en passende europæisk cybersikkerhedscertificeringsordning for så vidt angår denne artikels stk. 2, kan Kommissionen efter høring af samarbejdsgruppen og Den Europæiske Cybersikkerhedscertificeringsgruppe anmode ENISA om at udarbejde et forslag til ordning i henhold til artikel 48, stk. 2, i forordning (EU) 2019/881.

Artikel 25

Standardisering

1. For at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske og internationale

standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

2. ENISA udarbejder i samarbejde med medlemsstaterne og, hvor det er relevant, efter høring af relevante interessenter vejledning og retningslinjer om de tekniske områder, der skal overvejes vedrørende stk. 1, samt om allerede eksisterende standarder, herunder nationale standarder, som vil give mulighed for at dække disse områder.

KAPITEL V
JURISDIKTION OG REGISTRERING

Artikel 26

Jurisdiktion og territorialitet

1. Enheder, der er omfattet af dette direktivs anvendelsesområde, anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de er etableret, med undtagelse af:

a) udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester

b) DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner eller af platforme for sociale netværkstjenester, som anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen i henhold til stk. 2

c) offentlige forvaltningsenheder, som anses for at henhøre under jurisdiktionen i den medlemsstat, der har oprettet dem.

2. Med henblik på dette direktiv anses en enhed som omhandlet i stk. 1, litra b), for at have sit hovedforretningssted i Unionen i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici overvejende træffes. Hvis en sådan medlemsstat ikke kan fastslås, eller hvis sådanne beslutninger ikke træffes i Unionen, anses hovedforretningsstedet for at være i den medlemsstat, hvor der udføres cybersikkerhedsoperationer. Hvis en sådan

medlemsstat ikke kan fastslås, anses hovedforretningsstedet for at være i den medlemsstat, hvor den pågældende enheds forretningssted med det største antal ansatte i Unionen er beliggende.

3. Hvis en enhed som omhandlet i stk. 1, litra b), ikke er etableret i Unionen, men udbyder tjenester inden for Unionen, skal den udpege en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. En sådan enhed anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret. Hvis der ikke findes en repræsentant i Unionen, der er udpeget i henhold til dette stykke, kan enhver medlemsstat, hvor enheden leverer tjenester, tage retlige skridt mod enheden for overtrædelse af dette direktiv.

4. Det forhold, at en enhed som omhandlet i stk. 1, litra b), har udpeget en repræsentant, forhindrer ikke, at der kan tages retlige skridt mod enheden selv.

5. Medlemsstater, der har modtaget en anmodning om gensidig bistand vedrørende en enhed som omhandlet i stk. 1, litra b), kan inden for rammerne af denne anmodning træffe passende tilsyns- og håndhævelsesforanstaltninger over for den pågældende enhed, der leverer tjenester eller har et net- og informationssystem på deres område.

Artikel 27

Register over enheder

1. ENISA opretter og fører et register over DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavnsregistreringstjenester, og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester på grundlag af de oplysninger, der modtages fra det centrale kontaktpunkt i overensstemmelse med stk. 4. Efter anmodning giver ENISA de kompetente myndigheder adgang til dette register, idet det i givet fald sikrer de nødvendige garantier til at beskytte fortroligheden af oplysninger.

2. Medlemsstaterne pålægger de i stk. 1, omhandlede enheder at indgive følgende oplysninger til de kompetente myndigheder senest den 17. januar 2025:

a) enhedens navn

b) den relevante sektor og delsektor og typen af enhed, som i givet fald er omhandlet i bilag I eller II

c) adressen på enhedens hovedforretningssted og dens andre retlige forretningssteder i Unionen eller, hvis den ikke er etableret i Unionen, på den repræsentant, der er udpeget i henhold til artikel 26, stk. 3

d) ajourførte kontaktoplysninger, herunder e-mailadresser og telefonnumre på enheden og i givet fald dens repræsentant udpeget i henhold til artikel 26, stk. 3

e) de medlemsstater, hvor enheden leverer tjenester og

f) enhedens IP-intervaller.

3. Medlemsstaterne sikrer, at de i stk. 1 omhandlede enheder straks og under alle omstændigheder senest tre måneder efter den dato, hvor ændringen trådte i kraft, underretter den kompetente myndighed om enhver ændring af de oplysninger, de har indsendt i henhold til stk. 2.

4. Efter modtagelsen af oplysningerne omhandlet i stk. 2 og 3, med undtagelse af oplysningerne omhandlet i stk. 2, litra f), videresender den berørte medlemsstats centrale kontaktpunkt dem, til ENISA uden unødigt ophold.

5. De i denne artikels stk. 2 og 3 omhandlede oplysninger fremsendes i givet fald via den nationale mekanisme, der er omhandlet i artikel 3, stk. 4, fjerde afsnit.

Artikel 28

Database over domænenavnsregistreringsdata

1. Med henblik på at bidrage til DNS' sikkerhed, stabilitet og modstandsdygtighed pålægger medlemsstaterne topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, med rettidig omhu at indsamle og vedligeholde nøjagtige og fuldstændige domænenavnsregistreringsdata i en særlig database i overensstemmelse med EU-databeskyttelsesretten for så vidt angår personoplysninger.

2. Med henblik på stk. 1 stiller medlemsstaterne krav om, at databasen over domænenavnsregistreringsdata indeholder de fornødne oplysninger til at identificere og kontakte indehaverne af domænenavne og de kontaktpunkter, der forvalter domænenavne under topdomæner. Sådanne oplysninger omfatter:

a) Domænenavnet

b) registreringsdatoen

c)registrantens navn, kontakt-e-mailadresse og telefonnummer

d) kontakt-e-mailadresse og telefonnummer på det kontaktpunkt, der administrerer domænenavnet, i det tilfælde at de er forskellige fra registrantens.

3. Medlemsstaterne stiller krav om, at topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, har indført politikker og procedurer, herunder verifikationsprocedurer, for at sikre, at de i stk. 1 omhandlede databaser indeholder nøjagtige og fuldstændige oplysninger. Medlemsstaterne kræver, at sådanne politikker og procedurer gøres offentligt tilgængelige.

4. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, uden unødigt ophold efter registreringen af et domænenavn at gøre domænenavnsregistreringsdata, som ikke er personoplysninger, offentligt tilgængelige.

5. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der udbyder domænenavnsregistreringstjenester, at give adgang til specifikke domænenavnsregistreringsdata efter lovlige og behørigt begrundede anmodninger fra legitime adgangssøgende i overensstemmelse med EU-databeskyttelsesretten. Medlemsstaterne pålægger topdomænenavneadministratorerne og de enheder, der udbyder domænenavnsregistreringstjenester, at besvare anmodninger om adgang uden unødigt ophold og under alle omstændigheder inden for 72 timer efter modtagelse af anmodninger. Medlemsstaterne skal kræve, at sådanne politikker og procedurer gøres offentligt tilgængelige.

6. Overholdelse af de forpligtelser, der er fastsat i stk. 1-5, må ikke føre til en gentagelse af indsamlingen af domænenavnsregistreringsdata. Med henblik herpå pålægger medlemsstaterne topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, at samarbejde med hinanden.

KAPITEL VI
UDVEKSLING AF OPLYSNINGER

Artikel 29

Ordninger for udveksling af cybersikkerhedsoplysninger

1. Medlemsstaterne sikrer, at enheder, der er omfattet af dette direktivs anvendelsesområde, og, hvor det er relevant, andre enheder, der ikke er omfattet af dette direktivs anvendelsesområde, på frivillig basis er i stand til at udveksle relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, nærvedhændelser, sårbarheder, teknikker og procedurer, kompromitteringsindikatorer, fjendtlige taktikker, specifikke oplysninger vedrørende trusselsaktører, cybersikkerhedsadvarsler og anbefalinger vedrørende konfiguration af cybersikkerhedsværktøjer til opdagelse af cyberangreb, hvor sådan udveksling af oplysninger:

a) har til formål at forebygge, opdage, reagere på eller reetablere sig efter hændelser eller afbøde deres virkninger

b) øger cybersikkerhedsniveauet, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre sådanne truslers evne til at sprede sig, støtte en række forsvarskapaciteter, afhjælpe og offentliggøre sårbarheder, teknikker til opdagelse, begrænsning og forebyggelse af trusler, afbødningsstrategier eller indsats- og genopretningsfaser eller fremme samarbejde mellem offentlige og private enheder om forskning i trusler.

2. Medlemsstaterne sikrer, at udvekslingen af oplysninger finder sted inden for fællesskaber af væsentlige og vigtige enheder og, hvor det er relevant, deres leverandører eller tjenesteudbydere. En sådan udveksling skal gennemføres ved hjælp af ordninger for udveksling af cybersikkerhedsoplysninger for så vidt angår den potentielt følsomme karakter af de udvekslede oplysninger.

3. Medlemsstaterne fremmer etableringen af ordninger for udveksling af cybersikkerhedsoplysninger, der er omhandlet i denne artikels stk. 2. Sådanne ordninger kan specificere operationelle elementer, herunder brugen af særlige IKT-platforme og automatiseringsværktøjer, i, indholdet af og betingelserne for ordningerne for udveksling af oplysninger. Ved fastlæggelsen af de nærmere bestemmelser om inddragelse af offentlige myndigheder i sådanne ordninger kan medlemsstaterne indføre betingelser for de oplysninger, som de kompetente myndigheder eller CSIRT'erne stiller til rådighed. Medlemsstaterne yder bistand til anvendelsen af sådanne ordninger i overensstemmelse med deres politikker, der er omhandlet i artikel 7, stk. 2, litra h).

4. Medlemsstaterne sikrer, at væsentlige og vigtige enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 2 omhandlede ordninger for udveksling af cybersikkerhedsoplysninger, når de indtræder i sådanne ordninger, eller, i givet faldt, om deres udtræden af sådanne ordninger, når denne udtræden træder i kraft.

5. ENISA yder bistand til oprettelsen af ordninger for udveksling af cybersikkerhedsoplysninger, der er omhandlet i stk. 2, ved at udveksle bedste praksis og give vejledning.

Artikel 30

Frivillig meddelelse af relevante oplysninger

1. Medlemsstaterne sikrer, at der, i tilgift til underretningsforpligtelsen i medfør af artikel 23 kan indgives underretninger til CSIRT'er eller i givet fald til de kompetente myndigheder på frivillig basis af:

a) væsentlige og vigtige enheder for så vidt angår hændelser, cybertrusler og nærvedhændelser

b) enheder, udover dem der omhandlet i litra a), uanset om de er omfattet af dette direktivs anvendelsesområde, for så vidt angår væsentlige hændelser, cybertrusler og nærvedhændelser.

2. Medlemsstaterne behandler de i denne artikels stk. 1 omhandlede underretninger i overensstemmelse med proceduren, der er fastsat i artikel 23. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger.

Hvor det er nødvendigt, giver CSIRT'erne og i givet fald de kompetente myndigheder det centrale kontaktpunkt de oplysninger om underretninger, de har modtaget i medfør af denne artikel, samtidig med at de sikrer fortroligheden og passende beskyttelse af de oplysninger, der er afgivet af den underrettende enhed. Uden at det berører forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, må frivillig rapportering ikke medføre, at den underrettende enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde foretaget underretningen.

KAPITEL VII
TILSYN OG HÅNDHÆVELSE

Artikel 31

Generelle aspekter vedrørende tilsyn og håndhævelse

1. Medlemsstaterne sikrer, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at dette direktiv overholdes.

2. Medlemsstaterne kan tillade deres kompetente myndigheder at prioritere tilsynsopgaver. En sådan prioritering baseres på en risikobaseret tilgang. Med henblik herpå kan de kompetente myndigheder, når de udfører deres tilsynsopgaver i henhold til artikel 32 og 33, fastlægge tilsynsmetoder, der gør det muligt at prioritere sådanne opgaver efter en risikobaseret tilgang.

3. De kompetente myndigheder arbejder tæt sammen med tilsynsmyndigheder i henhold til forordning (EU) 2016/679, når de håndterer hændelser, der medfører brud på persondatasikkerheden, uden at det berører de kompetencer og opgaver, som tilsynsmyndighederne har i henhold til nævnte forordning.

4. Uden at det berører nationale lovgivningsmæssige og institutionelle rammer sikrer medlemsstaterne, at de kompetente myndigheder ved tilsynet med offentlige forvaltningsenheders overholdelse af dette direktiv og indførelsen af håndhævelsesforanstaltninger for så vidt angår overtrædelser af dette direktiv, har passende beføjelser til at udføre sådanne opgaver med operationel uafhængighed i forhold til de offentlige forvaltningsenheder, der føres tilsyn med. Medlemsstaterne kan beslutte at indføre passende, forholdsmæssige og effektive tilsyns- og håndhævelsesforanstaltninger over for disse enheder i overensstemmelse med de nationale lovgivningsmæssige og institutionelle rammer.

Artikel 32

Tilsyns- og håndhævelsesforanstaltninger vedrørende væsentlige enheder

1. Medlemsstaterne sikrer, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder for så vidt angår forpligtelserne fastsat i dette direktiv er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende væsentlige enheder, som minimum har beføjelse til at pålægge disse enheder:

a) kontrol på stedet og eksternt tilsyn, herunder stikprøvekontrol, som skal udføres af uddannede fagfolk

b) regelmæssige og målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed

c) ad hoc-audits, herunder hvor det er berettiget på grund af en væsentlig hændelse eller en overtrædelse af dette direktiv fra den væsentlige enheds side

d) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed

e) anmodninger om oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27

f) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver

g) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

De målrettede sikkerhedsaudits, der er omhandlet i første afsnit, litra b), baseres på risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger.

Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde når den kompetente myndighed bestemmer andet.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra e), f) eller g), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at deres kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for væsentlige enheder, som minimum har beføjelse til at:

a) udstede advarsler om de pågældende enheders overtrædelser af dette direktiv

b) udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af dette direktiv

c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder dette direktiv, og afstå fra at gentage denne adfærd

d) pålægge de pågældende enheder, på en nærmere angivet måde og inden for en nærmere angivet frist, at sikre, at deres foranstaltninger til styring af cybersikkerhedsrisici overholder artikel 21, eller at efterleve underretningsforpligtelserne i artikel 23

e) pålægge de pågældende enheder at underrette de fysiske eller juridiske personer med hensyn til hvilke de leverer tjenester eller udfører aktiviteter, som potentielt er berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

f) pålægge de pågældende enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsaudit, inden for en rimelig frist

g) udpege en overvågningsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med de pågældende enheders overholdelse af artikel 21 og 23

h) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af dette direktiv på en nærmere angivet måde

i) pålægge, eller anmode de relevante organer eller domstole om i overensstemmelse med national ret at pålægge, en administrativ bøde i henhold til artikel 34 ud over enhver af de foranstaltninger, der er omhandlet i dette stykkes litra a)-h).

5. Hvor håndhævelsesforanstaltninger vedtaget i henhold til stk. 4, litra a)-d) og f), er virkningsløse, sikrer medlemsstaterne, at deres kompetente myndigheder har beføjelse til at fastsætte en frist, inden for hvilken den væsentlige enhed anmodes om at tage de nødvendige tiltag for at afhjælpe manglerne eller opfylde disse myndigheders krav. Hvis de ønskede tiltag ikke tages inden for den fastsatte frist,

sikrer medlemsstaterne, at de kompetente myndigheder har 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

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.

Midlertidige suspensioner eller forbud, som er pålagt i henhold til dette stykke, anvendes kun, indtil den pågældende enhed træffer de nødvendige foranstaltninger til at afhjælpe manglerne eller opfylde den kompetente myndighed krav, som gav anledning til, at disse håndhævelsesforanstaltninger blev anvendt. Pålæggelse af sådanne 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.

Håndhævelsesforanstaltningerne i dette stykke finder ikke anvendelse på offentlige forvaltningsenheder, der er omfattet af dette direktiv.

6. Medlemsstaterne sikrer, at enhver fysisk person, der er ansvarlig for eller optræder som juridisk repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at den overholder dette direktiv. Medlemsstaterne sikrer, at det er muligt at drage sådanne fysiske personer til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelse af dette direktiv.

Med hensyn til offentlige forvaltningsenheder berører dette stykke ikke national ret for så vidt angår ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

7. Når de kompetente myndigheder træffer håndhævelsesforanstaltninger omhandlet i stk. 4 eller 5, skal de overholde retten til forsvar

og tage hensyn til omstændighederne i hver enkelt sag og som minimum tage behørigt hensyn til:

a) overtrædelsens grovhed og vigtigheden af de overtrådte bestemmelser, idet bl.a. følgende under alle omstændigheder skal betragtes som alvorlige overtrædelser:

   i) gentagne overtrædelser

   ii) manglende underretning om eller afhjælpning af væsentlige hændelser

   iii) manglende afhjælpning af mangler efter bindende instrukser fra kompetente myndigheder

   iv) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse

   v) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i artikel 21 og 23

b) overtrædelsens varighed

c)den pågældende enheds relevante tidligere overtrædelser

d) 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

e) hvorvidt gerningsmanden har begået overtrædelsen forsætligt eller uagtsomt

f) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den materielle eller immaterielle skade

g) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt

h) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige, samarbejder med de kompetente myndigheder.

8. De kompetente myndigheder giver en detaljeret begrundelse for deres håndhævelsesforanstaltninger. Inden de kompetente myndigheder træffer sådanne foranstaltninger, underretter de berørte enheder om deres foreløbige resultater. De giver også disse enheder en rimelig frist til at fremsætte bemærkninger, undtagen i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret.

9. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv underretter de relevante kompetente myndigheder i samme medlemsstat i henhold til direktiv (EU) 2022/2557, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en enhed, der er identificeret som en kritisk enhed i henhold til direktiv (EU) 2022/2557, overholder nærværende direktiv. Hvor det er relevant, kan de kompetente myndigheder i henhold til direktiv (EU) 2022/2557 anmode de kompetente myndigheder i henhold til nærværende direktiv om at udøve deres tilsyns- og håndhævelsesbeføjelser med hensyn til en enhed, som er identificeret som en kritisk enhed i henhold til direktiv (EU) 2022/2557.

10. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv samarbejder med de relevante kompetente myndigheder i den berørte medlemsstat i henhold til forordning (EU) 2022/2554. Medlemsstaterne sikrer navnlig, at deres kompetente myndigheder i henhold til nærværende direktiv underretter tilsynsforummet oprettet i henhold til artikel 32, stk. 1, i forordning (EU) 2022/2554, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en væsentlig enhed, der er udpeget som en kritisk tredjepartsudbyder af IKT-tjenester i henhold til artikel 31, i forordning (EU) 2022/2554, overholder nærværende direktiv.

Artikel 33

Tilsyns- og håndhævelsesforanstaltninger vedrørende vigtige enheder

1. Når medlemsstaterne kommer i besiddelse af dokumentation for eller tegn på eller oplysninger om, at en vigtig enhed angiveligt ikke overholder dette direktiv, navnlig artikel 21 og 23 deri, sikrer de, at de kompetente myndigheder træffer foranstaltninger, hvor det er nødvendigt, gennem efterfølgende tilsynsforanstaltninger. Medlemsstaterne sikrer, at disse foranstaltninger er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende vigtige enheder, som minimum har beføjelse til at pålægge disse enheder:

a) kontrol på stedet og eksternt efterfølgende tilsyn udført af uddannede fagfolk

b) målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed

c) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed

d) anmodninger om oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27

e) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaverne

f) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

De målrettede sikkerhedsaudits, der er omhandlet i første afsnit, litra b), baseres risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger.

Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde når den kompetente myndighed bestemmer andet.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra d), e) eller f), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for vigtige enheder, som minimum har beføjelse til at:

a) udstede advarsler om de pågældende enheders overtrædelser af dette direktiv

b) udstede bindende instrukser eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af dette direktiv

c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder dette direktiv, og afstå fra at gentage denne adfærd

d) pålægge de pågældende enheder, på en nærmere angivet måde og inden for en nærmere angivet frist, at sikre, at deres foranstaltninger til styring af cybersikkerhedsrisici overholder artikel 21, eller at efterleve underretningsforpligtelserne i artikel 23

e) pålægge de pågældende enheder at underrette de fysiske eller juridiske personer med hensyn til hvilke de leverer tjenester eller udfører aktiviteter, som potentielt er berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

f) pålægge de pågældende enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsaudit, inden for en rimelig frist

g) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af dette direktiv på en nærmere angivet måde

h) pålægge eller anmode de relevante organer eller domstole om i overensstemmelse med national ret at pålægge en administrativ bøde i henhold til artikel 34 ud over enhver af de foranstaltninger, der er omhandlet i dette stykkes litra a)-g).

5. Artikel 32, stk. 6, 7 og 8, finder tilsvarende anvendelse på tilsyns- og håndhævelsesforanstaltningerne i denne artikel for vigtige enheder.

6. Medlemsstaterne sikrer, at deres kompetente myndigheder i henhold til dette direktiv samarbejder med de relevante kompetente myndigheder i den berørte medlemsstat i henhold til forordning (EU) 2022/2554. Medlemsstaterne sikrer navnlig, at deres kompetente myndigheder i henhold til nærværende direktiv underretter tilsynsforummet oprettet i henhold til artikel 32, stk. 1, i forordning (EU) 2022/2554, når de udøver deres tilsyns- og håndhævelsesbeføjelser med det formål at sikre, at en vigtig enhed, der er udpeget som en kritisk tredjepartsudbyder af IKT-tjenester i henhold til artikel 31, i forordning (EU) 2022/2554, overholder nærværende direktiv.

Artikel 34

Generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder

1. Medlemsstaterne sikrer, at de administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til denne artikel for så vidt angår overtrædelser af dette direktiv, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning, under hensyntagen til omstændighederne i hver enkelt sag.

2. Administrative bøder pålægges i tillæg til en hvilken som helst af foranstaltningerne omhandlet i artikel 32, stk. 4, litra a)-h), artikel 32, stk. 5, og artikel 33, stk. 4, litra a)-g).

3. Når det besluttes, om der skal pålægges en administrativ bøde, og der træffes afgørelse om dens størrelse i hver enkelt sag, tages der som minimum behørigt hensyn til de i artikel 32, stk. 7, angivne elementer.

4. Medlemsstaterne sikrer, at hvor væsentlige enheder overtræder artikel 21 eller 23, straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 10 000 000 EUR eller et maksimum på mindst 2 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

5. Medlemsstaterne sikrer, at hvor vigtige enheder overtræder artikel 21 eller 23, straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 7 000 000 EUR eller et maksimum på mindst 1,4 % af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.

6. Medlemsstaterne kan fastsætte beføjelser til at pålægge tvangsbøder for at tvinge en væsentlig eller vigtig enhed til at bringe en overtrædelse af dette direktiv til ophør i overensstemmelse med en forudgående afgørelse truffet af den kompetente myndighed.

7. Uden at det berører tilsynsmyndighedernes beføjelser i henhold til artikel 32 og 33, kan hver enkelt medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder kan pålægges offentlige forvaltningsorganer.

8. Hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, sørger den pågældende medlemsstat for, at denne artikel anvendes på en sådan måde, at den kompetente myndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges

af de kompetente myndigheder. De bøder, der pålægges, skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaten giver Kommissionen meddelelse om bestemmelserne i de love, som den vedtager i henhold til dette stykke, senest den 17. oktober 2024 og underretter den straks om eventuelle senere ændringslove eller ændringer, der berører dem.

Artikel 35

Overtrædelser, der medfører brud på persondatasikkerheden

1. Hvor de kompetente myndigheder i forbindelse med tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af forpligtelserne i dette direktivs artikel 21 og 23 kan medføre et brud på persondatasikkerheden som defineret i artikel 4, nr. 12), i forordning (EU) 2016/679, som skal anmeldes i henhold til nævnte forordnings artikel 33, underretter de uden unødigt ophold tilsynsmyndigheder som omhandlet i nævnte forordnings artikel 55 eller 56.

2. Hvor tilsynsmyndighederne som omhandlet i artikel 55 eller 56 i forordning (EU) 2016/679 pålægger en administrativ bøde i henhold til nævnte forordnings artikel 58, stk. 2, litra i), må de kompetente myndigheder ikke pålægge en administrativ bøde i henhold til dette direktivs artikel 34 for en i nærværende artikels stk. 1 omhandlet overtrædelse, der skyldes den samme adfærd som den, der var genstand for den administrative bøde i henhold til artikel 58, stk. 2, litra i), i forordning (EU) 2016/679. De kompetente myndigheder kan dog anvende de håndhævelsesforanstaltninger eller pålægge de sanktioner, der er omhandlet i dette direktivs artikel 32, stk. 4, litra a)-h), artikel 32, stk. 5, og artikel 33, stk. 4, litra a)-g).

3. Hvor den tilsynsmyndighed, der er kompetent i henhold til forordning (EU) 2016/679, er etableret i en anden medlemsstat end den kompetente myndighed, underretter den kompetente myndighed tilsynsmyndigheden, der er etableret i sin egen medlemsstat, om det i stk. 1 omhandlede potentielle brud på persondatasikkerheden.

Artikel 36

Sanktioner

Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er ved-

taget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver senest den 17. januar 2025 Kommissionen meddelelse om disse regler og foranstaltninger og underretter den straks om alle senere ændringer, der berører dem.

Artikel 37

Gensidig bistand

1. Hvor en enhed leverer tjenester i mere end én medlemsstat, eller hvor den leverer tjenester i en eller flere medlemsstater og dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder i de pågældende medlemsstater med og bistå hinanden efter behov. Dette samarbejde indebærer mindst, at:

a) de kompetente myndigheder, der anvender tilsyns- eller håndhævelsesforanstaltninger i en medlemsstat, via det fælles kontaktpunkt underretter og hører de kompetente myndigheder i de øvrige berørte medlemsstater om de tilsyns- og håndhævelsesforanstaltninger, der er truffet

b) en kompetent myndighed kan anmode en anden kompetent myndighed om at træffe tilsyns- eller håndhævelsesforanstaltninger

c) en kompetent myndighed efter modtagelse af en begrundet anmodning fra en anden kompetent myndighed yder bistand til den anden kompetente myndighed, der står i et rimeligt forhold til dens egne ressourcer, således at tilsyns- eller håndhævelsesforanstaltningerne kan gennemføres på en effektiv, virkningsfuld og konsekvent måde.

Den gensidige bistand, der er omhandlet i første afsnit, litra c), kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller eksternt tilsyn eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, må ikke afvise anmodningen, medmindre det er fastslået, at den ikke er kompetent til at yde den ønskede bistand, at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds tilsynsopgaver, eller anmodningen vedrører oplysninger eller indebærer aktiviteter, som, hvis de blev videregivet eller udført, ville stride mod den medlemsstats væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før den kompetente myndighed afslår en sådan

anmodning, hører den de øvrige berørte kompetente myndigheder samt, efter anmodning fra en af de berørte medlemsstater, Kommissionen og ENISA.

2. Hvor det er hensigtsmæssigt og efter fælles overenskomst, kan de kompetente myndigheder fra forskellige medlemsstater gennemføre fælles tilsynstiltag.

KAPITEL VIII
DELEGEREDE RETSAKTER OG GENNEMFØRELSES-RETSAKTER

Artikel 38

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastsatte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 24, stk. 2, tillægges Kommissionen for en periode på fem år fra den 16. januar 2023.

3. Den i artikel 24, stk. 2, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i *Den Europæiske Unions Tidende* eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelse af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 24, stk. 2, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har informeret

Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 39

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

3. Når udvalgets udtalelse indhentes efter en skriftlig procedure, afsluttes proceduren uden noget resultat, hvis formanden for udvalget træffer beslutning herom, eller hvis et medlem af udvalget anmoder herom inden for tidsfristen for afgivelse af udtalelsen.

KAPITEL IX
AFSLUTTENDE BESTEMMELSER

Artikel 40

Evaluering

Senest den 17. oktober 2027 og derefter hver 36. måned evaluerer Kommissionen, hvorledes dette direktiv fungerer og forelægger en rapport for Europa-Parlamentet og Rådet. Rapporten skal navnlig vurdere relevansen af størrelsen af de berørte enheder og sektorerne, delsektorerne og typerne af enheder omhandlet i bilag I og II for, hvordan økonomien og samfundet fungerer i relation til cybersikkerhed. I det øjemed og med henblik på yderligere at fremme det strategiske og operationelle samarbejde tager Kommissionen hensyn til samarbejdsgruppens og CSIRT-netværkets rapporter om de erfaringer, der er gjort på strategisk og operationelt plan. Rapporten ledsages om nødvendigt af et lovgivningsforslag.

Artikel 41

Gennemførelse

1. Medlemsstaterne vedtager og offentliggør senest den 17. oktober 2024 de love og bestemmelser, der er nødvendige for at efterkomme dette direktiv. De underretter straks Kommissionen herom.

De anvender disse love og bestemmelser fra den 18. oktober 2024.

2. De i stk. 1 omhandlede love og bestemmelser skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. Medlemsstaterne fastsætter de nærmere regler for henvisningen.

Artikel 42

Ændringer af forordning (EU) nr. 910/2014

I forordning (EU) nr. 910/2014 udgår artikel 19 med virkning fra den 18. oktober 2024.

Artikel 43

Ændring af direktiv (EU) 2018/1972

I direktiv (EU) 2018/1972 udgår artikel 40 og 41 med virkning fra den 18. oktober 2024.

Artikel 44

Ophævelse

Direktiv (EU) 2016/1148 ophæves med virkning fra den 18. oktober 2024.

Henvisninger til det ophævede direktiv gælder som henvisninger til nærværende direktiv og læses efter sammenligningstabellen i bilag III.

Artikel 45

Ikrafttræden

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Artikel 46

Adressater

Dette direktiv er rettet til medlemsstaterne.
Udfærdiget i Strasbourg, den 14. december 2022.

På Europa-Parlamentets vegne

R. METSOLA

Formand

På Rådets vegne

M. BEK

Formand

([1]) EUT C 233 af 16.6.2022, s. 22.

([2]) EUT C 286 af 16.7.2021, s. 170.

([3]) Europa-Parlamentets holdning af 10.11.2022 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 28.11.2022.

([4]) 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 i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

([5]) Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

([6]) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

([7]) Europa-Parlamentets og Rådets direktiv 97/67/EF af 15. december 1997 om fælles regler for udvikling af Fællesskabets indre marked for posttjenester og forbedring af disse tjenesters kvalitet (EFT L 15 af 21.1.1998, s. 14).

([8]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

([9]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

([10]) Europa-Parlamentets og Rådets forordning (EU) 2022/2554 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 (se side 1 i denne EUT).

([11]) Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed inden for civil

luftfart og om ophævelse af forordning (EF) nr. 2320/2002 (EUT L 97 af 9.4.2008, s. 72).

([12]) Europa-Parlamentets og Rådets forordning (EU) 2018/1139 af 4. juli 2018 om fælles regler for civil luftfart og oprettelse af Den Europæiske Unions Luftfartssikkerhedsagentur og om ændring af forordning (EF) nr. 2111/2005, (EF) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 og direktiv 2014/30/EU og 2014/53/EU og om ophævelse af (EF) nr. 552/2004 og (EF) nr. 216/2008 og Rådets forordning (EØF) nr. 3922/91 (EUT L 212 af 22.8.2018, s. 1).

([13]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (se side 164 i denne EUT).

([14]) Europa-Parlamentets og Rådets forordning (EU) 2021/696 af 28. april 2021 om oprettelse af Unionens rumprogram og Den Europæiske Unions Agentur for Rumprogrammet og om ophævelse af forordning (EU) nr. 912/2010, (EU) nr. 1285/2013 og (EU) nr. 377/2014 og afgørelse nr. 541/2014/EU (EUT L 170 af 12.5.2021, s. 69).

([15]) Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

([16]) Rådets gennemførelsesafgørelse (EU) 2018/1993 af 11. december 2018 om EU's integrerede ordninger for politisk kriserespons (EUT L 320 af 17.12.2018, s. 28).

([17]) Europa-Parlamentets og Rådets afgørelse nr. 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme (EUT L 347 af 20.12.2013, s. 924).

([18]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

([19]) Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 Cybersikkerheden i forbindelse med 5G-net (EUT L 88 af 29.3.2019, s. 42).

([20]) Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

([21]) Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240 (EUT L 166 af 11.5.2021, s. 1).

([22]) EUT L 123 af 12.5.2016, s. 1.

([23]) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

([24]) Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EUT L 277 af 27.10.2022, s. 1).

([25]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).

([26]) EUT C 183 af 11.5.2021, s. 3.

([27]) Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT L 335 af 17.12.2011, s. 1).

([28]) Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

([29]) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

([30]) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

([31]) Europa-Parlamentets og Rådets direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbru-

gerne på det indre marked og om ændring af Rådets direktiv 84/450/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF, 98/27/EF og 2002/65/EF og Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 (direktivet om urimelig handelspraksis) (EUT L 149 af 11.6.2005, s. 22).

([32]) Europa-Parlamentets og Rådets forordning (EU) 2019/1150 af 20. juni 2019 om fremme af retfærdighed og gennemsigtighed for erhvervsbrugere af onlineformidlingstjenester (EUT L 186 af 11.7.2019, s. 57).

BILAG I

SEKTORER AF SÆRLIGT KRITISK BETYDNING

Sektor	Delsektor	Type enhed
1. Energi	a)Elektricitet	—Elektricitetsvirksomheder som defineret i artikel 2, nr. 57), i Europa-Parlamentets og Rådets direktiv (EU) 2019/944 ([1]), der varetager »levering« som defineret i nævnte direktivs artikel 2, nr. 12)
		—Distributionssystemoperatører som defineret i artikel 2, nr. 29), i direktiv (EU) 2019/944
		—Transmissionssystemoperatører som defineret i artikel 2, nr. 35), i direktiv (EU) 2019/944
		—Producenter som defineret i artikel 2, nr. 38), i direktiv (EU) 2019/944
		—Udpegede elektricitetsmarkedsoperatører som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets forordning (EU) 2019/943 ([2])
		—Markedsdeltagere som defineret i artikel 2, nr. 25), i forordning (EU) 2019/943, der leverer tjenester, der vedrører aggregering, fleksibelt elforbrug eller energilagring som defineret i arti-

		kel 2, nr. 18), 20) og 59), i direktiv (EU) 2019/944 —Operatører af ladestationer, der er ansvarlige for forvaltningen og driften af en ladestation, som leverer en ladetjeneste til slutbrugere, herunder i en mobilitetstjenesteudbyders navn og på dennes vegne
	b)Fjernvarme og fjernkøling	—Operatører af fjernvarme eller fjernkøling som defineret i artikel 2, nr. 19), i Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 ([3])
	c) Olie	— Olierørledningsoperatører
		—Operatører af olieproduktionsanlæg, -raffinaderier og -behandlingsanlæg, olielagre og olietransmission
		—Centrale lagerenheder som defineret i artikel 2, litra f), i Rådets direktiv 2009/119/EF ([4])
	d) Gas	—Forsyningsvirksomheder som defineret i artikel 2, nr. 8), i Europa-Parlamentets og Rådets direktiv 2009/73/EF ([5])
		—Distributionssystemoperatører som defineret i artikel 2, nr. 6), i direktiv 2009/73/EF
		—Transmissionssystemoperatører som defineret i artikel 2, nr. 4), i direktiv 2009/73/EF
		—Lagersystemoperatører som defineret i artikel 2, nr. 10), i direktiv 2009/73/EF
		—LNG-systemoperatører som defineret i artikel 2, nr. 12), i direktiv 2009/73/EF
		—Naturgasvirksomheder som defineret i artikel 2, nr. 1), i direktiv 2009/73/EF
		—Operatører af naturgasraffinaderier og -behandlingsanlæg

	e) Brint	—Operatører inden for brintproduktion, -lagring og -transmission
2. Transport	a) Luft	—Luftfartsselskaber som defineret i artikel 3, nr. 4), i forordning (EF) nr. 300/2008, der anvendes til kommercielle formål
		—Lufthavnsdriftsorganer som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets direktiv 2009/12/EF ([6]), lufthavne som defineret i nævnte direktivs artikel 2, nr. 1), herunder de hovedlufthavne, der er anført i afsnit 2 i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 ([7]); og enheder med tilknyttede anlæg i lufthavne
		—Trafikledelses- og kontroloperatører, der udøver flyvekontroltjenester som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 ([8])
	b) Jernbane	—Infrastrukturforvaltere som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets direktiv 2012/34/EU ([9])
		—Jernbanevirksomheder som defineret i artikel 3, nr. 1), i direktiv 2012/34/EU, herunder operatører af servicefaciliteter som defineret i nævnte direktivs artikel 3, nr. 12)
	c) Vand	—Rederier, som udfører passager- og godstransport ad indre vandveje, i højsøfarvand eller kystnært farvand som defineret for søtransport i bilag I til Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 ([10]), bortset fra de enkelte fartøjer, som drives af disse rederier
		—Driftsorganer i havne som defineret i artikel 3, nr. 1), i Europa-Parlamentets og Rådets direktiv 2005/65/EF ([11]), herun-

		der deres havnefaciliteter som defineret i artikel 2, nr. 11), i forordning (EF) nr. 725/2004; og enheder, der opererer anlæg og udstyr i havne
		—Operatører af skibstrafiktjenester som defineret i artikel 3, litra o), i Europa-Parlamentets og Rådets direktiv 2002/59/EF ([12])
	d)Vejtrans-port	—Vejmyndigheder som defineret i artikel 2, nr. 12), i Kommissionens delegerede forordning (EU) 2015/962 ([13]), der er ansvarlige for trafikledelse, med undtagelse af offentlige enheder, for hvilke trafikledelse eller drift af intelligente transportsystemer er en ikkevæsentlig del af deres generelle aktivitet
		—Operatører af intelligente transportsystemer som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets direktiv 2010/40/EU ([14])
3.Bankvirk-somhed		Kreditinstitutter som defineret i artikel 4, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 ([15])
4.Finansielle markeds-infrastruk-turer		—Operatører af markedspladser som defineret i artikel 4, nr. 24), i Europa-Parlamentets og Rådets direktiv 2014/65/EU ([16])
		—Centrale modparter (CCP'er) som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([17])
5. Sundhed		—Sundhedstjenesteydere som defineret i artikel 3, litra g), i Europa-Parlamentets og Rådets direktiv 2011/24/EU ([18])
		—EU-referencelaboratorier, der er omhandlet i artikel 15, i Europa-Parlamentets og Rådets forordning (EU) 2022/2371 ([19])

		—Enheder, der udfører forsknings- og udviklingsaktiviteter vedrørende lægemidler som defineret i artikel 1, nr. 2), i Europa-Parlamentets og Rådets direktiv 2001/83/EF ([20]) —Enheder, der fremstiller farmaceutiske råvarer og farmaceutiske præparater som omhandlet i hovedafdeling C, hovedgruppe 21, i NACE rev. 2 —Enheder, som fremstiller medicinsk udstyr, som den anser for at være kritisk i en folkesundhedsmæssig krisesituation (»liste over kritisk medicinsk udstyr til folkesundhedsmæssige krisesituationer«) i den i artikel 22 i Europa-Parlamentets og Rådets forordning (EU) 2022/123 ([21]) anvendte betydning
6.Drikkevand		Leverandører og distributører af drikkevand som defineret i artikel 2, nr. 1), litra a), i Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 ([22]) bortset fra distributører, for hvilke distribution af drikkevand er en ikkevæsentlig del af deres generelle aktivitet med distribution af andre råvarer og varer
7.Spildevand		Virksomheder, der indsamler, bortskaffer eller behandler byspildevand, husspildevand eller industrispildevand som defineret i artikel 2, nr. 1), 2) og 3), i Rådets direktiv 91/271/EØF ([23]), bortset fra virksomheder, for hvilke indsamling, bortskaffelse eller behandling af byspildevand, husspildevand eller industrispildevand er en ikkevæsentlig del af deres generelle aktivitet
8.Digital infrastruktur		—Udbydere af internetudvekslingspunkter —DNS-tjenesteudbydere, bortset fra operatører af rodnavneservere —Topdomænenavneadministratorer

		—Udbydere af cloudcomputingtjenester
		—Udbydere af datacentertjenester
		—Udbydere af indholdsleveringsnetværk
		— Tillidstjenesteudbydere
		—Udbydere af offentlige elektroniske kommunikationsnet
		—Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester
9.Forvaltning af IKT-tjenester(business to-business)		—Udbydere af administrerede tjenester —Udbydere af administrerede sikkerhedstjenester
10.Offentlig forvaltning		—Offentlige forvaltningsenheder under den centrale forvaltning som defineret af en medlemsstat i overensstemmelse med national ret
		—Offentlige forvaltningsenheder på regionalt plan som defineret af en medlemsstat i overensstemmelse med national ret
11.Rummet		Operatører af jordbaseret infrastruktur, der ejes, forvaltes og drives af medlemsstater eller private parter, og som understøtter levering af rumbaserede tjenester, undtagen udbydere af offentlige elektroniske kommunikationsnet

([1]) Europa-Parlamentets og Rådets direktiv (EU) 2019/944 af 5. juni 2019 om fælles regler for det indre marked for elektricitet og om ændring af direktiv 2012/27/EU (EUT L 158 af 14.6.2019, s. 125).

([2]) Europa-Parlamentets og Rådets forordning (EU) 2019/943 af 5. juni 2019 om det indre marked for elektricitet (EUT L 158 af 14.6.2019, s. 54).

([3]) Europa-Parlamentets og Rådets direktiv (EU) 2018/2001 af 11. december 2018 om fremme af anvendelsen af energi fra vedvarende energikilder (EUT L 328 af 21.12.2018, s. 82).

([4]) Rådets direktiv 2009/119/EF af 14. september 2009 om forpligtelse for medlemsstaterne til at holde minimumslagre af råolie og/eller olieprodukter (EUT L 265 af 9.10.2009, s. 9).

([5]) Europa-Parlamentets og Rådets direktiv 2009/73/EF af 13. juli 2009 om fælles regler for det indre marked for naturgas og om ophævelse af direktiv 2003/55/EF (EUT L 211 af 14.8.2009, s. 94).

([6]) Europa-Parlamentets og Rådets direktiv 2009/12/EF af 11. marts 2009 om lufthavnsafgifter (EUT L 70 af 14.3.2009, s. 11).

([7]) Europa-Parlamentets og Rådets forordning (EU) nr. 1315/2013 af 11. december 2013 om Unionens retningslinjer for udvikling af det transeuropæiske transportnet og om ophævelse af afgørelse nr. 661/2010/EU (EUT L 348 af 20.12.2013, s. 1).

([8]) Europa-Parlamentets og Rådets forordning (EF) nr. 549/2004 af 10. marts 2004 om rammerne for oprettelse af et fælles europæisk luftrum (»rammeforordningen«) (EUT L 96 af 31.3.2004, s. 1).

([9]) Europa-Parlamentets og Rådets direktiv 2012/34/EU af 21. november 2012 om oprettelse af et fælles europæisk jernbaneområde (EUT L 343 af 14.12.2012, s. 32).

([10]) Europa-Parlamentets og Rådets forordning (EF) nr. 725/2004 af 31. marts 2004 om bedre sikring af skibe og havnefaciliteter (EUT L 129 af 29.4.2004, s. 6).

([11]) Europa-Parlamentets og Rådets direktiv 2005/65/EF af 26. oktober 2005 om bedre havnesikring (EUT L 310 af 25.11.2005, s. 28).

([12]) Europa-Parlamentets og Rådets direktiv 2002/59/EF af 27. juni 2002 om oprettelse af et trafikovervågnings- og trafikinformationssystem for skibsfarten i Fællesskabet og om ophævelse af Rådets direktiv 93/75/EØF (EFT L 208 af 5.8.2002, s. 10).

([13]) Kommissionens delegerede forordning (EU) 2015/962 af 18. december 2014 om supplerende regler til Europa-Parlamentets og Rådets direktiv 2010/40/EU for så vidt angår tilrådighedsstillelse af EU-dækkende tidstro trafikinformationstjenester (EUT L 157 af 23.6.2015, s. 21).

([14]) Europa-Parlamentets og Rådets direktiv 2010/40/EU af 7. juli 2010 om rammerne for indførelse af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportformer (EUT L 207 af 6.8.2010, s. 1).

([15]) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

([16]) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 af 12.6.2014, s. 349).

([17]) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).

([18]) Europa-Parlamentets og Rådets direktiv 2011/24/EU af 9. marts 2011 om patientrettigheder i forbindelse med grænseoverskridende sundhedsydelser (EUT L 88 af 4.4.2011, s. 45).

([19]) Europa-Parlamentets og Rådets forordning (EU) 2022/2371 af 23. november 2022 om alvorlige grænseoverskridende sundhedstrusler og om ophævelse af afgørelse nr. 1082/2013/EU (EUT L 314 af 6.12.2022, s. 26).

([20]) Europa-Parlamentets og Rådets direktiv 2001/83/EF af 6. november 2001 om oprettelse af en fællesskabskodeks for humanmedicinske lægemidler (EFT L 311 af 28.11.2001, s. 67).

([21]) Europa-Parlamentets og Rådets forordning (EU) 2022/123 af 25. januar 2022 om styrkelse af Det Europæiske Lægemiddelagenturs rolle i forbindelse med kriseberedskab og krisestyring med hensyn til lægemidler og medicinsk udstyr (EUT L 20 af 31.1.2022, s. 1).

([22]) Europa-Parlamentets og Rådets direktiv (EU) 2020/2184 af 16. december 2020 om kvaliteten af drikkevand (EUT L 435 af 23.12.2020, s. 1).

([23]) Rådets direktiv 91/271/EØF af 21. maj 1991 om rensning af byspildevand (EFT L 135 af 30.5.1991, s. 40).

BILAG II

ANDRE KRITISKE SEKTORER

Sektor	Delsektor	Type enhed
1. Post- og kurertjenester		Postbefordrende virksomheder som defineret i artikel 2, nr. 1a), i direktiv

		97/67/EF, herunder udbydere af kurertjenester
2.Affaldshåndtering		Virksomheder, der varetager affaldshåndtering som defineret i artikel 3, nr. 9), i Europa-Parlamentets og Rådets direktiv 2008/98/EF ([1]), bortset fra virksomheder, for hvilke affaldshåndtering ikke er deres vigtigste økonomiske aktivitet
3.Fremstilling, produktion og distribution af kemikalier		Virksomheder, der beskæftiger sig med fremstilling af stoffer og distribution af stoffer eller blandinger som omhandlet i artikel 3, nr. 9) og 14), i Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 ([2]) og virksomheder, der beskæftiger sig med produktion af artikler som defineret i artikel 3, nr. 3), i nævnte forordning ud af stoffer eller blandinger
4.Produktion, tilvirkning og distribution af fødevarer		Fødevarevirksomheder som defineret i artikel 3, nr. 2), i Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 ([3]), der beskæftiger sig med engrosdistribution og industriel produktion og tilvirkning
5.Fremstilling	a)Fremstilling af medicinsk udstyr og medicinsk udstyr til in vitro-diagnostik	Enheder, der fremstiller medicinsk udstyr som defineret i artikel 2, nr. 1), i Europa-Parlamentets og Rådets forordning (EU) 2017/745 ([4]), og enheder, der fremstiller medicinsk udstyr til in vitro-diagnostik som defineret i artikel 2, nr. 2), i Europa-Parlamentets og Rådets forordning (EU) 2017/746 ([5]), med undtagelse af enheder, der fremstiller medicinsk udstyr omhandlet i dette direktivs bilag I, punkt 5, femte led
	b)Fremstilling af computere og elektroniske og	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 26, i NACE rev. 2

	optiske produkter	
	c)Fremstilling af elektrisk udstyr	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 27, i NACE rev. 2
	d)Fremstilling af maskiner og udstyr i.a.n.	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 28, i NACE rev. 2
	e)Fremstilling af motorkøretøjer, påhængsvogne og sættevogne	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 29, i NACE rev. 2
	f)Fremstilling af andre transportmidler	Virksomheder, der udøver en af de økonomiske aktiviteter, der er omhandlet i hovedafdeling C, hovedgruppe 30, i NACE rev. 2
6.Digitale udbydere		—Udbydere af onlinemarkedspladser
		—Udbydere af onlinesøgemaskiner
		—Udbydere af platforme for sociale netværkstjenester
7.Forskning		Forskningsorganisationer

([1]) Europa-Parlamentets og Rådets direktiv 2008/98/EF af 19. november 2008 om affald og om ophævelse af visse direktiver (EUT L 312 af 22.11.2008, s. 3).

([2]) Europa-Parlamentets og Rådets forordning (EF) nr. 1907/2006 af 18. december 2006 om registrering, vurdering og godkendelse af samt begrænsninger for kemikalier (REACH), om oprettelse af et europæisk kemikalieagentur og om ændring af direktiv 1999/45/EF og ophævelse af Rådets forordning (EØF) nr. 793/93 og Kommissionens forordning (EF) nr. 1488/94 samt Rådets direktiv 76/769/EØF og Kommissionens direktiv 91/155/EØF, 93/67/EØF, 93/105/EF og 2000/21/EF (EUT L 396 af 30.12.2006, s. 1).

([3]) Europa-Parlamentets og Rådets forordning (EF) nr. 178/2002 af 28. januar 2002 om generelle principper og krav i fødevarelovgivningen, om oprettelse af Den Europæiske Fødevaresikkerhedsautoritet og om procedurer vedrørende fødevaresikkerhed (EFT L 31 af 1.2.2002, s. 1).

([4]) Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1).

([5]) Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og om ophævelse af direktiv 98/79/EF og Kommissionens afgørelse 2010/227/EU (EUT L 117 af 5.5.2017, s. 176).

BILAG III

SAMMENLIGNINGSTABEL

Direktiv (EU) 2016/1148	Nærværende direktiv
Artikel 1, stk. 1	Artikel 1, stk. 1
Artikel 1, stk. 2	Artikel 1, stk. 2
Artikel 1, stk. 3	—
Artikel 1, stk. 4	Artikel 2, stk. 12
Artikel 1, stk. 5	Artikel 2, stk. 13
Artikel 1, stk. 6	Artikel 2, stk. 6 og 11
Artikel 1, stk. 7	Artikel 4
Artikel 2	Artikel 2, stk. 14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	—
Artikel 6	—
Artikel 7, stk. 1	Artikel 7, stk. 1 og 2
Artikel 7, stk. 2	Artikel 7, stk. 4

Artikel 7, stk. 3	Artikel 7, stk. 3
Artikel 8, stk. 1-5	Artikel 8, stk. 1-5
Artikel 8, stk. 6	Artikel 13, stk. 4
Artikel 8, stk. 7	Artikel 8, stk. 6
Artikel 9, stk. 1, 2 og 3	Artikel 10, stk. 1, 2 og 3
Artikel 9, stk. 4	Artikel 10, stk. 9
Artikel 9, stk. 5	Artikel 10, stk. 10
Artikel 10, stk. 1, stk. 2 og stk. 3, første afsnit	Artikel 13, stk. 1, 2 og 3
Artikel 10, stk. 3, andet afsnit	Artikel 23, stk. 9
Artikel 11, stk. 1	Artikel 14, stk. 1 og 2
Artikel 11, stk. 2	Artikel 14, stk. 3
Artikel 11, stk. 3	Artikel 14, stk. 4, første afsnit, litra a)-q) og litra s), og stk. 7
Artikel 11, stk. 4	Artikel 14, stk. 4, første afsnit, litra r), og andet afsnit
Artikel 11, stk. 5	Artikel 14, stk. 8
Artikel 12, stk. 1-5	Artikel 15, stk. 1-5
Artikel 13	Artikel 17
Artikel 14, stk. 1 og 2	Artikel 21, stk. 1-4
Artikel 14, stk. 3	Artikel 23, stk. 1
Artikel 14, stk. 4	Artikel 23, stk. 3
Artikel 14, stk. 5	Artikel 23, stk. 5, 6 og 8
Artikel 14, stk. 6	Artikel 23, stk. 7
Artikel 14, stk. 7	Artikel 23, stk. 11
Artikel 15, stk. 1	Artikel 31, stk. 1
Artikel 15, stk. 2, første afsnit, litra a)	Artikel 32, stk. 2, litra e)
Artikel 15, stk. 2, første afsnit, litra b)	Artikel 32, stk. 2, litra g)

Artikel 15, stk. 2, andet afsnit	Artikel 32, stk. 3
Artikel 15, stk. 3	Artikel 32, stk. 4, litra b)
Artikel 15, stk. 4	Artikel 31, stk. 3
Artikel 16, stk. 1 og 2	Artikel 21, stk. 1-4
Artikel 16, stk. 3	Artikel 23, stk. 1
Artikel 16, stk. 4	Artikel 23, stk. 3
Artikel 16, stk. 5	—
Artikel 16, stk. 6	Artikel 23, stk. 6
Artikel 16, stk. 7	Artikel 23, stk. 7
Artikel 16, stk. 8 og 9	Artikel 21, stk. 5, og artikel 23, stk. 11
Artikel 16, stk. 10	—
Artikel 16, stk. 11	Artikel 2, stk. 1, 2 og 3
Artikel 17, stk. 1	Artikel 33, stk. 1
Artikel 17, stk. 2, litra a)	Artikel 32, stk. 2, litra e)
Artikel 17, stk. 2, litra b)	Artikel 32, stk. 4, litra b)
Artikel 17, stk. 3	Artikel 37, stk. 1, litra a) og b)
Artikel 18, stk. 1	Artikel 26, stk. 1, litra b), og stk. 2
Artikel 18, stk. 2	Artikel 26, stk. 3
Artikel 18, stk. 3	Artikel 26, stk. 4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	—
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46

Bilag I, punkt 1	Artikel 11, stk. 1
Bilag I, punkt 2, litra a), nr. i)-iv)	Artikel 11, stk. 2, litra a)-d)
Bilag I, punkt 2, litra a), nr. v)	Artikel 11, stk. 2, litra f)
Bilag I, punkt 2, litra b)	Artikel 11, stk. 4
Bilag I, punkt 2, litra c), nr. i) og ii)	Artikel 11, stk. 5, litra a)
Bilag II	Bilag I
Bilag III, punkt 1 og 2	Bilag II, punkt 6
Bilag III, punkt 3	Bilag I, punkt 8

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Danmark er blandt de mest digitaliserede samfund i verden. Et stærkt digitaliseret samfund som Danmark er i stigende grad afhængigt af telenettet, der bl.a. anvendes som platform for telefoni og datakommunikation. Det samlede telenet er således en af de mest kritiske dele af samfundets informations- og kommunikationsteknologiske infrastruktur. Det er en forudsætning for det digitale samfund, at mennesker og maskiner kan kommunikere digitalt på en sikker og effektiv måde. Tilgængelighed, fortrolighed og integritet af teletjenesterne er af kritisk betydning for samfundets funktion og sikkerhed.

Dermed er samfundet også særdeles sårbart, hvis dele af telenettet i kortere eller længere perioder er ude af drift.

Hertil kommer, at vi står over for et mere sammensat og komplekst trusselsbillede end for blot få år siden. Det gælder ikke mindst på cybersikkerhedsområdet, hvilket understreges af Center for Cybersikkerheds trusselsvurdering fra 2024. Det fremgår bl.a. heraf, at niveauet for cyberkriminalitet er MEGET HØJT, og at truslen fra cyberaktivisme er HØJ. Truslen fra destruktive cyberangreb er tidligere på året blevet hævet fra LAV til MIDDEL. Niveauet blev hævet på baggrund af en udvikling i Ruslands risikovillighed i forhold til at anvende hybride virkemidler, herunder destruktive cyberangreb, mod europæiske NATO-lande. Hertil kommer risikoen for sabotage og hærværk mod kritiske dele af teleinfrastrukturen. De store datamængder, som sendes via telenettet, indebærer desuden, at telenettet er et oplagt mål for aktører, der vil udøve industrispionage mod virksomheder eller spionage mod myndigheder og personer. I dag er truslen fra cyberspionage blandt de mest alvorlige trusler, som vores samfund står overfor.

Danmarks sårbarhed over for bl.a. cybertruslen vil øges i takt med den fortsatte digitale udvikling. Den fortsatte digitale udvikling stiller nye og større krav til vores håndtering af sikkerheden i teleinfrastrukturen. Det gælder ikke kun i Danmark, men på tværs af EU. Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af cybertrusler og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater.

Dette er bl.a. baggrunden for, at Europa-Parlamentet og Rådet har vedtaget 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) 2016/2259 (NIS 2-direktivet).

NIS 2-direktivet har til formål at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne. Direktivet stiller bl.a. cybersikkerhedskrav til virksomheder, myndigheder og organisationer (enheder) inden for en lang række samfundskritiske sektorer, som bl.a. omfatter energi, transport, bankvirksomhed, sundhed, drikke- og spildevand, digital infrastruktur og den offentlige forvaltning. Samtidig fastsættes en række oplysnings- og underretningspligter over for myndighederne, herunder underretning ved væsentlige hændelser samt pligt til at oplyse enhedernes brugere om bl.a. væsentlige hændelser og eventuelle modforholdsregler, som brugerne kan træffe. Direktivet styrker desuden myndighedernes tilsynsbeføjelser og håndhævelsesmuligheder.

Formålet med dette lovforslag er at implementere NIS 2-direktivet for telesektoren. Telesektoren spiller en afgørende rolle i et højt digitaliseret samfund som det danske. Der eksisterer derfor allerede omfattende regulering af informationssikkerhed og beredskab i telesektoren, herunder navnlig lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021. På visse områder, herunder navnlig i forhold til leverandørsikkerhed, vurderes den nuværende regulering af telesektoren at sikre et højere sikkerhedsniveau end det, der følger af NIS 2-direktivet.

Det er derfor Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at implementeringen af NIS 2-direktivet for telesektoren bør ske særskilt, således at implementeringen af NIS 2-direktivets minimumskrav ikke medfører, at kravene i den eksisterende regulering for sikkerheden og beredskabet i telesektoren sænkes.

Forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, der implementerer NIS 2-direktivet i de omfattede sektorer, fremsættes samtidig med nærværende lovforslag.

2. Baggrund

2.1. Formål

Formålet med lovforslaget er at implementere NIS 2-direktivet i telesektoren. Med nærværende lovforslag foreslås det, at implementeringen af NIS 2-direktivet i telesektoren sker gennem en integration med den eksisterende regulering på området, herunder navnlig lov om sikkerhed i net og tjenester,

jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Med henblik på at skabe et ensartet og overskueligt regelsæt på teleområdet foreslås det derfor, at teleloven ophæves, og at implementeringen af NIS 2-direktivet i telesektoren og den eksisterende regulering på området samles i én lov.

Lov om sikkerhed i net og tjenester fastsætter en overordnet ramme for de informationssikkerheds- og beredskabskrav samt oplysnings- og underretningspligter, der gælder for teleudbydere, ligesom loven regulerer tilsyns- og håndhævelsesbeføjelser samt sanktionsmuligheder. Lovens bestemmelser om informationssikkerheds- og beredskabskrav samt oplysnings- og underretningspligter er primært udformet som bemyndigelser, der er udmøntet i fire bekendtgørelser.

Lov om sikkerhed i net og tjenester suppleres i øvrigt af lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur, som bl.a. giver myndighederne mulighed for at forbyde konkrete leverandøraftaler vedrørende den kritiske teleinfrastruktur, hvis aftalerne vurderes at udgøre en trussel mod statens sikkerhed.

Dele af lov om sikkerhed i net og tjenester og de bekendtgørelser, der er udstedt i medfør af loven, bygger på EU-regulering. Lovgivningen implementerer således en række bestemmelser i Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EU's telekodeks).

2.1.1. Generelt om EU's telekodeks

Den 11. december 2018 vedtog Europa-Parlamentet og Rådet direktiv (EU) 2018/1972 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EU's telekodeks). EU's telekodeks samler og reviderer de fire centrale EU-direktiver på teleområdet, herunder bl.a. rammedirektivet og forsyningspligtsdirektivet.

EU's telekodeks har til formål at forenkle EU-reguleringens struktur, således at der skabes en mere sammenhængende regulering af elektroniske kommunikationsnet og -tjenester. Samtidig tager EU's telekodeks højde for den samfundsmæssige udvikling, hvor forbrugere og virksomheder i stadig stigende grad anvender digitale, internetbaserede tjenester frem for traditionelle teletjenester. Samtidig har EU's telekodeks til formål at sikre, at digi-

tale internetbaserede tjenester bliver omfattet af bl.a. passende informationssikkerhedskrav.

EU's telekodeks fastlægger en retlig ramme for reguleringen af elektronisk kommunikation og indeholder bl.a. bestemmelser om sikkerheden i offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester. EU's telekodeks fastlægger således bl.a. overordnede sikkerhedskrav til samt oplysnings- og underretningspligter for teleudbydere.

Derudover fastlægger EU's telekodeks en generel forpligtelse for medlemsstaterne til at sikre, at der er kompetente myndigheder, som fører tilsyn med bl.a. teleudbydernes overholdelse af sikkerhedskravene- samt oplysnings- og underretningspligterne, ligesom direktivet – med henblik på at sikre overholdelsen heraf – fastlægger tilsyns- og håndhævelsesbeføjelser. Den centrale bestemmelse i den henseende er direktivets artikel 41, der ligeledes er implementeret i lov om sikkerhed i net og tjenester.

Endvidere indeholder EU's telekodeks mulighed for, at medlemsstaterne kan fastsætte sanktioner, herunder bøder, for overtrædelse af de fastsatte sikkerhedskrav samt oplysnings- og underretningspligter, som ligeledes er implementeret i lov om sikkerhed i net og tjenester.

De sikkerhedskrav samt oplysnings- og underretningspligter mv., der gælder for teleudbydere, har således på EU-plan hidtil været fastlagt i EU's telekodeks.

2.1.2. Generelt om NIS 2-direktivet

NIS 2-direktivet ophæver og erstatter 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 i hele Unionen (NIS 1-direktivet).

NIS 1-direktivet fastlægger for det første krav til rammerne for arbejdet med sikkerhed i net- og informationssystemer både nationalt og på EU-niveau, herunder krav til samarbejdsorganer og myndighedsstruktur. For det andet stiller direktivet krav om, at der fastsættes sikkerhedskrav og underretningspligter for operatører af væsentlige tjenester og udbydere af digitale tjenester. Med NIS 1-direktivet er der således allerede taget skridt hen mod at øge cybersikkerheden på tværs af EU.

Baggrunden for NIS 2-direktivet er, at der fra EU's side er konstateret store forskelle i medlemsstaternes gennemførelse af NIS 1-direktivet, herunder med hensyn til, hvilke enheder der anses for omfattet af direktivet, da afgrænsningen heraf i vid udstrækning blev overladt til medlemsstaternes skøn. NIS 1-direktivet giver også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af direktivets sikkerheds- og hændelsesrapporteringsforpligtelser samt bestemmelserne om tilsyn og håndhævelse.

Formålet med NIS 2-direktivet er derfor at skabe et højere og mere ensartet cybersikkerhedsniveau på tværs af medlemsstaterne. NIS 2-direktivet omfatter også telesektoren og indebærer derfor bl.a., at artikel 40 og 41 i EU's telekodeks ophæves. Fremadrettet vil det således primært være NIS 2-direktivet, der på EU-plan fastlægger krav til og forpligtelser for teleudbydernes sikkerhed, ligesom medlemsstaternes tilsyns- og håndhævelsesbeføjelser samt sanktionsmuligheder over for teleudbyderne vil følge heraf.

Det følger af NIS 2-direktivets præambelbetragtning nr. 92, at baggrunden for ophævelsen af artikel 40 og 41 i EU's telekodeks er et ønske fra EU's side om at strømline de krav og forpligtelser til cybersikkerhed, der pålægges teleudbydere, med de krav og forpligtelser, der pålægges enheder i de øvrige sektorer mv., som omfattes af NIS 2-direktivets anvendelsesområde. Derudover er der fra EU's side et ønske om at gøre det muligt for teleudbyderne og myndighederne at drage fordel af de retlige rammer, der er fastsat i NIS 2-direktivet i forhold til samarbejdsorganer og myndighedsstruktur.

NIS 2-direktivet fastsætter på den baggrund nærmere regler for cybersikkerhedsforanstaltninger (artikel 21) og rapporteringsforpligtelser (artikel 23) og mekanismer for effektivt samarbejde på nationalt plan og på EU-plan (kapitel II og III), ligesom direktivet tilvejebringer styrkede tilsyns- og håndhævelsesbeføjelser (kapitel VII), der skal bidrage til at sikre en effektiv overholdelse og håndhævelse af forpligtelserne i direktivet.

2.1.3. Implementering af NIS 2-direktivet for telesektoren

Henset til, at NIS 2-direktivet omfatter telesektoren og ændrer i EU's telekodeks, er der behov for at tilpasse den gældende lov om sikkerhed i net og tjenester. Foruden bestemmelser, der implementerer EU's telekodeks, indeholder lov om sikkerhed i net og tjenester også nationale særregler, herunder skærpede krav til teleudbydernes informationssikkerhed og beredskab. Der

er tale om krav, der på visse områder går videre end de krav, der følger af EU-reguleringen på området.

Baggrunden for indførelsen af de skærpede nationale særregler var navnlig at sikre, at kravene til teleudbydernes sikkerhed i højere grad tog højde for samfundets afhængighed af telenettet og afspejlede det aktuelle trusselsbillede, idet Forsvarets Efterretningstjeneste vurderede, at truslen fra især cyberangreb og avanceret industrispionage var stærkt stigende, jf. Folketingstidende 2015-16, tillæg A, L 10 som fremsat, side 5. Center for Cybersikkerhed har i centerets seneste trusselsvurdering om cybertruslen mod Danmark 2024 bl.a. vurderet, at truslen fra cyberspionage og cyberkriminalitet er MEGET HØJ, at truslen fra cyberaktivisme mod Danmark er HØJ, og at truslen fra destruktive cyberangreb er MIDDEL.

På baggrund af det skærpede trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet som følge af danske myndigheders, virksomheders og borgeres afhængighed af en velfungerende teleinfrastruktur er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de eksisterende nationale særregler bør videreføres med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau i telesektoren.

Idet de eksisterende nationale særregler ønskes videreført, finder Ministeriet for Samfundssikkerhed og Beredskab, at implementeringen af NIS 2-direktivet bør ske ved et sektorspecifikt lovforslag. Dermed vil kravene og forpligtelserne, der følger af NIS 2-direktivet, kunne integreres med den eksisterende regulering af sikkerheden og beredskab i telesektoren. Henset til, at implementeringen af NIS 2-direktivet vil berøre et større antal af bestemmelserne i den gældende lov om sikkerhed i net og tjenester, har Ministeriet for Samfundssikkerhed og Beredskab valgt at fremsætte forslag til en ny hovedlov frem for en ændring af den gældende lov. Det vurderes, at en ny hovedlov vil bidrage til at gøre den nye regulering mere overskuelig for teleudbyderne og andre aktører på området.

Det bemærkes i den forbindelse, at der med lovforslaget ikke indføres nye skærpede nationale særregler. Derudover vil de nye cybersikkerhedskrav samt oplysnings- og underretningspligter, som følger af NIS 2-direktivet, blive gennemført ud fra princippet om direktivnær implementering. Nærværende lovforslag vil således ikke medføre, at teleudbydere vil blive pålagt nye krav eller pligter, der vil gå videre end det, der følger af et NIS 2-direktivets minimumskrav.

Telesektoren er således ikke omfattet af forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, som fremsættes af Ministeriet for Samfundssikkerhed og Beredskab samtidig med nærværende lovforslag, og som skaber en fælles lovgivningsramme på tværs af en række af de øvrige sektorer, der er omfattet af NIS 2-direktivet. De myndighedsstrukturer og samarbejdsorganer, som NIS 2-direktivet fastsætter rammerne for, vil imidlertid blive beskrevet – og i relevant omfang reguleret – i det tværgående lovforslag, og nærværende lovforslag skal således ses i sammenhæng hermed.

2.1.3.1. Sammenhængen med lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, herunder udpegelse af en national CSIRT

NIS 2-direktivet implementeres ved, at Ministeriet for Samfundssikkerhed og Beredskab fremsætter forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, som skaber en fælles lovgivningsramme på tværs af de sektorer, der er omfattet af NIS 2-direktivet med undtagelse af bl.a. telesektoren.

Det følger således af § 1, stk. 2, 2. pkt., i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, at loven ikke finder anvendelse på enheder i det omfang, de er omfattet af lov om cybersikkerhed i telesektoren. Det følger af bestemmelsens 3. pkt., at lovens § 17 dog finder anvendelse for bl.a. telesektoren.

§ 17 i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau implementerer NIS 2-direktivets artikel 10, som forpligter medlemsstaterne til at oprette eller udpege en eller flere nationale kompetente myndigheder, et nationalt centralt kontaktpunkt samt en eller flere nationale CSIRT'er (Computer Security Incident Response Teams, dvs. enheder der håndterer it-sikkerhedshændelser).

Center for Cybersikkerhed blev ved implementeringen af NIS 1-direktivet udpeget som CSIRT i Danmark, og opgaven har hidtil været varetaget som en del af Netsikkerhedstjenesten i Center for Cybersikkerhed.

Med den kongelige resolution af 29. august 2024 er Center for Cybersikkerhed, bortset fra bl.a. Netsikkerhedstjenesten, blevet overdraget til Ministeriet for Samfundssikkerhed og Beredskab. Det betyder, at ansvaret for CSIRT-funktionen indtil videre forbliver på Forsvarsministeriets område.

Med nærværende lovforslag lægges der op til, at bl.a. hændelser skal indberettes til både Center for Cybersikkerhed og CSIRT'en. Det forudsættes på den baggrund, at der vil være et tæt samarbejde mellem Center for Cybersikkerhed og CSIRT'en. En nærmere fastlæggelse af rammerne for samarbejdet vil kunne ske i en samarbejdsaftale.

Der henvises i øvrigt til kapitel 5 i lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau og bemærkningerne hertil.

2.2. Sammenhængen med CER-direktivet

NIS 2-direktivet skal ses i sammenhæng med Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF (CER-direktivet).

Ministeriet for Samfundssikkerhed og Beredskab fremsætter samtidig med nærværende lovforslag et lovforslag om kritiske enheders modstandsdygtighed, der vil implementere CER-direktivet på tværs af de omfattede sektorer med undtagelse af energisektoren.

CER-direktivet har til formål at styrke kritiske enheders modstandsdygtighed, således at de er bedre i stand til at håndtere risiciene for deres drift, som kan føre til forstyrrelse i leveringen af væsentlige tjenester. CER-direktivet fastlægger derfor bl.a. overordnede sikkerhedskrav og oplysnings- og underretningspligter samt tilsyns- og håndhævelsesbeføjelser, herunder sanktioner, i forhold til enheder, som medlemsstaterne identificerer som kritiske enheder inden for en række sektorer og delsektorer, ligesom direktivet fastsætter krav til myndighedsopgaver, herunder myndighedsstruktur og samarbejdsorganer.

Det følger imidlertid bl.a. af CER-direktivets artikel 8, at medlemsstaterne skal sikre, at direktivets sikkerhedskrav og oplysnings- og underretningspligter (kapitel III) samt tilsyns- og håndhævelsesbeføjelser, herunder sanktioner (kapitel VI), ikke finder anvendelse for enheder, der er omfattet af den digitale infrastruktur. Til denne kategori hører bl.a. teleudbydere.

Det følger af NIS 2-direktivets præambelbetragtning nr. 31, at baggrunden for denne undtagelse i CER-direktivets artikel 8 er, at teleudbydere i det væsentligste er baseret på net- og informationssystemer, og derfor bør de krav og forpligtelser, der pålægges disse i medfør af NIS 2-direktivet, om-

handle sådanne systemers fysiske sikkerhed. Det følger endvidere af CER-direktivets præambelbetragtning nr. 20, at trusler mod sikkerheden i net- og informationssystemer kan have forskellig oprindelse, og NIS 2-direktivet anvender derfor en tilgang, der omfatter alle farer, og som omfatter net- og informationssystemers modstandsdygtighed samt disse systemers fysiske komponenter og fysiske miljø. Eftersom kravene og forpligtelserne i NIS 2-direktivet mindst svarer til de tilsvarende krav og forpligtelser i CER-direktivet, bør kravene og forpligtelserne ikke finde anvendelse på teleudbydere for at undgå dobbeltarbejde og unødvendige administrative byrder. Da disse spørgsmål således er omfattet af NIS 2-direktivet, finder de nævnte kapitler i CER-direktivet ikke anvendelse for teleudbydere.

Det skal imidlertid bemærkes, at medlemslandene ikke desto mindre skal identificere, hvilke teleudbydere der skal anses for kritiske enheder i henhold til CER-direktivets artikel 6.

3. Lovforslagets hovedpunkter

3.1. Teleudbyderbegrebet

3.1.1. Gældende ret

Der er i lov om sikkerhed i net og tjenester bl.a. fastsat regler om informationssikkerheds- og beredskabskrav til samt oplysnings- og underretningspligter for de teleudbydere, der er omfattet af artikel 40 og 41 i EU's telekodeks omkring sikkerhed i net og tjenester.

3.1.1.1. Kategorisering af typer af udbydere

I lov om sikkerhed i net og tjenester skelnes mellem udbyder, erhvervsmæssige udbydere og udbydere af NUIK-tjenester.

En udbyder defineres i lov om sikkerhed i net og tjenesters § 2, nr. 4, som den, der med et kommercielt formål stiller produkter, elektroniske kommunikationsnet eller -tjenester til rådighed for andre. Det fremgår af bemærkningerne til lovens § 2, nr. 4, jf. Folketingstidende 2015-16, A, L 10 som fremsat den 7. oktober 2015, at definitionen indholdsmæssigt er identisk med den tilsvarende definition i telelovens § 2, nr. 1, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Det fremgår af de specielle bemærkninger til telelovens § 2, nr. 1, jf. Folketingstidende 2015-16, A, L 10 som fremsat den 7. oktober 2015, at enhver, der markedsfører og sælger produkter og elektroniske kommunikationsnet eller -tjenester omfattet af lovforslaget til andre, anses for at være udbydere

med de rettigheder, dette giver bl.a. i relation til netadgang. Det vil sige, at alle virksomheder, som på kommercielt grundlag betjener andre slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester med henblik på at formidle dele af disses teletrafik, er omfattet af lovens udbyderbegreb.

Det er i den forbindelse uden betydning, om de pågældende har anlagt egen infrastruktur eller baserer deres aktiviteter fuldt ud på lejet infrastrukturkapacitet. Det er ligeledes uden betydning, om de pågældende udbyder offentligt tilgængelige tjenester eller tjenester eksempelvis i form af lukkede net, herunder virtuelle lukkede net, til andre.

Endelig er det uden betydning, hvilken form for tjenester der udbydes, herunder om der eventuelt alene tilbydes formidling af internettrafik, håndtering af udgående samtaler via operatørforvalg og fast operatørvalg, gensalg af andre virksomheders tjenester, et eller flere netadgangs- eller samtrafikprodukter til andre udbydere af elektroniske kommunikationsnet eller -tjenester eller lignende.

Det fremgår endvidere af de specielle bemærkninger til telelovens § 2, nr. 1, at boligforeninger, hoteller, cafeer mv., som udbyder elektroniske kommunikationsnet eller -tjenester, vil kunne være omfattet af definitionen, hvis udbuddet sker med et kommercielt formål. Det afgørende ved vurderingen heraf er, om udbuddet af nettet eller tjenesten sker på markedsmæssige vilkår, herunder som led i markedsføringen af virksomheden eller foreningen. Således kan også indirekte kommerciel tilrådighedsstillelse være omfattet af definitionen, eksempelvis hvis en virksomhed som et direkte eller indirekte led i markedsføringen stiller for eksempel en internettjeneste gratis til rådighed for virksomhedens kunder eller gæster.

Erhvervsmæssige udbydere defineres i lov om sikkerhed i net og tjenesters § 2, nr. 5, som udbydere, der med et kommercielt formål udbyder produkter, elektroniske kommunikationsnet og -tjenester som sin hovedydelse eller som en ikke accessorisk del af virksomheden. Det fremgår af bemærkningerne til bestemmelsen, at definitionen er identisk med den tilsvarende definition i telelovens § 2, nr. 2, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis. Det fremgår af de specielle bemærkninger til telelovens § 2, nr. 2, at erhvervsmæssige udbydere skal anses som en underkategori til udbyderbegrebet i nr. 1, som har til formål at nuancere udbyderbegrebet, således at der tages højde for den teknologiske udvikling og de niveauer af rettigheder og forpligtelser, som knytter sig til loven og anden lovgivning. I forlængelse heraf fremgår det af be-

mærkningerne, at den teknologiske udvikling bl.a. indebærer, at det i dag er relativt mange, der er udbydere af elektroniske kommunikationsnet eller -tjenester. Dette omfatter ifølge bemærkningerne bl.a. tilfælde, hvor en virksomhed etablerer trådløs infrastruktur med henblik på at levere internetadgang til deres kunder eller lignende.

Etableringen af underkategorien 'erhvervsmæssige udbydere' skal således ifølge bemærkningerne ses i lyset af, at det ikke vurderes hensigtsmæssigt at anvende det brede udbyderbegreb i telelovens § 2, nr. 1, uden yderligere afgrænsning. Begrebet erhvervsmæssige udbydere omfatter ifølge bemærkningerne til telelovens § 2, nr. 2, udbydere, der driver virksomhed omfattet af loven som deres hovedvirksomhed eller som en selvstændig del af virksomheden. Udbydere, der har mobiltelefoni, fastnettelefoni, bredbånd mv. som deres hovedvirksomhed, vil således være omfattet af denne kategori. Ved 'som ikke accessorisk del af virksomheden' forstås, at udbuddet ikke kun er en accessorisk del af virksomheden. Et hotel, der eksempelvis tilbyder sine kunder adgang til trådløst internet, vil som udgangspunkt ikke være erhvervsmæssig udbyder, idet udbuddet i den forbindelse må anses for at være en integreret del af at leje et hotelværelse. Det følger dog af bemærkningerne, at der altid vil være tale om en konkret vurdering.

3.1.1.2. Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester

Lov om sikkerhed i net og tjenester finder kun anvendelse for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester.

I lov om sikkerhed i net og tjenesters § 2, nr. 1, defineres et elektronisk kommunikationsnet som et transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres. Lovens § 2, nr. 1, implementerer artikel 2, nr. 1, i EU's telekodeks.

En elektronisk kommunikationstjeneste defineres i lovens § 2, nr. 2, som en tjeneste, der helt eller delvis består i elektronisk overførsel af kommunika-

tion i form af lyd, billeder, tekst eller kombinationer heraf ved hjælp af radio- eller telekommunikationsteknik mellem nettermineringspunkter.

Offentligt tilgængelige elektroniske kommunikationsnet og -tjenester skal anses som en underkategori til elektroniske kommunikationsnet og -tjenester, og defineres i lovens § 2, nr. 3, som elektroniske kommunikationsnet og -tjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

Det fremgår af bemærkningerne til bestemmelsen, jf. Folketingstidende 2015-16, A, L 10 som fremsat den 7. oktober 2015, at definitionen skal fortolkes i overensstemmelse med såvel offentlige elektroniske kommunikationsnet i telelovens § 2, nr. 5, som offentlig elektronisk kommunikationstjeneste i telelovens § 2, nr. 8, og at bestemmelsen derfor skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevant praksis.

Det fremgår af bemærkningerne til telelovens § 2, nr. 5, jf. Folketingstidende 2010-11, A, L 59 som fremsat den 17. november 2010, at for at være et offentligt elektronisk kommunikationsnet skal udbuddet af nettet ske til en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester. Enhver kan derfor principielt anmode om at købe ydelserne i modsætninger til net eller tjenester, der alene tilbydes til specifikke, afgrænsede kundesegmenter, herunder eksempelvis banker, forsikringsselskaber, skoler eller andre undervisningsinstitutioner. Lukkede net eller tjenester, herunder virtuelle lukkede net eller tjenester, er således heller ikke omfattet af definitionen af offentlige elektroniske kommunikationsnet.

Det fremgår i forlængelse heraf af bemærkningerne til telelovens § 2, nr. 5, at det er uden betydning, om der er tale om et landsdækkende udbud eller udbud i en mindre del af landet, eller om der udbydes tjenester, der i praksis alene er relevante for mindre grupper af brugere. Infrastrukturselskaber, der alene udbyder for eksempel infrastrukturkapacitet til andre udbydere af elektroniske kommunikationsnet eller -tjenester, vil således også blive betragtet som udbydende offentlige elektroniske kommunikationsnet, i det omfang der er tale om udbud af elektroniske kommunikationsydelser til en ikke på forhånd afgrænset.

For vidt angår telelovens definition af offentlige elektroniske kommunikationstjenester, fremgår det af bemærkningerne til telelovens § 2, nr. 9, at for at være en offentlig elektronisk kommunikationstjeneste skal udbuddet af tjenesten ske til en ikke på forhånd afgrænset kreds af slutbrugere eller ud-

bydere af elektroniske kommunikationsnet eller -tjenester. Bemærkningerne henviser herudover til bemærkningerne til lovens § 2, nr. 5, som er anført ovenfor.

3.1.2. NIS 2-direktivet

3.1.2.1. Anvendelsesområde

NIS 2-direktivet finder ifølge direktivets artikel 2, nr. 1, anvendelse på offentlige eller private enheder af den type, der er omfattet af direktivets bilag I eller II, som udgør mellemstore virksomheder i henhold til artikel 2 i bilaget til henstilling 2003/361/EF, eller overskrider tærsklerne for mellemstore virksomheder fastsat i direktivets stk. 2, og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen. Det fremgår af direktivets bilag I, at direktivet bl.a. finder anvendelse for sektoren for digital infrastruktur, herunder bl.a. udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester.

Som hovedregel finder direktivet således kun anvendelse for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, såfremt udbyderen opfylder størrelseskravet som defineret i direktivets artikel 2, stk. 1.

Det fremgår af direktivets artikel 2, stk. 2, litra a, nr. i, at direktivet uanset enhedens størrelse, finder anvendelse på enheder af den type, der er omhandlet i bilag I eller II, hvor tjenester leveres af udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester.

Direktivets artikel 6, nr. 37, definerer en elektronisk kommunikationstjeneste som en elektronisk kommunikationstjeneste som defineret i artikel 2, nr. 4, i direktiv (EU) 2018/1972, altså EU's telekodeks. En elektronisk kommunikationstjeneste defineres i EU's telekodeks som en tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester omfatter a) internetadgangstjenester, b) interpersonelle kommunikationstjenester og c) tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

Et offentligt elektronisk kommunikationsnet defineres i direktivets artikel 6, nr. 36, som et offentligt elektronisk kommunikationsnet som defineret i ar-

tikel 2, nr. 8, i direktiv (EU) 2018/1972, altså EU's telekodeks. I EU's telekodeks defineres et offentligt elektronisk kommunikationsnet, som et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem nettermineringspunkter.

Direktivet indeholder ikke en nærmere definition af, hvem der anses for at være udbydere af offentligt tilgængelige kommunikationsnet og -tjenester.

3.1.2.2. Opdeling i væsentlige- og vigtige enheder

NIS 2-direktivet sondrer grundlæggende mellem væsentlige og vigtige enheder. De materielle regler for de to typer af enheder er som udgangspunkt ens, men sondringen har navnlig betydning for tilsynet med enhederne og de håndhævelsesforanstaltninger, der kan anvendes over for enhederne.

Væsentlige enheder defineres i NIS 2-direktivets artikel 3, stk. 1, og omfatter bl.a. udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske, der udgør mellemstore virksomheder i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, eller overskrider tærsklerne for mellemstore virksomheder i henhold til den nævnte henstilling.

I artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder afgrænses kategorien af mikrovirksomheder, små og mellemstore virksomheder (SMV'er) som virksomheder, som beskæftiger under 250 personer, og har en årlig omsætning på ikke over 50 mio. EUR eller en årlig samlet balance på ikke over 43 mio. EUR.

I kategorien for SMV'er defineres små virksomheder i henstillingen som virksomheder, som beskæftiger under 50 personer, og som har en årlig omsætning eller en samlet årlig balance på ikke over 10 mio. EUR. Tilsvarende defineres mikrovirksomheder i henstillingen som virksomheder, som beskæftiger under 10 personer og som har en årlig omsætning eller en samlet årlig balance på ikke over 2 mio. EUR.

Virksomheder falder således inden for definitionen af mellemstore virksomheder, når virksomheden har 50 ansatte eller derover eller en årlig omsætning på 10 mio. EUR eller derover og en årlig balance på 10 mio. EUR eller derover.

Det følger af NIS 2-direktivets artikel 3, stk. 2, at enheder som omhandlet i direktivets bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder, anses for at være vigtige enheder.

3.1.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivet finder som hovedregel kun anvendelse for udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som udgør mellemstore virksomheder og som leverer deres tjenester eller udfører deres aktiviteter inden for Unionen.

Det fremgår imidlertid af direktivets artikel 2, stk. 2, litra a), nr. i, at direktivet uanset størrelse bl.a. finder anvendelse på enheder, hvor tjenester leveres af udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester.

Der lægges med NIS 2-direktivet endvidere op til, at enheder, der er omfattet af direktivet med henblik på overholdelse af foranstaltninger til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, bør inddeles i to kategorier som henholdsvis væsentlige og vigtige enheder.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester alene skal anses for at være væsentlige og vigtige teleudbydere, hvis teleudbyderen med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige kommunikationstjenester som sin hovedydelse eller som en ikke-accessorisk del af virksomheden. Definitionen svarer til definitionen af 'erhvervsmæssige udbydere' i den gældende lov om sikkerhed i net og tjenester og skal fortolkes i overensstemmelse hermed.

Formålet med denne præcisering af udbyderbegrebet er at sikre, at de nye skærpede regler efter NIS 2-direktivet ikke finder anvendelse for udbydere, der ikke meningsfuldt kan siges at falde ind under kategorien væsentlige eller vigtige teleudbydere efter NIS 2-direktivet. Disse typer udbydere bør derfor i stedet falde ind under kategorien "teleudbydere" med en videreførelse af de samme krav, som gælder for disse udbydere i dag.

Henset til overskueligheden af reguleringen er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der bør foretages konsekvensrettelser

af teleudbyderbegrebet i den gældende regulering for telesektoren på Ministeriet for Samfundssikkerhed og Beredskabs område, herunder navnlig i lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

3.1.4. Den foreslåede ordning

Det foreslås, at loven finder anvendelse for samtlige udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester uanset deres størrelse.

Af hensyn til differentieringen af de forskellige krav til udbydere afhængigt af deres kritikalitet foreslås det, at loven bør skelne mellem henholdsvis teleudbydere, vigtige teleudbydere og væsentlige teleudbydere.

Det foreslås, at den eksisterende definition af en 'teleudbyder' i lov om net- og informationssikkerheds § 2, nr. 4, videreføres. Ved teleudbyder forstås således en udbyder, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre. Kategorien vil bl.a. omfatte udbydere af radiobaserede lokalnet (RLAN).

Det foreslås endvidere, at kredsen af væsentlige teleudbydere afgrænses til at omfatte udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som overskrider tærsklerne for mellemstore virksomheder, og som med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke accessorisk del af virksomheden.

Desuden vil teleudbydere i overensstemmelse med NIS 2-direktivet i særlige tilfælde uanset størrelse skulle anses som værende væsentlige teleudbydere, herunder f.eks. hvis teleudbyderen er den eneste udbyder i en medlemsstat af en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. Dette gælder dog kun, hvis teleudbyderen med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse eller som en ikke accessorisk del af virksomheden.

Det foreslås endvidere, at teleudbydere, der ikke opfylder kriterierne for at være væsentlige udbydere, bør anses som vigtige enheder, såfremt de med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet

eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke accessorisk del af virksomheden.

Det foreslås dog, at Center for Cybersikkerhed efter en konkret vurdering kan træffe afgørelse om, at en udbyder tillige skal anses som vigtig, hvis 1) enheden er den eneste udbyder i en medlemsstat af en tjenester, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) en forstyrrelse af den tjeneste, enheden leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden, 3) en forstyrrelse af den tjeneste, enheden leverer, vil kunne medføre en væsentlig systemisk risiko, navnlig for sektorer, hvor en sådan forstyrrelse kan have grænseoverskridende virkning eller 4) enheden er kritisk på grund af sin specifikke betydning på nationalt eller regionalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i medlemsstaten.

Det bemærkes, at udbyderbegrebet i nærværende lov vil adskille sig fra de gældende definitioner på telesektoren, herunder bl.a. udbyderbegrebet i lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr 955 af 17. juni 2022, som hører under Digitaliseringsministeriers område. Dette skyldes navnlig, at lov om elektroniske kommunikationsnet og -tjenester – ligesom lovgivningen på telesektoren i dag – primært opererer med to udbyderbegreber, navnlig udbydere og erhvervsmæssige udbydere.

Der henvises i øvrigt til bemærkningerne til de foreslåede §§ 3 og 4.

3.2. Foranstaltninger til styring af sikkerhedsrisici mv.

3.2.1. Gældende ret

Efter § 3, stk. 1, i lov om sikkerhed i net og tjenester fastsætter Center for Cybersikkerhed regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester. Reglerne kan omfatte krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Bestemmelsen i § 3, stk. 1, implementerer artikel 40, stk. 1, i EU's telekodeks.

Bemyndigelsen i § 3, stk. 1, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester.

3.2.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 40, stk. 1, i EU's telekodeks.

NIS 2-direktivets artikel 21 indeholder overordnet en forpligtelse til at foretage risikostyring og træffe passende tekniske, operationelle og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau hos enhederne.

Direktivet foreskriver således i artikel 21, stk. 2, at foranstaltningerne skal baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende: a) Politikker for risikoanalyse og informationssystemsikkerhed, b) håndtering af hændelser, c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring, d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere, e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder, f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici, g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse, h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering, i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver og j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

Foranstaltningerne skal være proportionale og tilvejebringe et sikkerhedsniveau i enhedens net- og informationssystemer, der står i forhold til risiciene under hensyntagen til sådanne foranstaltningers aktuelle teknologiske stade og i givet fald til relevante europæiske og internationale standarder samt gennemførelsesomkostningerne. Det er desuden forudsat i direktivet, at foranstaltningerne bør stå i et passende forhold til de væsentlige og vigtige enheders risikoeksponering, deres størrelse og til den samfundsmæssige og økonomiske indvirkning, som en hændelse ville have. Foranstaltningerne

skal desuden tage hensyn til bl.a. leverandørsikkerhed og sårbarheder i den anledning.

Det påhviler i medfør af direktivet en enhed, der finder, at den ikke overholder direktivets krav til foranstaltninger i artikel 21, stk. 2, uden unødigt ophold at træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Direktivets artikel 20 stiller desuden krav til enhedernes ledelsesorganer, herunder bl.a. om ledelsesgodkendelse af foranstaltningerne til styring af cybersikkerhedsrisici, ledelsens tilsyn med foranstaltningernes gennemførelse, samt ledelsens deltagelse i kurser. Enhederne tilskyndes desuden til at tilbyde kurser til deres ansatte.

Det følger herudover af NIS 2-direktivets artikel 24, at medlemsstaterne kan kræve, at væsentlige og vigtige enheder – for at påvise overensstemmelse med bestemte krav i direktivets artikel 21 – bruger særlige informations- og kommunikationsprodukter, -tjenester og -processer (IKT-produkter, -tjenester og -processer), der er udviklet af den væsentlige eller vigtige enhed eller indkøbt fra tredjeparter, og som er certificeret i henhold til den europæiske cybersikkerhedscertificeringsordning, der er vedtaget i henhold til Europa-Parlamentets og Rådets forordning 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed).

Europa-Kommissionen er i medfør af NIS 2-direktivets artikel 24, stk. 2, tillagt beføjelser til at vedtage delegerede retsakter, der præciserer hvilke kategorier af væsentlige og vigtige enheder, der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til forordningen om cybersikkerhed. Det er forudsat i direktivet, at der først vedtages delegerede retsakter, hvis der konstateres utilstrækkelige cybersikkerhedsniveauer.

3.2.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivets bestemmelse om foranstaltninger fastsætter et minimumsniveau for foranstaltninger.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 82 forudsættes det således, at der ved fastlæggelsen af foranstaltninger til styring af cybersikkerhedsrisici, der er tilpasset væsentlige og vigtige enheder, bør der tages behørigt hensyn til væsentlige og vigtige enheders forskellige risikoeksponering, herunder enhedens kritiske betydning, de risici, herunder samfundsmæssige risici, som den er eksponeret for, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning. Der vil således i overensstemmelse med NIS 2-direktivets forudsætninger kunne differentieres i kravene til teleudbyderne henset til forskelle i teleudbydernes risikoeksponering, deres størrelse og den potentielle samfundsmæssige og økonomiske betydning af eventuelle hændelser.

Henset til, at der ved implementeringen af NIS 2-direktivet i telesektoren skal ske en integration af den eksisterende regulering på teleområdet, er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at foranstaltningerne – som det også er tilfældet i dag – tillige bør omfatte generelle sikkerhedsrisici som led i teleudbydernes beredskab og ikke alene cybersikkerhedsrisici. Det skyldes bl.a., at der foruden foranstaltninger på cybersikkerhedsområdet er behov for andre sikkerhedsforanstaltninger, som f.eks. kan beskytte de kritiske dele af teleinfrastrukturen mod sabotage og hærværk.

Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at en nærmere konkretisering bør ske i bekendtgørelsesform med henblik på at sikre, at der løbende og smidigt kan ske en tilpasning af kravene i takt med den teknologiske udvikling og udviklingen i trusselsbilledet. Det samme gør sig gældende for så vidt angår anvendelse af særlige IKT-produkter, -tjenester og -processer med henblik på at sikre, at kravene løbende og smidigt kan tilpasses og målrettes, og således at det kan sikres, at kravene er i overensstemmelse med eventuelle delegerede retsakter, som Europa-Kommissionen måtte vedtage.

3.2.4. Den foreslåede ordning

Det foreslås, at der fastsættes en pligt for væsentlige og vigtige teleudbydere til at træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse teleudbydere anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester.

Det foreslås endvidere, at foranstaltningerne som minimum skal omfatte eller tage højde for de elementer, der fremgår af NIS 2-direktivets artikel 21, stk. 2.

Det foreslås i forlængelse heraf, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om krav til foranstaltninger efter NIS 2-direktivet og yderligere generelle foranstaltninger, som væsentlige og vigtige teleudbydere skal træffe til styring af sikkerhedsrisici. Ministeriet for Samfundssikkerhed og Beredskab vil i den forbindelse bl.a. kunne fastsætte nærmere regler om sikkerhedsforanstaltninger for så vidt angår teleudbydernes beredskab, således at indholdet af de skærpede nationale særregler herom opretholdes som hidtil. Der er med videreførelsen ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold eller anvendelsesområde og det forventes således, at ministeriet i vidt omfang vil videreføre de gældende regler i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester.

Det foreslås endvidere, at en væsentlig eller vigtig teleudbyder, der finder, at den ikke overholder krav til foranstaltninger, som følger af loven eller regler udstedt i medfør af loven, uden unødigt ophold skal træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger. Det foreslås desuden, at de foranstaltninger, der træffes, skal være godkendte af teleudbyderens ledelsesorgan, at ledelsesorganet skal føre tilsyn med foranstaltningernes gennemførelse og sikre, at foranstaltningerne har den fornødne effekt, samt at medlemmer af ledelsesorganet skal deltage i relevante kurser om styring af cybersikkerhedsrisici.

Derudover foreslås det, at Ministeriet for Samfundssikkerhed og Beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal anvende særlige informations- og kommunikationsprodukter, -tjenester og -processer (IKT-produkter, -tjenester og -processer), som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i reglerne om foranstaltninger til styring af cybersikkerhedsrisici, herunder de nærmere regler herom, som fastsættes i bekendtgørelsesform. Produkterne kan udvikles af den væsentlige eller vigtige teleudbyder eller indkøbes fra tredjeparter.

3.3. Hændelsesrapportering samt oplysnings- og underretningspligter

3.3.1. Gældende ret

Efter § 4 i lov om sikkerhed i net og tjeneste fastsætter Center for Cybersikkerhed bl.a. regler om underretningspligter for udbydere og udbydere af NUIK-tjenester.

Disse regler kan efter lovens § 4, nr. 3, omfatte krav om udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af Center for Cybersikkerhed uden unødigt ophold om sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Efter § 4, nr. 4, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed desuden fastsætte regler om udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters underretning af offentligheden ved sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester.

Det bemærkes, at lovens § 4, nr. 3 og 4, implementerer artikel 40, stk. 2, i EU's telekodeks.

Efter § 4, nr. 5, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed herudover fastsætte regler om udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters og udbydere af NUIK-tjenesters informering af deres potentielt berørte brugere om mulige beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som brugerne kan træffe i tilfælde af en særlig og betydelig trussel om en sikkerhedshændelse i udbyderens net eller tjenester. Der kan endvidere stilles krav om, at de pågældende udbydere skal informere deres brugere om selve truslen. Lovens § 4, nr. 5, implementerer artikel 40, stk. 3, i EU's telekodeks.

Bemyndigelserne i § 4, nr. 3, 4 og 5, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 1414 af 30. november 2023 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens §§ 7-13.

Underretninger om hændelser indgives i dag via selvbetjeningsløsningen Virk.dk. Når teleudbydere indgiver en hændelsesunderretning på Virk.dk, fordeles denne automatisk til Center for Cybersikkerhed. Center for Cybersikkerhed kan anvende hændelsesunderretningerne til arbejdet med at styrke cybersikkerheden samt til at vurdere, om centeret som tilsynsmyndighed skal iværksætte opfølgende skridt, herunder indlede tilsyn.

§ 4, nr. 2, og § 5, stk. 2, i lov om sikkerhed i net og tjenester indeholder derudover nationale særregler, der ikke er implementering af EU-regulering, hvorefter der kan fastsættes yderligere underretningspligter for teleudbyderne.

Efter § 4, nr. 2, i lov om sikkerhed i net og tjenester fastsætter Center for Cybersikkerhed regler om erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenesters underretning af Center for Cybersikkerhed ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf. Der kan endvidere stilles krav om, at udbyderne skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

Med lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur (telesikkerhedsloven) blev § 4, nr. 2, i lov om sikkerhed i net og tjenester suppleret med et ekstra værktøj. Efter telesikkerhedsloven kan Center for Cybersikkerhed forhindre, at en væsentlig erhvervsmæssig udbyder indgår eller opretholder en aftale, såfremt indgåelsen eller opretholdelsen af aftalen vurderes at udgøre en trussel eller en væsentlig trussel mod statens sikkerhed. Center for Cybersikkerhed har således med telesikkerhedsloven fået mulighed for at nedlægge forbud mod henholdsvis indgåelse og opretholdelse af en aftale. Standstill-perioden blev i forbindelse med loven ændret fra 10 arbejdsdage til 25 arbejdsdage.

Bemyndigelsen i § 4, nr. 2, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 1414 af 30. november 2022 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens §§ 3-6 om underretning af Center for Cybersikkerhed om aftaleforhandlinger.

Det fremgår af § 5, stk. 2, i lov om sikkerhed i net og tjenester, at for erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester kan det i regler efter § 5, stk. 1, endvidere fastsættes, at udbyderne med henblik på at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer skal 1) udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces og 2) planlægge og deltage i øvelsesaktiviteter.

Bemyndigelsen i § 5, stk. 2, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2022 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 5 om krisestyring i beredskabssituationer og i andre ekstraordinære situationer.

3.3.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 40, stk. 2 og 3, i EU's telekodeks.

Det følger af NIS 2-direktivets artikel 3, stk. 4, at væsentlige og vigtige enheder, skal indgive følgende oplysninger til de kompetente myndigheder: a) enhedens navn, b) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre, c) i givet fald den relevante sektor eller delsektor i direktivets bilag I eller II, samt d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af dette direktivs anvendelsesområde.

NIS 2-direktivets artikel 23, stk. 1, 1. pkt., fastsætter en pligt for væsentlige og vigtige enheder til uden unødigt ophold at underrette deres CSIRT eller kompetente myndighed om enhver hændelse, der har væsentlig indvirkning på leveringen af enhedens tjenester. Direktivet fastsætter i artikel 23, stk. 3, nærmere kriterier for, hvornår en hændelse anses for at være væsentlig, herunder a) hvis den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

Det følger desuden af NIS 2-direktivets præambelbetragtning nr. 101, at vurderingen bl.a. bør tage de berørte net- og informationssystemer i betragtning, navnlig deres betydning for leveringen af enhedens tjenester, alvoren og de tekniske karakteristika af en cybertrussel, eventuelle underliggende sårbarheder, der udnyttes, samt enhedens erfaring med tilsvarende hændelser. Indikatorer såsom graden af påvirkning af tjenestens funktionsdygtighed, varigheden af en hændelse eller antallet af berørte tjenestemodtagere vil kunne spille en vigtig rolle med hensyn til at fastslå, om den driftsmæssige forstyrrelse af tjenesten er alvorlig.

Den grundlæggende tilgang i NIS 2-direktivets artikel 23, stk. 1, 1. pkt., svarer i det væsentligste til tilgangen i artikel 40, stk. 2, i EU's telekodeks, og der vil således fortsat skulle ske underretning af Center for Cybersikkerhed ved en hændelse med »væsentlig indvirkning«. NIS 2-direktivet bygger imidlertid videre herpå og tilføjer yderligere elementer, der skal lægges vægt på ved fastlæggelsen af en hændelses indvirkning. Der vil som noget nyt eksempelvis skulle lægges vægt på, om hændelsen har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke fysisk skade.

NIS 2-direktivet fastsætter i artikel 23, stk. 4 – som noget nyt i forhold til EU's telekodeks – hvad de berørte enheder i forbindelse med en underretning skal fremsende til CSIRT'en eller den kompetente myndighed. Det drejer sig om en tidlig varsling, en ajourføring heraf, en foreløbig rapport, eventuelt en statusrapport og en endelig rapport. Direktivet fastsætter i den forbindelse ligeledes frister for fremsendelserne heraf.

Det påhviler efter NIS 2-direktivets artikel 23, stk. 5 – i modsætning til EU's telekodeks – CSIRT'en eller den kompetente myndighed at give den underrettende enhed en tilbagemelding, herunder – såfremt det ønskes – operativ rådgivning og vejledning om mulige foranstaltninger, som enheden kan træffe for at håndtere den væsentlige hændelse, og supplerende teknisk bistand.

Efter NIS 2-direktivets artikel 23, stk. 1, 2. pkt., skal væsentlige og vigtige enheder, hvor det er relevant, uden unødigt ophold underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt. NIS 2-direktivet medfører således – sammenholdt med artikel 40, stk. 2 og 3, i EU's telekodeks – en yderligere underretningspligt for teleudbyderne over for modtagerne af deres tjenester.

Det følger endvidere af NIS 2-direktivets artikel 23, stk. 2, at væsentlige og vigtige enheder uden unødigt ophold skal meddele modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, eventuelle foranstaltninger og modforholdsregler, som disse kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige trussel.

NIS 2-direktivet ændrer således ikke ved, at teleudbydernes modtagere af deres tjenester skal have meddelelse om bl.a. eventuelle foranstaltninger, som disse kan træffe, men NIS 2-direktivet anvender begrebet »væsentlig cybertrussel« som kriterium for meddelelsen i modsætning til det hidtidige begreb i EU's telekodeks »særlig og betydelig trussel«. Samtidig tilføjes der – som noget nyt – et krav om, at meddelelsen skal ske uden unødigt ophold. NIS 2-direktivet viderefører i øvrigt forpligtelsen fra artikel 40, stk. 3, i EU's telekodeks om informering af modtagerne – hvor det er relevant – om selve truslen, dog med det ændrede trusselsbegreb, som er beskrevet ovenfor.

Herudover foreskriver NIS 2-direktivets artikel 23, stk. 7, at CSIRT'en eller den kompetente myndighed efter høring af den berørte enhed kan informere

offentligheden om en væsentlig hændelse eller kræve, at enheden gør det, såfremt dette er nødvendigt eller i øvrigt i offentlighedens interesse. Dette svarer – med den justering, at der desuden kan ske offentliggørelse, såfremt »det er nødvendigt« – således til forpligtelsen i artikel 40, stk. 2, i EU's telekodeks. Det vil – som hidtil – skulle sikres, at offentligheden informeres på en ansvarlig måde, som ikke kompromitterer kommercielt fortrolige oplysninger.

3.3.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivet indeholder forskellige oplysnings- og underretningspligter for væsentlige og vigtige udbydere.

Samtidig indeholder den gældende lov om sikkerhed i net og tjenester regler om underretningsforpligtelser for udbydere, der er omfattet af loven.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets krav om underretningspligter vedrørende væsentlige hændelser bør implementeres direktivnært, således at direktivets krav om hændelsesindberetninger samt oplysnings- og underretningspligter overføres direkte til loven. Henset til kriteriernes kvalitative og skønsprægede karakter vurderes det endvidere, at der i bekendtgørelsesform bør kunne fastsættes nærmere regler om, hvornår en hændelse anses for at være væsentlig inden for telesektoren, herunder ved fastsættelse af kvantitative kriterier vedrørende eksempelvis hændelsens varighed eller skadens omfang.

Det er samtidig Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at direktivets krav bør bygge ovenpå de krav, der i forvejen gælder for hændelsesindberetning mv. på teleområdet. Det indebærer bl.a., at begrebet "væsentlig sikkerhedstrussel" vil skulle anvendes som kriterium for meddelelsen, der vil skulle ske til Center for Cybersikkerhed uden unødigt ophold.

Det er på denne baggrund Ministeriet for Samfundssikkerheds opfattelse, at de gældende oplysnings- og underretningspligter, herunder vedrørende beredskabssituationer og andre ekstraordinære situationer i lov om sikkerhed i net og tjenester, bør videreføres. Der forudsættes ikke en ændring af den eksisterende praksis.

3.3.4. Den foreslåede ordning

Det foreslås, at væsentlige og vigtige teleudbydere skal registrere sig hos Center for Cybersikkerhed og i den forbindelse oplyse a) enhedens navn, b) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre, c) i givet fald den relevante sektor eller delsektor i direktivets bilag I eller II, samt d) i givet fald en liste over de medlemsstater, hvor enheden leverer tjenester, der er omfattet af dette direktivs anvendelsesområde. Det foreslås, at de nævnte oplysninger skal indgives til Center for Cybersikkerhed senest den 1. oktober 2025. En væsentlig eller vigtig teleudbyder, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne senest to uger efter, at teleudbyderen omfattes af loven.

Det foreslås, at alle teleudbydere uden unødigt ophold skal underrette Center for Cybersikkerhed og CSIRT'en om enhver væsentlig hændelse, og at kravene til fremgangsmåden og fristerne for underretningerne indholdsmæssigt svarer til NIS 2-direktivets.

Det foreslås endvidere, at ministeriet for samfundssikkerhed og beredskab kan fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig. Henset til kriteriernes generelle udformning finder Ministeriet for Samfundssikkerhed det således hensigtsmæssigt, at der gives mulighed for, at Center for Cybersikkerhed vil kunne fastsætte nærmere regler om væsentlige hændelser, herunder f.eks. af hensyn til særligt kritiske systemer.

Det foreslås desuden, at Center for Cybersikkerhed bemyndiges til at fastsætte nærmere regler om regler om oplysnings- og underretningspligter for væsentlige- og vigtige teleudbydere, herunder krav om 1) afgivelse af oplysninger om væsentlige dele teleudbyderens net eller tjenester eller driften heraf samt 2) krav om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, herunder regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

Det foreslås herudover, at væsentlige og vigtige teleudbydere uden unødigt ophold skal underrette modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt. Teleudbyderne skal endvidere uden unødigt ophold oplyse modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan

træffe som reaktion på den pågældende trussel, og eventuelt også informere om selve truslen.

Endvidere foreslås det, at Center for Cybersikkerhed under visse betingelser kan informere offentligheden om den væsentlige hændelse eller kræve, at teleudbyderen gør det.

I tilfælde, hvor hændelsen berører flere samfundsvigtige sektorer, herunder eventuelt også sektorer uden for lovens anvendelsesområde, eller hvor der er tale om en hændelse i en anden EU-medlemsstat, vil det dog være CSIRT'en, som vil kunne informere offentligheden om den væsentlige hændelse.

Forud for orientering af offentligheden foreslås det, at Center for Cybersikkerhed hører den væsentlige eller vigtige teleudbyder, der har underrettet om hændelsen, herunder med henblik på vurdering af, hvilke oplysninger, der må betragtes som fortrolige. Center for Cybersikkerhed skal desuden ved overvejelse om orientering af offentligheden om en hændelse sikre, at de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentligt ansattes tavshedspligt, iagttages. Dette omfatter bl.a. hensynet til enkeltpersoners private forhold, forretningshemmeligheder samt hensynet til forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Som nærmere beskrevet under afsnit 3.3.1 indeholder lov om sikkerhed i net og tjenester i § 4, nr. 2, og § 5, stk. 2, yderligere underretningspligter for teleudbyderne, der går videre end NIS 2-direktivet. Med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren finder Ministeriet for Samfundssikkerhed og Beredskab, at indholdet af § 4, nr. 2, og § 5, stk. 2, i lov om sikkerhed i net og tjenester bør videreføres. Ministeriet for Samfundssikkerhed og Beredskab vurderer, at dette er væsentligt henset til det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet.

3.4. Beredskabs- og andre ekstraordinære situationer

3.4.1. Gældende ret

Efter § 5, stk. 1, i lov om sikkerhed i net og tjenester fastsætter Center for Cybersikkerhed regler om, at udbydere skal foretage nødvendig planlægning og træffe nødvendige foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Det fremgår af § 5, stk. 2, i lov om sikkerhed i net og tjenester, at for erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester kan det i regler efter stk. 1, endvidere fastsættes, at udbyderne med henblik på at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer skal 1) udarbejde beredskabsplaner baseret på en dokumenteret og ledelsesforankret risikostyringsproces og 2) planlægge og deltage i øvelsesaktiviteter.

Bemyndigelserne i § 5, stk. 1 og 2, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 5 om krisestyring i beredskabssituationer og i andre ekstraordinære situationer.

Det følger af § 5, stk. 3, i lov om sikkerhed i net og tjenester, at Center for Cybersikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Center for Cybersikkerhed kan endvidere fastsætte regler om, at erhvervsmæssige udbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Bemyndigelsen er udmøntet i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Det følger endvidere af § 5 a i lov om sikkerhed i net og tjenester, at Center for Cybersikkerhed kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne. Bemyndigelsen er ikke udmøntet.

3.4.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at bestemmelserne i kapitel 5 om elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer i lov om sikkerhed i net og tjenester videreføres med nærværende lov.

Videreførelsen skal navnlig ses i lyset af, at elektronisk kommunikation i stigende grad er en forudsætning for opretholdelse af samfundets funktioner, hvilket stiller krav til en robust teleinfrastruktur. I beredskabssituationer og

i andre ekstraordinære situationer, hvor samfundet rammes af naturskabte eller menneskeskabte ulykker eller katastrofer, vil den elektroniske kommunikation og dermed en fungerende teleinfrastruktur være nødvendig for, at samfundsvigtige funktioner kan opretholdes.

Ikke mindst de forskellige aktører, der indgår i samfundets beredskab, kan i beredskabssituationer og i andre ekstraordinære situationer have behov for elektronisk kommunikation for at udføre en række af deres opgaver, ligesom elektronisk kommunikation er en forudsætning for, at de kan koordinere deres indsats.

Det er derfor nødvendigt med et beredskab på teleområdet, som sikrer, at den elektroniske kommunikation i videst muligt omfang opretholdes i beredskabssituationer og i andre ekstraordinære situationer, og som tilgodeser beredskabsaktørernes behov for elektronisk kommunikation.

3.4.3. Den foreslåede ordning

Det foreslås, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester. Det foreslås endvidere, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige- og vigtige teleudbydere skal underrette Center for Cybersikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder, herunder regler om, hvordan underretningen skal foretages.

Det foreslås desuden, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede ordning vil ikke medføre en ændring af gældende ret, idet bestemmelserne i kapitel 5 i lov om sikkerhed i net og tjenester videreføres.

3.6. Aktindsigt i oplysninger og underretninger

3.6.1. Gældende ret

Lov om sikkerhed i net og tjenester fastsætter i lovens kapitel 5 regler om aktindsigt i underretninger mv.

Det følger således af lovens § 7, at det i regler udstedt i medfør af lovens § 4, kan fastsættes, at underretninger og afgivelse af oplysninger efter lovens § 4, nr. 1-3, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Dette indebærer således, at underretninger til Center for Cybersikkerhed om 1) væsentlige dele af teleudbyderens net eller tjenester eller driften heraf, 2) indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf og sikkerhedshændelser, der har haft væsentlig indvirkning på driften af net eller tjenester, kan undtages fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Bemyndigelsen til at fastsætte regler om aktindsigt er i dag udmøntet i bekendtgørelse nr. 258 af 22. februar 2021 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 14.

Det følger endvidere af lovens § 8, stk. 2, at underretninger fra myndigheder og virksomheder vedrørende hændelser, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale servicer, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Mulighederne for undtagelse af retten til aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven, skal navnlig ses i lyset af, at

3.6.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de eksisterende regler om aktindsigt i underretninger mv. bør videreføres.

Bemyndigelsen til at fastsætte regler om aktindsigt er i dag udmøntet i bekendtgørelse nr. 258 af 22. februar 2021 om oplysnings- og underretnings-

pligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 14.

De oplysninger, som Center for Cybersikkerhed som led i påbudsordningen modtager fra væsentlige og vigtige teleudbydere vedrørende væsentlige dele af udbyderens net og tjenester eller varetagelsen af driften heraf, vil ofte indeholde oplysninger om fejl eller sårbarheder i net eller tjenester, som kan misbruges af potentielle angribere, hvis de kommer til uvedkommendes kendskab. Det vurderes derfor, at oplysningerne i deres helhed bør undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven, således at aktindsigtsanmodninger ikke – som det ellers ville være tilfældet – behandles efter principperne i offentlighedsloven. Undtagelsen kan omfatte underretningssagen som helhed.

Undtagelsen fra aktindsigt vil bør efter ministeriets opfattelse også gælde i de tilfælde, hvor oplysningerne videregives til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse bør der endvidere ikke være adgang til aktindsigt i de udkast til aftaler, som væsentlige og vigtige teleudbydere indsender til Center for Cybersikkerhed i medfør af regler fastsat efter denne lov. Aftalerne vil således ofte indeholde en lang række oplysninger om udbydernes net og tjenester samt aftaleforhold, som dels er kommercielt fortrolige, dels kan misbruges af potentielle angribere.

Undtagelsen fra aktindsigt omfatter ikke teleudbydernes adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

3.6.3. Den foreslåede ordning

Det foreslås, at teleudbyderes underretninger til Center for Cybersikkerhed og CSIRT'en vedrørende væsentlige hændelser, hændelser, der ikke er omfattet af lovens § 9, nærvedhændelser og cybertrusler,

Det foreslås derudover, at det i regler udstedt i medfør af bemyndigelsesbestemmelserne i lovens § 9, stk. 5, om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf. og § 14, stk. 3, om underretningspligter ved

aktivering af beredskab eller beredskabssituationer kan fastsættes, at underretning og afgivelse af oplysninger i de nærmere fastsatte regler.

Den foreslåede ordning har til formål at implementere NIS 2-direktivet og videreføre de eksisterende regler om aktindsigt i lov om sikkerhed i net og tjenester.

Videreførelsen skal navnlig ses i lyset af, at en velfungerende underretningsordning forudsætter, at der ikke er risiko for, at de ofte særligt kommercielt følsomme oplysninger, som vil blive modtaget fra teleudbyderne, kan tilgå teleudbydernes konkurrenter eller potentielle angribere.

Underretning af Center for Cybersikkerhed skaber de bedst mulige forudsætninger for, at centeret kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand på den danske del af internettet. Underretningerne sætter således Center for Cybersikkerhed i stand til at varsle hurtigere om trusler og styrke grundlaget for centerets rådgivning om risici og passende sikkerhedstiltag.

Oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor en virksomhed har mistet data, kan imidlertid i høj grad skade virksomhedens omdømme, og risikoen for, at oplysningerne via aktindsigt bliver offentligt tilgængelige, kan i praksis afholde mange virksomheder fra at underrette Center for Cybersikkerhed om et sådant hackerangreb. Derfor bør også disse særlige underretninger være undtaget fra aktindsigt.

Der henvises i øvrigt til bemærkninger til de foreslåede §§ 15-16.

3.5. Sikkerhedsgodkendelser

3.5.1. Gældende ret

3.5.1.1. Sikkerhedsgodkendelser efter sikkerhedscirkulæret

Cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret) indeholder de almindelige regler for bl.a. sikkerhedsundersøgelser og sikkerhedsgodkendelser af ansatte i offentlige myndigheder og ansatte i private firmaer, der arbejder for en offentlig myndighed. Sikkerhedsgodkendelsen har kun gyldighed for den sikkerhedsgodkendte persons arbejde for den pågældende myndighed. Det fremgår af

stk. 3, at Politiets Efterretningstjeneste foretager en sikkerhedsundersøgelse til brug for den offentlige myndigheds afgørelse om sikkerhedsgodkendelse af ansatte.

Afgørelse om sikkerhedsgodkendelse træffes i medfør af sikkerhedscirkulærets § 14 på grundlag af en konkret vurdering af alle de oplysninger, der foreligger om personen. Der lægges herved navnlig vægt på, om den pågældende har udvist ubestridt loyalitet, og om den pågældende har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed i forbindelse med håndtering af klassificerede informationer.

3.5.1.2. Sikkerhedsgodkendelser efter lov om sikkerhed i net og tjenester

Lov om sikkerhed i net og tjenester indeholder i lovens kapitel 4 regler om sikkerhedsgodkendelser. Det følger således af lovens § 6, stk. 1, at en udbyder skal indstille medarbejdere og repræsentanter for udbyderen til sikkerhedsgodkendelse hos sikkerhedsmyndigheden, når de pågældende som led i deres konkrete opgaveløsning for udbyderen skal behandle klassificerede informationer eller andre informationer, der er særligt beskyttelsesværdige i relation til sikkerhed i net og tjenester eller beredskab.

Det fremgår derudover at bestemmelsens stk. 2, at erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet skal sikre, at medarbejdere eller repræsentanter for udbyderen, der varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af lovens § 5, stk. 2, i fornødent omfang sikkerhedsgodkendes efter stk. 1.

Det følger af bestemmelsens stk. 3, at udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, skal sikre overholdelse af sikkerhedsmyndighedens anvisninger om behandling af klassificerede informationer.

Det fremgår derudover af bestemmelsens stk. 4, at udbydere, hvis medarbejdere eller repræsentanter sikkerhedsgodkendes efter stk. 1, uden ugrundet ophold skal underrette sikkerhedsmyndigheden, når sikkerhedsgodkendte personer ikke længere varetager de opgaver for udbyderen, som lå til grund for sikkerhedsgodkendelsen.

Det fremgår endvidere af bestemmelsens stk. 5, at sikkerhedsmyndigheden kan tilbagekalde en sikkerhedsgodkendelse, når betingelserne for sikkerhedsgodkendelse ikke længere er til stede.

Endelig giver bestemmelsens stk. 6 Center for Cybersikkerhed hjemmel til at fastsætte regler om sikkerhedsgodkendelse af udbyderes medarbejdere eller repræsentanter for udbydere, der har adgang til udstyr eller systemer, som benyttes i forbindelse med indgreb i meddelelseshemmeligheden.

3.5.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de gældende regler for sikkerhedsgodkendelser i § 6 i lov om sikkerhed i net og tjenester i et vist omfang bør videreføres, dog således, at loven alene fastsætter de overordnede rammer for den personkreds, der skal være omfattet af kravet om sikkerhedsgodkendelse, mens de nærmere regler herom vil blive fastsat i en bekendtgørelse. Dette vil skabe fleksibilitet i regelsættet i forhold til nye udviklinger, trusselsvurderinger mv., der kan have betydning for vurderingen af, hvilken personkreds der bør sikkerhedsgodkendes.

Videreførelsen skal ses i lyset af det aktuelle trusselsbillede, herunder navnlig behovet for at vurdere medarbejdere i væsentlige og vigtige enheders pålidelighed og imødegå risikoen for bl.a. spionage og sabotage.

3.5.3. Den foreslåede ordning

Det foreslås, at medarbejdere eller repræsentanter for en væsentlig eller vigtig teleudbyder, når 1) det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage, eller 2) den pågældende varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 14, stk. 3.

Endvidere foreslås det, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler for sikkerhedsgodkendelser, herunder regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgning samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser. Det foreslås, at reglerne skal fastsættes efter forhandling med justitsministeren.

3.6. Tilsyn

3.6.1. Gældende ret

Center for Cybersikkerhed varetager Ministeriet for Samfundssikkerhed og Beredskabs myndighedsopgaver i relation til informationssikkerhed og beredskab for telesektoren. Der er på den baggrund i § 9, stk. 1, i lov om sikkerhed i net og tjenester fastsat en forpligtelse for Center for Cybersikkerhed til at føre tilsyn med overholdelsen af loven og regler, der er udstedt af medfør i loven.

Efter § 9, stk. 2, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed som led i sit tilsyn kræve, at udbydere og udbydere af NUIK-tjenester fremlægger alle de oplysninger og det materiale om sikkerhed i net og tjenester, beredskab og sikkerhedsgodkendelse, der er nødvendige for centerets tilsynsvirksomhed, herunder til afgørelse af, om et forhold falder ind under denne lov eller regler, der er udstedt i medfør af loven.

Bestemmelsen suppleres af lovens § 4, hvorefter Center for Cybersikkerhed mere generelt med henblik på at sikre informationssikkerheden i net og tjenester kan fastsætte regler om oplysnings- og underretningspligter for udbydere af offentligt tilgængelige net og tjenester.

Efter § 9, stk. 3, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed stille krav om, hvordan og i hvilken form oplysninger og materiale efter § 9, stk. 2, skal afgives.

Lovens § 9, stk. 2 og 3, i lov om sikkerhed i net og tjenester er delvis implementering af artikel 20, stk. 1, i EU's telekodeks.

I forbindelse med tilsynet med udbydernes overholdelse af reglerne kan Center for Cybersikkerhed efter § 9, stk. 5, i lov om sikkerhed i net og tjenester desuden stille krav om, at udbydere og udbydere af NUIK-tjenester skal foranstalte en uafhængig sikkerhedsrevision og stille resultaterne heraf til rådighed for centeret.

Lovens § 9, stk. 5, i lov om sikkerhed i net og tjenester er delvis implementering af artikel 41, stk. 2, litra b, i EU's telekodeks.

§ 9, stk. 4, 6 og 7, i lov om sikkerhed i net og tjenester indeholder derudover nationale særregler, der ikke implementerer EU-regulering, hvorefter Center for Cybersikkerhed er tillagt yderligere tilsynsbeføjelser overfor teleudbyderne.

Efter § 9, stk. 4, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed afkræve udbydere skriftlige udtalelser og redegørelser om faktiske forhold af betydning for centerets tilsynsvirksomhed.

Efter § 9, stk. 6, i lov om sikkerhed i net og tjenester har Center for Cybersikkerhed, såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til udbyderes forretningslokaler med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Efter § 9, stk. 7, i lov om sikkerhed i net og tjenester, har Center for Cybersikkerhed endvidere, såfremt det er nødvendigt af hensyn til sikkerheden i net og tjenester, efter et skriftligt varsel på mindst 7 arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos udbyderes samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, i relation til outsourcet aktivitet. Center for Cybersikkerhed kan ikke i forbindelse med adgang til forretningslokaler tilgå kommunikation til, fra eller mellem udbyderens kunder.

Ved tilsynsbesøg hos samarbejdspartnere, leverandører eller underleverandører gælder de samme betingelser som efter lovens § 9, stk. 6.

3.6.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 41, stk. 2, litra b, i EU's telekodeks.

NIS 2-direktivets artikel 31, stk. 1, fastsætter herefter en pligt for medlemsstaterne til at sikre, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at direktivet overholdes. I medfør af direktivets artikel 31, stk. 2, kan medlemsstaterne dog tillade, at de kompetente myndigheder prioriterer deres tilsynsopgaver baseret på en risikobaseret tilgang. Efter direktivets artikel 32, stk. 1, og 33, stk. 1, skal bl.a. tilsynsforanstaltningerne være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Efter NIS 2-direktivets præambelbetragtning nr. 95 kan medlemsstaterne tildele de kompetente myndigheder efter EU's telekodeks samme rolle efter NIS 2-direktivet med henblik på at sikre videreførelsen af den nuværende praksis og for at bygge videre på den viden og erfaring, der er opnået som et resultat af gennemførelsen af EU's telekodeks. Center for Cybersikkerhed vil således fortsat varetage myndighedsopgaverne på området.

Sondringen mellem væsentlige og vigtige enheder i NIS 2-direktivet ses bl.a. at være relevant i relation til tilsyn. Det er i NIS 2-direktivet således forudsat, at tilsynet med henholdsvis væsentlige og vigtige enheder kan differentieres med henblik på at sikre en rimelig balance mellem forpligtelser for disse enheder og for de kompetente myndigheder. Direktivet forudsætter, at væsentlige enheder underlægges et omfattende forudgående og efterfølgende tilsyn, mens vigtige enheder derimod underlægges et lettere og rent reaktivt tilsyn, hvor de ikke er forpligtet til systematisk at dokumentere overholdelsen af foranstaltninger til styring af cybersikkerhedsrisici, og hvor de kompetente myndigheder ikke har en generel forpligtelse til at føre løbende tilsyn med disse enheder. Det reaktive tilsyn med vigtige enheder vil eksempelvis kunne aktiveres, hvis der modtages oplysninger fra andre myndigheder, enheder, borgere eller medier, eller hvis myndigheden i forbindelse med udførelsen af dennes opgaver i øvrigt kommer i besiddelse af oplysninger, der peger på mulige overtrædelser af reguleringen, jf. NIS 2-direktivets præambelbetragtning nr. 122.

NIS 2-direktivet oplister i artikel 32, stk. 2 og 3, og 33, stk. 2 og 3, en række tilsynsbeføjelser, som de kompetente myndigheder som minimum skal kunne anvende ved deres tilsyn med henholdsvis væsentlige og vigtige enheder. Der er navnlig tale om, at de kompetente myndigheder skal kunne føre kontrol på stedet hos enhederne, foretage målrettede sikkerhedsaudits og sikkerhedsscanninger samt kræve at få udleveret oplysninger og dokumentation, der er nødvendige for udførelsen af myndighedernes tilsynsopgaver.

Oplistningerne af tilsynsbeføjelser for henholdsvis væsentlige og vigtige enheder er i vidt omfang identiske, idet NIS 2-direktivets forudsætning om en differentieret tilgang til tilsynet med væsentlige og vigtige enheder dog afspejler sig i visse forskelle i de beføjelser, der som minimum skal kunne anvendes. Direktivet foreskriver eksempelvis, at myndighederne skal kunne foretage stikprøvekontrol med væsentlige enheder, hvilket ikke gør sig gældende for vigtige enheder. De målrettede sikkerhedsaudits, som skal kunne pålægges både væsentlige og vigtige enheder, skal efter direktivet kun for

de væsentlige enheder kunne være regelmæssige. Herudover foreskriver direktivet, at væsentlige enheder under visse omstændigheder skal kunne pålægges sikkerhedsaudits ad hoc, hvilket ikke er tilfældet for vigtige enheder.

3.6.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Den grundlæggende tilgang i NIS 2-direktivet og EU's telekodeks i forhold til tilsyn svarer i det væsentligste til hinanden. Som beskrevet ovenfor giver EU's telekodeks i artikel 20 og artikel 41, stk. 2, litra b, medlemsstaterne beføjelse til – som led i deres tilsyn – at kræve, at der fremlægges oplysninger og materiale, ligesom der kan kræves en uafhængig sikkerhedsrevision. NIS 2-direktivet bygger imidlertid videre herpå og indeholder en minimumsliste over tilsynsbeføjelser, der foruden de beføjelser, der følger af EU's telekodeks, navnlig som noget nyt omfatter kontrol på stedet – og stikprøvekontrol for de væsentlige teleudbydere – samt sikkerhedsscanninger.

Hertil kommer, at § 9, stk. 4, 6 og 7, i lov om sikkerhed i net og tjenester indeholder yderligere tilsynsbeføjelser for Center for Cybersikkerhed, der går videre end de tilsynsbeføjelser, der følger af direktivet.

Med henblik på at sikre et effektivt tilsyn med teleudbydernes efterlevelse af loven og de regler, der er udstedt i medfør af loven, finder Ministeriet for Samfundssikkerhed og Beredskab, at indholdet af lovens § 9, stk. 4, 6 og 7, bør videreføres.

Videreførelsen skal navnlig ses i lyset af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet.

3.6.4. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed – som hidtil – inden for telesektoren fører tilsyn med teleudbyderes efterlevelse af loven og de regler, der udstedes i medfør af loven.

Det foreslås i forlængelse heraf, at Center for Cybersikkerhed tillægges tilsynsbeføjelser, der indholdsmæssigt svarer til det, som NIS 2-direktivet foreskriver, herunder med de forudsatte forskelle i tilgangen til væsentlige og vigtige teleudbydere. I overensstemmelse med forudsætningerne i direktivet foreslås det derfor, at Center for Cybersikkerhed ved tilrettelæggelsen af sit

tilsyn anlægger en risikobaseret tilgang, hvor der kan anvendes forskellige tilgange til tilsyn med henholdsvis væsentlige og vigtige teleudbydere.

Endelig foreslås det, at indholdet af de skærpede nationale særregler omkring Center for Cybersikkerheds beføjelser til at kræve skriftlige udtalelser og redegørelser samt adgang til teleudbyderes samt deres samarbejdspartneres, leverandørers eller underleverandørers forretningslokaler opretholdes som hidtil. Der er med videreførelsen således ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold. Det indebærer bl.a., at udbydere af nummeruafhængige interpersonelle kommunikationstjenester – som hidtil – ikke foreslås at være omfattet af disse bestemmelsers indhold.

3.7. Håndhævelse

3.7.1. Gældende ret

Center for Cybersikkerhed kan som led i varetagelsen af myndighedsopgaver i relation til informationssikkerhed og beredskab for telesektoren iværksætte tiltag med henblik på at sikre sikkerheden i net og tjenester, som kan vise sig nødvendige på baggrund af eksempelvis tilsyn.

Efter § 3, stk. 3, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester og udbydere af NUIK-tjenester at træffe konkrete foranstaltninger, der er nødvendige for at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme, når en betydelig trussel er identificeret. Centret fastsætter nærmere regler herom.

Bemyndigelsen i § 3, stk. 3, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 4 vedrørende påbud om konkrete informationssikkerhedsforanstaltninger.

Bestemmelsen – og de dele af bekendtgørelsen, der er udstedt i medfør heraf – implementerer artikel 41, stk. 1, i EU's telekodeks.

§ 3, stk. 2 og 4, samt § 5, stk. 4, i lov om sikkerhed i net og tjenester indeholder derudover nationale særregler, der ikke er implementering af EU-regulering, hvorefter Center for Cybersikkerhed kan udstede yderligere påbud til teleudbyderne.

Efter § 3, stk. 2, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed påbyde udbydere af offentligt tilgængelige elektroniske kommu-

nikationsnet og -tjenester at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og tjenester i deres risikostyringsprocesser efter lovens § 3, stk. 1.

Efter § 3, stk. 4, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed, såfremt det er af væsentlig samfundsmæssig betydning, påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net og tjenester. Centeret fastsætter nærmere regler herom.

Bemyndigelsen i § 3, stk. 4, i lov om sikkerhed i net og tjenester er udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 4 vedrørende påbud om konkrete informationssikkerhedsforanstaltninger.

Efter § 5, stk. 4, i lov om sikkerhed i net og tjenester kan Center for Cybersikkerhed i beredskabssituationer og i andre ekstraordinære situationer påbyde erhvervsmæssige udbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.

3.7.2. NIS 2-direktivet

Med artikel 43 i NIS 2-direktivet ophæves bl.a. artikel 41, stk. 1, i EU's telekodeks.

Der er i NIS 2-direktivets artikel 31-33 fastsat bestemmelser om tilsyn og håndhævelse. Medlemsstaterne forpligtes i disse bestemmelser til at sikre, at deres kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger til at sikre, at direktivet overholdes.

Foranstaltningerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

NIS 2-direktivets sondring mellem væsentlige og vigtige enheder er navnlig relevant i relation til tilsyn og håndhævelse. Direktivet oplister i henholdsvis artikel 32, stk. 4, og artikel 33, stk. 4, de håndhævelsesforanstaltninger, der som minimum skal kunne anvendes over for henholdsvis væsentlige og vigtige enheder, herunder for så vidt angår vigtige teleudbydere a) udstede advarsler om de pågældende enheders overtrædelser af direktivet, b) udstede

bindende instrukser eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af direktivet, c) pålægge de pågældende enheder at ophøre med at udvise adfærd, der overtræder dette direktiv, og afstå fra at gentage denne adfærd, d) pålægge de pågældende enheder, på en nærmere angivet måde og inden for en nærmere angivet frist at sikre, at deres foranstaltninger til styring af cybersikkerhedsrisici overholder artikel 21, eller at efterleve underretningsforpligtelserne i artikel 23, e) pålægge de pågældende enheder at underrette de fysiske eller juridiske personer med hensyn til hvilke de leverer tjenester eller udfører aktiviteter, som potentielt er berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel, f) pålægge de pågældende enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsaudit, inden for en rimelig frist og g) pålægge de pågældende enheder at offentliggøre aspekter af overtrædelser af dette direktiv på en nærmere angivet måde, og h) pålægge eller anmode de relevante organer eller domstole om i overensstemmelse med national ret at pålægge en administrativ bøde i henhold til artikel 34 ud over enhver af de foranstaltninger, der er omhandlet i artikel 33, stk. 4, litra a)-g).

Overfor væsentlige enheder kan kompetente myndighed dog efter direktivets artikel 32, stk. 4, litra g, som noget særligt kan udpege en monitoreringsansvarlig med veldefinerede opgaver til i en nærmere fastsat periode at føre tilsyn med de pågældende enheders overholdelse af kravene til foranstaltninger til styring af cybersikkerhedsrisici og underretningsforpligtelser.

Den grundlæggende tilgang i NIS 2-direktivet og EU's telekodeks om, at teleudbyderne skal kunne pålægges håndhævelsesforanstaltninger svarer i vidt omfang til hinanden. Artikel 41, stk. 1, i EU's telekodeks giver imidlertid alene medlemsstaterne beføjelse til at pålægge teleudbydere at træffe foranstaltninger med henblik på at afhjælpe en sikkerhedshændelse eller hindre en sådan i at forekomme. Med den minimumsliste, som NIS 2-direktivet indeholder, tillægges medlemsstaterne dermed en række nye håndhævelsesforanstaltninger. Derudover er det med NIS 2-direktivet imidlertid alene væsentlige enheder, der kan pålægges at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

NIS 2-direktivet foreskriver nærmere, hvilke hensyn der skal indgå i en afgørelse om at iværksætte håndhævelsesforanstaltninger. I direktivets artikel 32, stk. 7, er følgende hensyn oplistet: 1) Overtrædelsens grovhed og vig-

tigheden 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 kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i artiklerne 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 der ved overtrædelsen er handlet 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 for overtrædelsen, samarbejder med de kompetente myndigheder

2.7.2.1. Særligt om midlertidige suspensioner

For så vidt angår væsentlige enheder indeholder direktivet i artikel 32, stk. 5, et særligt virkemiddel i tilfælde, hvor en række mindre indgribende midler har vist sig ikke at være tilstrækkelige. I så fald skal de kompetente myndigheder – efter udløbet af en fastsat frist for at afhjælpe manglerne eller opfylde myndighedens krav – kunne a) midlertidigt 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) 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 følger endvidere af direktivets artikel 32, stk. 5, 2. led, at de midlertidige suspensioner eller forbud alene må anvendes, indtil den pågældende enhed træffer de nødvendige tiltag til at afhjælpe manglerne eller opfylde den kompetente myndigheds krav, som gav anledning til, at suspensionen eller forbuddet blev anvendt.

Efter direktivets artikel 32, stk. 5, 3. led, kan sådanne midlertidige suspensioner eller midlertidige forbud mod, at fysiske personer må udøve ledelsesfunktioner, ikke anvendes på offentlige forvaltningsenheder, der er omfattet af NIS 2-direktivet.

3.7.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

NIS 2-direktivet sonderer mellem håndhævelsesforanstaltninger for henholdsvis væsentlige og vigtige teleudbydere.

Derudover indeholder § 3, stk. 2 og 4, samt § 5, stk. 4, i lov om sikkerhed i net og tjenester yderligere håndhævelsesbeføjelser for Center for Cybersikkerhed, der går videre end de håndhævelsesbeføjelser, som følger af direktivet. Det drejer sig f.eks. om, at Center for Cybersikkerhed har mulighed for at påbyde, at udbyderen skal inddrage nærmere angivne områder af dens virksomhed og nærmere angivne trusler mod sikkerheden i net og tjenester i deres risikostyringsprocesser eller muligheden for, såfremt det er af væsentlig samfundsmæssig betydning, at påbyde udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net og tjenester. Ministeriet vurderer, at Center for Cybersikkerhed fortsat har brug for disse yderligere håndhævelsesforanstaltninger som supplement til de håndhævelsesforanstaltninger, der fremgår af NIS 2-direktivet.

Med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren finder Ministeriet for Samfundssikkerhed og Beredskab, at indholdet af lovens § 3, stk. 2 og 4, samt § 5, stk. 4, bør videreføres. Ministeriet for Samfundssikkerhed og Beredskabs vurderer, at dette er væsentligt henset til det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at det er mest hensigtsmæssigt, at en afgørelse om midlertidigt at suspendere en certificering eller godkendelse eller midlertidigt at forbyde en fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos enheden at udøve ledelsesfunktioner i den væsentlige enhed i første omgang træffes af Center for Cybersikkerhed, der vil kunne belyse og begrunde, hvorfor indgrebet vurderes påkrævet.

3.7.4. Den foreslåede ordning

Det foreslås, at Center for Cybersikkerhed tillægges håndhævelsesforanstaltninger, der indholdsmæssigt svarer til det, som NIS 2-direktivet foreskriver, herunder med de forudsatte forskelle i tilgangen til væsentlige og vigtige teleudbydere, dog således, at indholdet af de skærpede nationale særregler omkring Center for Cybersikkerheds beføjelser til at påbyde teleudbydere at inddrage, træffe og iværksætte nærmere foranstaltninger opretholdes som hidtil. Der er med videreførelsen således ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold.

Det foreslås i forlængelse heraf i forhold til den særlige suspensions- og forbudsordning, som NIS 2-direktivet foreskriver i forhold til væsentlige teleudbydere, at såfremt Center for Cybersikkerhed vurderer, at allerede pålagte håndhævelsesforanstaltninger har vist sig at være utilstrækkelige, kan centeret fastsætte en frist, inden for hvilken den væsentlige teleudbyder skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde centrets krav. Er tiltagene ikke foretaget inden for den fastsatte frist, kan Center for Cybersikkerhed træffe afgørelse om 1) midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, udbyderen leverer, eller aktiviteter, der udføres af udbydere, og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner i den pågældende udbyder.

Det foreslås endvidere, at Center for Cybersikkerhed skal kunne fastsætte nærmere regler for, hvilke certificeringer og godkendelser som skal kunne midlertidigt suspenderes. Det forudsættes ligeledes, at der ikke vil ske midlertidige suspensioner af certificeringer eller godkendelser, før Center for Cybersikkerhed har anvendt den tillagte bemyndigelse.

Det vil være en forudsætning for anvendelse af ordningen, at mindre indgribende midler i form af anvendte håndhævelsesforanstaltninger har vist sig utilstrækkelige.

I overensstemmelse med direktivet foreslås det, at sådanne midlertidige suspensioner eller midlertidige forbud mod, at fysiske personer må udøve ledelsesfunktioner, kun kan anvendes, indtil teleudbyderen træffer de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at tiltagene blev anvendt.

Det foreslås endvidere, at teleudbyderen eller den fysiske person, som afgørelsen vedrører, kan forlange, at en afgørelse om suspension eller et midler-

tidigt forbud mod at fysiske personer må udøve ledelsesfunktioner, indbringes for domstolene.

Center for Cybersikkerhed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den teleudbyder eller person, som har forlangt sagen indbragt.

3.8. Ansvar og sanktioner

3.8.1. Gældende ret

Efter § 14, stk. 1, i lov om sikkerhed i net og tjenester straffes med bøde, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der 1) undlader at efterkomme Center for Cybersikkerheds påbud efter § 3, stk. 2, 3 eller 4, eller § 5, stk. 4, 2) overtræder § 6, stk. 1-4, 3) undlader at efterkomme Center for Cybersikkerheds krav efter § 9, stk. 2, 4 eller 5, eller 4) hindrer Center for Cybersikkerhed i at få adgang efter § 9, stk. 6 eller 7.

Efter § 14, stk. 2, i lov om sikkerhed i net og tjenester kan der i regler, som udfærdiges i medfør af § 3, stk. 1, 3 eller 4, § 4, § 5, stk. 1, 2 eller 3, § 5 a eller § 6, stk. 6, fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Bemyndigelsen i § 14, stk. 2, i lov om sikkerhed i net og tjenester er, for så vidt angår lovens § 3, stk. 1, 3 og 4, og § 5, stk. 1 og 2, udmøntet i bekendtgørelse nr. 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester. De nærmere regler følger af bekendtgørelsens kapitel 6 om straffebestemmelser og ikrafttrædelse.

Derudover er bemyndigelsen, for så vidt angår lovens § 4, udmøntet i bekendtgørelse nr. 1414 af 11. november 2023 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 15 om straffebestemmelser.

Bemyndigelsen er endvidere, for så vidt angår lovens 5, stk. 3, udmøntet i bekendtgørelse nr. 261 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv. De nærmere regler følger af bekendtgørelsens kapitel 6 om straffebestemmelser og ikrafttrædelse.

Endeligt er bemyndigelsen, for så vidt angår lovens § 6, stk. 6, udmøntet i bekendtgørelse nr. 260 af 22. februar 2021 om sikkerhedsgodkendelse af medarbejdere på området for sikkerhed i net og tjenester. De nærmere regler følger af bekendtgørelsens § 2.

Efter § 14, stk. 3, i lov om sikkerhed i net og tjenester kan der pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Lov om sikkerhed i net og tjenester indeholder derimod ikke nærmere bestemmelser om ansvar for bestemte fysiske personer.

Lovens § 14, stk. 1-3 – og de dele af bekendtgørelserne, der er udstedt i medfør af lovens § 14, stk. 2 – er delvis implementering af artikel 29 i EU's telekodeks.

Det bemærkes således, at visse af de bestemmelser, der efter § 14 i lov om sikkerhed i net og tjenester er strafbelagte, udgør en del af den nationale særregulering, der ikke er implementering af EU-regulering, og som er fastsat for at sikre, at der tages højde for det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet, jf. afsnit 2.1.3 ovenfor.

3.8.2. NIS 2-direktivet

Med NIS 2-direktivet ophæves alene artikel 40 og 41 i EU's telekodeks. Henset til, at de sikkerhedskrav og underretningspligter, som teleudbyderne skal efterleve, fremgår af NIS 2-direktivet, må de sanktioner, der følger af NIS 2-direktivet, efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse ligeledes anses for at finde anvendelse for disse.

NIS 2-direktivets artikel 36 fastsætter herefter en forpligtelse for medlemsstaterne til at fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelse af de nationale foranstaltninger, der er vedtaget i medfør af direktivet, ligesom medlemsstaterne skal træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Den grundlæggende tilgang i NIS 2-direktivets artikel 36 svarer således i det væsentligste til tilgangen i artikel 29 i EU's telekodeks.

NIS 2-direktivets artikel 34 indeholder imidlertid – som noget nyt i forhold til EU's telekodeks – regler om generelle betingelser for pålæggelse af administrative bøder til væsentlige og vigtige enheder.

Der lægges således i NIS 2-direktivets artikel 34 op til, at bøder pålægges administrativt – det vil sige af de kompetente myndigheder – medmindre

medlemsstaternes nationale retssystem ikke giver mulighed herfor. I givet fald skal bestemmelserne om administrative bøder efter direktivets artikel 34, stk. 8, anvendes således, at disse i sidste ende pålægges af de nationale domstole. Det skal sikres, at virkningen svarer til virkningen af administrative bøder.

3.8.3. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser

Det følger af NIS 2-direktivets artikel 34, stk. 2, at (administrative) bøder vil kunne blive pålagt i tillæg til en hvilken som helst af håndhævelsesforanstaltningerne vedrørende væsentlige og vigtige enheder, herunder – for så vidt angår væsentlige enheder – også den særlige suspensions- og forbudsordning.

NIS 2-direktivets artikel 34, stk. 3, foreskriver desuden nærmere, hvilke hensyn, der skal indgå i beslutningen om, hvorvidt der skal pålægges en bøde samt bødens størrelse. Hensynene er de samme som de hensyn, der skal indgå i en afgørelse om at træffe håndhævelsesforanstaltninger efter artikel 32, stk. 7, jf. afsnit 3.4.2 ovenfor.

Efter NIS 2-direktivets artikel 34, stk. 4, skal væsentlige enheders overtrædelse af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) straffes med et maksimum på mindst 10.000.000 EUR eller et maksimum på mindst 2 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter, hvad der er højest.

Efter NIS 2-direktivets artikel 34, stk. 5, skal vigtige enheders overtrædelse af direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser) straffes med et maksimum på mindst 7.000.000 EUR eller et maksimum på mindst 1,4 pct. Af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter, hvad der er højest.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets undtagelsesbestemmelse i artikel 34, stk. 8, i forhold til administrative bøder finder anvendelse. Direktivets bestemmelser om administrative bøder vil således skulle fortolkes og implementeres på en måde, hvor bøder ikke pålægges administrativt, men i det almindelige strafferetlige system. Det indebærer, at Center for Cybersikkerhed i givet fald vil skulle

indgive politianmeldelse, såfremt de konstaterer strafbelagte overtrædelser af denne lov eller regler udstedt i medfør af denne lov.

Center for Cybersikkerhed vil skulle påse, at denne lov og regler udstedt i medfør af loven efterleves, herunder undersøge mulige overtrædelser af lovgivningen. I den situation, hvor Center for Cybersikkerhed måtte blive bekendt med, at der kan være sket en strafbar overtrædelse af loven eller regler udstedt i medfør af loven, vil centeret efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse skulle foretage en konkret vurdering – under hensyntagen til omstændighederne i hver enkelt sag og sanktionsregimets effektivitet, forholdsmæssighed og afskrækkende virkning – og på den baggrund beslutte, om forholdet skal anmeldes til politiet.

Det bemærkes, at indførelsen af administrative bøder i dansk ret giver betænkeligheder i forhold til grundloven. I dansk retspleje er det et grundlæggende princip, at bøder, der har karakter af en strafferetlig sanktion, kun kan idømmes ved domstolene og i strafferetsplejens former, der sikrer den sigtede en effektiv beskyttelse.

Henset til, at der ikke anvendes administrative bøder i dansk ret, jf. ovenfor, forudsættes det, at de pågældende hensyn indgår i Center for Cybersikkerheds beslutning om politianmeldelse af et forhold samt i politi- og anklagemyndighedens samt domstolenes vurdering af sagen, herunder ved udmålingen af en eventuel bøde.

Derudover gælder der i dansk ret typiske ikke noget lovbestemt maksimum for bødestørrelse. Det er dog Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der bør fastsættes maksimale bødeniveauer svarende til de niveauer, der er fastsat i direktivet. Dermed vil der ikke kunne straffes med højere bøder end det minimumsniveau, der er forudsat i direktivet.

3.8.3.1. Særligt om tvangsbøder

Det følger af NIS 2-direktivets artikel 34, stk. 6 – som noget nyt i forhold til EU's telekodeks – at medlemsstaterne kan fastsætte beføjelser til at pålægge tvangsbøder for at tvinge en væsentlig eller vigtig enhed til at bringe en overtrædelse af direktivet til ophør i overensstemmelse med en forudgående afgørelse truffet af den kompetente myndighed.

Efter retsplejelovens § 997, stk. 3, kan der i domme, hvorved nogen tilpligtes at opfylde en forpligtelse mod det offentlige, som tvangsmiddel fastsættes en fortløbende bøde, der tilfalder statskassen (tvangsbøder).

Det følger således allerede af de almindelige regler i retsplejeloven, at domstolene kan pålægge tvangsbøder for at få nogen til at opfylde en forpligtelse mod det offentlige, herunder de kompetente myndigheder.

Administrative tvangsbøder er derimod tvangsbøder, som ikke pålægges af domstolene, men af forvaltningen. En administrativ tvangsbøde er således en afgørelse om, at en økonomisk sanktion vil blive pålagt, hvis en handlepligt ikke opfyldes – f.eks. et påbud eller en pligt til at udlevere bestemte oplysninger.

Sådanne bøder kan ofte opfattes som en straf, og der er ikke samme retssikkerhedsgarantier som tvangsbøder pålagt af domstolene. Det antages derfor normalt i dansk ret, at der kun bør derfor gives hjemmel til administrative tvangsbøder, hvis der foreligger et helt særligt behov for effektiv kontrol og håndhævelse på det pågældende område. Endvidere bør de forhold, der udløser tvangsbøderne, være let konstaterbare.

På denne baggrund er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der ikke bør skabes hjemmel til administrative tvangsbøder på dette område. Det skal bl.a. ses i lyset af, at det på nuværende tidspunkt er usikkert, om de forhold, der i givet fald vil kunne begrunde tvangsbøder, er så tilstrækkeligt objektivt konstaterbare, at det vil være ubetænkeligt at skabe en sådan hjemmel.

Ministeriet for Samfundssikkerhed og Beredskab vurderer således som udgangspunkt, at de retsmidler, der foreslås med denne lov, herunder tilsyns- og håndhævelsesforanstaltningerne samt muligheden for at offentliggøre afgørelser mv., er tilstrækkelige til at sikre, at reglerne efterleves. Dette skal også ses i lyset af de eksisterende muligheder i retsplejeloven for at anvende tvangsbøder.

3.8.3.2. Særligt om fysiske personers strafansvar, herunder valg af ansvarssubjekt

NIS 2-direktivets artikel 34 indeholder generelle betingelser for pålæggelse af bøder rettet mod væsentlige og vigtige enheder, og dermed de juridiske personer som sådan. De forudsatte bødeniveauer udmåles bl.a. på baggrund af virksomhedens årsomsætning.

Det følger dog af NIS 2-direktivets artikel 32, stk. 6 – som noget nyt i forhold til EU's telekodeks – at medlemsstaterne sikrer, at enhver fysisk per-

son, der er ansvarlig for eller optræder som juridisk repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at den overholder dette direktiv. Medlemsstaterne sikrer, at det er muligt at drage sådanne fysiske personer til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelse af dette direktiv.

Det er i NIS 2-direktivets præambelbetragtning nr. 130 forudsat, at hvor en bøde pålægges en person, der ikke er en virksomhed, bør den kompetente myndighed ved fastsættelsen af en passende bødestørrelse tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske stilling.

Efter NIS 2-direktivets artikel 20, stk. 1, skal væsentlige og vigtige enheders ledelsesorganer kunne gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i artikel 21 (om foranstaltninger til styring af cybersikkerhedsrisici). Artikel 20, stk. 1, berører dog ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv, jf. bestemmelsens 2. led.

Det følger af Rigsadvokatmeddelelse CIR1H nr. 11550 af 17. april 2015 om strafansvar for juridiske personer, at udgangspunktet ved valg af ansvarssubjekt i særlovgivningen er, at tiltalen rejses mod den juridiske person.

Det er i den forbindelse en forudsætning for at pålægge en juridisk person ansvar, at der inden for dens virksomhed er begået en overtrædelse, der kan tilregnes en eller flere til virksomheden knyttede personer eller virksomheden som sådan, jf. straffelovens § 27, stk. 1.

Det fremgår dog også af rigsadvokatmeddelelsen, at der i en række tilfælde kan være anledning til – ud over tiltalen mod den juridiske person – tillige at rejse tiltale mod en eller flere fysiske personer, såfremt den eller de pågældende har handlet forsætligt eller udvist grov uagtsomhed. Der angives endvidere retningslinjer for anklagemyndighedens afgørelsen herom.

Det beskrives i den forbindelse, at der på en række områder er fastsat særlige regler, som pålægger enkeltpersoner et selvstændigt og individuelt strafansvar i kraft af deres særlige stilling eller funktion, eksempelvis piloter og besætningsmedlemmer. I så fald er udgangspunktet, at der rejses tiltale mod den pågældende person samt i almindelighed tillige mod den juridiske per-

son. I visse tilfælde indeholder lovgivningen endvidere mulighed for et selvstændigt og individuelt strafansvar, selv om overtrædelsen ikke kan tilregnes de pågældende som forsætlig eller uagtsom (objektivt individualansvar).

Ministeriet for Samfundssikkerhed og Beredskab finder ikke på dette område anledning til at fastsætte særlige regler om et selvstændigt og individuelt strafansvar for fysiske personer, herunder regler, som går videre end strafansvaret for juridiske personer. Det er således Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at NIS 2-direktivets krav om, at nærmere bestemte fysiske personer kan drages til ansvar for tilsidesættelse af deres forpligtelser efter direktivet ikke synes at stille krav, der går videre end det, der allerede følger af de gældende regler.

Dermed vil et eventuelt strafansvar for fysiske personer følge det almindelige udgangspunkt i særlovgivningen, hvorefter der i tillæg til den juridiske person efter nærmere retningslinjer kan rejses tiltale mod en fysisk person, såfremt denne har handlet forsætligt eller groft uagtsomt. Bøder vil i givet fald skulle udmåles i overensstemmelse med direktivets forudsætninger om størrelsen heraf.

3.8.3.3. Særligt om brud på persondatasikkerheden

NIS 2-direktivets artikel 35, stk. 2, indeholder særlige bestemmelser, for så vidt angår overtrædelser af forpligtelserne i direktivets artikel 21 (om foranstaltninger til styring af cybersikkerhedsrisici) og artikel 23 (om rapporteringsforpligtelser), der (også) kan medføre et brud på persondatasikkerheden i medfør af databeskyttelsesforordningen.

Det følger således af direktivets artikel 35, stk. 2, at der ikke kan straffes med (administrativ) bøde for overtrædelser af de ovenfor nævnte bestemmelser i medfør af NIS 2-direktivet, såfremt den samme adfærd straffes med (administrativ) bøde efter databeskyttelsesforordningen.

Henset til, at der ikke anvendes administrative bøder i dansk ret, jf. ovenfor, vil bestemmelserne skulle fortolkes og gennemføres i lyset heraf.

Det bemærkes, at databeskyttelsesloven supplerer og gennemfører databeskyttelsesforordningen i dansk ret, og at lovens § 41 indeholder bestemmelser om straf for overtrædelser af databeskyttelsesforordningen og databeskyttelsesloven.

Henset til, at et brud på cybersikkerheden efter omstændighederne også kan udgøre et brud på persondatasikkerheden, er bestemmelsen i NIS 2-direktivets artikel 35, stk. 2, udtryk for det almindelige forbud mod dobbelt strafforfølgning. Det anføres således i præambelbetragtning nr. 131, at pålæggelse af sanktioner for overtrædelse af de nationale regler, der gennemfører NIS 2-direktivet, ikke bør føre til et brud på princippet om *ne bis in idem* som fortolket af Den Europæiske Unions Domstol.

Det følger af NIS 2-direktivet, at de kompetente myndigheder ikke er afskåret fra at anvende håndhævelsesforanstaltninger i de pågældende situationer.

For at sikre, at myndighederne har mulighed for at undgå, at den samme adfærd straffes dobbelt, forpligter NIS 2-direktivets artikel 35, stk. 1, de kompetente myndigheder efter NIS 2-direktivet til uden unødigt ophold at underrette tilsynsmyndighederne efter databeskyttelsesforordningen – i dansk ret Datatilsynet. Det omfatter tilfælde, hvor de kompetente myndigheder i forbindelse med deres tilsyn eller håndhævelse bliver opmærksomme på, at en væsentlig eller vigtig enheds overtrædelse af forpligtelserne i NIS 2-direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller 23 (rapporteringsforpligtelser) kan medføre et brud på persondatasikkerheden, som skal anmeldes i henhold til artikel 33 i databeskyttelsesforordningen.

Ministeriet for Samfundssikkerhed og Beredskab bemærker i forlængelse heraf, at det af databeskyttelsesforordningens artikel 4, nr. 12, følger, at »brud på persondatasikkerheden« er defineret som et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet. Bestemmelsen i forordningens artikel 33, stk. 1, indebærer, at den dataansvarlige skal anmelde et brud på persondatasikkerheden til Datatilsynet, »medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder«.

Center for Cybersikkerhed vil derfor alene skulle foretage underretning af Datatilsynet på baggrund af NIS 2-direktivets artikel 35, stk. 1, om mulige brud på persondatasikkerheden, hvis det ikke er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der må overlades Center for Cybersikkerhed et bredt skøn ved foretagelsen af denne vurdering.

Det forudsættes, at Center for Cybersikkerhed i relevant omfang hører Datatilsynet om, hvorvidt den adfærd, der var genstand for overtrædelsen af NIS 2-direktivet, er eller vil blive straffet med bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven med henblik på, at NIS 2-direktivets hensigt om at undgå dobbelt strafforfølgning kan indfries i praksis.

3.8.4. Den foreslåede ordning

Det foreslås, at der indsættes sanktionsbestemmelser i loven med det formål, at overtrædelse af alle materielle og processuelle krav i loven eller regler udstedt i medfør af loven til væsentlige og vigtige udbydere kan straffes med bøde.

På den baggrund foreslås det først og fremmest, at den, der overtræder § 5, stk. 1, eller 2, §§ 6, 8, 9, stk. 1, § 10, stk. 1 eller 2, eller § 12, undlader at efterkomme Center for Cybersikkkerheds afgørelse efter § 21, stk. 1, nr. 1 eller 2, undlader at efterkomme påbud og forbud efter §§ 22 eller 25, undlader at efterkomme krav efter § 13, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, eller § 24, stk. 1, nr. 2, eller nr. 4-7, eller hindrer Center for Cybersikkerhed i at føre tilsyn efter bestemmelserne § 21, stk. 1, nr. 1-4 eller § 24, stk. 1, nr. 1-3, straffes med bøde. Det foreslås i den forbindelse, at der ikke anvendes administrative bøder, men at bøder udstedes og udmåles i det almindelige straffeprocessuelle system.

Det foreslås desuden, at bøder vil kunne pålægges fysiske personer og selskaber mv. (juridiske personer), i det omfang de omfattes af lovens anvendelsesområde.

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 4 og 5, at bødens størrelse for væsentlige teleudbydere for så vidt angår overtrædelse af bestemmelserne i § 5, stk. 1 eller 2, §§ 6, 8, 9, stk. 1, § 10, stk. 1 eller 2, eller § 12, og reglerne udstedt i medfør af § 33, stk. 4, maksimalt vil udgøre et beløb svarende til 10.000.000 euro eller 2 pct. af udbyderens samlede globale årsomsætning i det foregående regnskabsår, alt efter, hvad der er højest. Det forudsættes desuden, at bødens størrelse for vigtige teleudbydere for så vidt angår overtrædelse af de samme bestemmelser maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct. af byderens samlede globale årsomsætning i det foregående regnskabsår, alt efter, hvad der er højest.

NIS 2-direktivet indeholder ikke særlige forudsætninger for så vidt angår det maksimale bødeniveau for manglende efterlevelse af forpligtelser i direktivet ud over artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) og artikel 23 (rapporteringsforpligtelser). På den baggrund fastsættes der ikke maksimale bødeniveauer for overtrædelse af lovens øvrige bestemmelser.

Bøderne vil kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 22, 23 og 25.

Ved afgørelse om at politianmelde et forhold, ved pålæg af en bøde og ved udmåling af bødens størrelse forudsættes det, at der lægges vægt på de i afsnit 3.9.3 ovenfor beskrevne hensyn.

Det foreslås endvidere i overensstemmelse med direktivet, at hvor der er pålagt en bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven, kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd.

Endeligt foreslås det, at de skærpede nationale særregler, der foreslås videreført i §§ 20 og 14, stk. 5, fortsat skal være strafbelagte som hidtil. Der er med videreførelsen således ikke tilsigtet materielle ændringer af de nuværende bestemmelsers indhold. Det indebærer, at for overtrædelse af de nævnte bestemmelser vil det således fortsat være de hidtidige bødeniveauer, der vil skulle udmåles efter.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Center for Cybersikkerhed, som er myndighed for informationssikkerhed og beredskab i telesektoren, vil fortsat skulle føre tilsyn med teleudbyderes overholdelse af loven, og regler, der er udstedt i medfør heraf. Center for Cybersikkerhed vil imidlertid i medfør af §§ 20 og 21, der bl.a. implementerer NIS 2-direktivet, kunne foretage et mere omfattende og – for så vidt angår de væsentlige teleudbydere – forudgående tilsyn end hidtil. Som følge heraf kan der være visse administrative meromkostninger forbundet hermed, men disse vil blive afholdt inden for den eksisterende bevillingsmæssige ramme.

I det omfang staten udbyder offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, vil de krav,

der efter lovforslaget stilles til udbydere af disse net og tjenester, også omfatte staten. Det vil kunne medføre økonomiske konsekvenser og implementeringskonsekvenser i samme omfang som for private udbydere.

Det bemærkes i den forbindelse, at kommuner og regioner, der udbyder offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, ikke er omfattet af nærværende lovforslag, men derimod forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau.

4.1. De syv principper for digitaliseringsklar lovgivning

Det er Ministeriet for Samfundssikkerhed og Beredskab vurdering, at lovforslaget er i overensstemmelse med principperne for digitaliseringsklar lovgivning.

Princip nr. 1 om enkle og klare regler er efter Ministeriet for Samfundssikkerhed og Beredskab opfattelse iagttaget, idet det i lovforslaget – inden for NIS 2-direktivets rammer – klart fremgår, hvilke forpligtelser der påhviler omfattede teleudbydere, og hvilke beføjelser Center for Cybersikkerhed har i sit tilsyn med teleudbydernes efterlevelse af deres forpligtelser.

Det er desuden Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at lovforslaget er udarbejdet i overensstemmelse med princip nr. 2 om digital kommunikation, idet § 35 indfører hjemmel til at fastsætte regler om digital kommunikation.

Derudover er det Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at lovforslaget er i overensstemmelse med princip nr. 5 om tryg og sikker datahåndtering henset til, at lovforslaget indeholder en grundig beskrivelse af forholdet til databeskyttelsesretten, ligesom NIS 2-direktivet fremmer et højere og mere ensartet cybersikkerhedsniveau på tværs af EU's medlemslande.

Det bemærkes navnlig i relation til registrerings- og underretningspligterne i § 7 og § 10, at der med lovforslaget forudsættes anvendt digitale selvbetjeningsløsninger såsom Virk.dk. Dermed anvendes eksisterende offentlig it-infrastruktur til digital kommunikation mellem teleudbyderne og Center for Cybersikkerhed, hvilket vurderes at være i overensstemmelse med princip nr. 6 om anvendelse af offentlig infrastruktur.

Det er Ministeriet for Samfundssikkerhed og Beredskab vurdering, at de øvrige principper ikke er relevante for lovforslaget.

5. Økonomiske og administrative konsekvenser for erhvervslivet mv.
På baggrund af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet er det Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de eksisterende skærpede nationale særregler bør videreføres med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren.

Det har ikke været muligt at foretage en kvantificering af de erhvervsøkonomiske og administrative konsekvenser for erhvervslivet, inden den offentlige høring. Det vurderes foreløbigt, at lovforslaget medfører øvrige efterlevelseskonsekvenser for erhvervslivet på mindre end 10 mio. kr. Det vurderes foreløbigt, at lovforslaget har administrative konsekvenser for erhvervslivet på mindre end 4 mio. kr. De erhvervsøkonomiske og administrative konsekvenser for erhvervslivet vil blive kvantificeret nærmere af Erhvervsstyrelsen, inden lovforslagets fremsættelse.

Innovations- og Iværksættertjekket vurderes ikke at være relevant for lovforslaget, fordi forslaget ikke påvirker virksomheders eller iværksætteres muligheder for at teste, udvikle og anvende nye teknologier og innovation.

6. Administrative konsekvenser for borgerne
Lovforslaget vurderes ikke at have administrative konsekvenser for borgerne.

7. Klimamæssige konsekvenser
Lovforslaget vurderes ikke at have klimamæssige konsekvenser.

8. Miljø- og naturmæssige konsekvenser
Lovforslaget vurderes ikke at have miljø- og naturmæssige konsekvenser.

9. Forholdet til databeskyttelsesretten
Behandling af personoplysninger er i almindelighed reguleret i databeskyttelsesforordningen og databeskyttelsesloven.

Spørgsmålet om, hvorvidt der må behandles personoplysninger, er i dag som udgangspunkt reguleret i databeskyttelsesforordningens artikel 6, stk. 1 (om behandling af almindelige personoplysninger), artikel 9, stk. 2 (om behandling af følsomme personoplysninger), og artikel 10 (om behandling af personoplysninger vedrørende straffedomme og lovovertrædelser).

Med lovforslaget gennemføres NIS 2-direktivet i telesektoren.

Lovforslaget indebærer en række forpligtelser for omfattede teleudbydere samt myndighedsopgaver for Center for Cybersikkerhed, der i et vist omfang vil indebære behandling af personoplysninger.

Der kan således indgå almindelige personoplysninger i de oplysninger, som teleudbyderne som led i overholdelsen af registreringsforpligtelsen i den foreslåede bestemmelse i § 8 skal indgive til Center for Cybersikkerhed, eksempelvis i form af visse kontaktoplysninger på medarbejdere hos teleudbyderen.

Derudover kan der indgå almindelige personoplysninger i en teleudbyders hændelsesunderretning til Center for Cybersikkerhed i medfør af de foreslåede bestemmelser i §§ 9 og 10. Dette vil eksempelvis kunne være i forbindelse med en redegørelse for hændelsens faktiske forløb, eller ved at der vedlægges e-mails, logningsoplysninger eller andet materiale, der belyser hændelsens forløb, karakter eller håndtering.

Der kan endvidere i forbindelse med anvendelsen af tilsyns- og håndhævelsesforanstaltninger i medfør af de foreslåede bestemmelser i § 21 og § 22 samt §§ 24-25 blive behandlet almindelige personoplysninger. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de oplysninger, der måtte blive behandlet i denne forbindelse, vil udgøre oplysninger om teleudbyderens medarbejdere. Disse oplysninger vil primært udgøre kontaktoplysninger på teleudbyderens kontaktpersoner, ligesom der eksempelvis kan være tale om oplysninger om hvilke medarbejdere, der har adgang til teleudbyderens net- og informationssystemer.

Det følger af NIS 2-direktivets artikel 2, stk. 14, 1. led, at enheder, de kompetente myndigheder, de centrale kontaktpunkter og CSIRT'erne behandler personoplysninger i det omfang, det er nødvendigt med henblik på dette direktiv og i overensstemmelse med databeskyttelsesforordningen, navnlig på grundlag af artikel 6 deri.

Det er Ministeriet for Samfundssikkerhed og Beredskab opfattelse, at behandling af almindelige personoplysninger i forbindelse med overholdelsen af registreringsforpligtelsen i § 8 og underretningsforpligtelserne i § 9 og § 10 samt i forbindelse med Center for Cybersikkerheds anvendelse af tilsyns- og håndhævelsesforanstaltninger efter § 21 og § 22 samt §§ 24-25 for private virksomheder vil kunne ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra c og e. Det følger af artikel 6, stk. 1, litra c, at behandling er lovlig, hvis den er nødvendig for at overholde en retlig forpligtelse,

som påhviler den dataansvarlige, ligesom det følger af litra e, at behandling er lovlig, hvis den er nødvendig af hensyn til udførelse af en opgave i samfundets interesse. Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at behandlingen af almindelige personoplysninger kan ske i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra f. Det følger af denne bestemmelse, at behandling er lovlig, hvis den er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

For så vidt angår offentlige myndigheder henvises der til forordningens artikel 6, stk. 1, litra e, hvorefter behandling bl.a. er lovlig, hvis behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse.

10. Forholdet til EU-retten

Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 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) i dansk ret. Derudover gennemfører loven og de bekendtgørelser, der vil udstedt i medfør af loven, dele af Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (omarbejdning).

Det følger af artikel 41, stk. 1, i NIS 2-direktivet, at direktivet skal være implementeret i dansk ret senest den 17. oktober 2024 og træde i kraft senest den 18. oktober 2024. Med den foreslåede bestemmelse i § 37 vil loven dermed træde i kraft 1. juli 2025. Det bemærkes, at de dele af EU's telekodeks, der i dag henhører under Ministeriet for Samfundssikkerhed og Beredskabs ressortansvar, tidligere er implementeret i dansk ret ved lov nr. 1831 af 8. december 2020 om ændring af lov om net- og informationssikkerhed (Implementering af direktivet om oprettelse af en europæisk kodeks for elektronisk kommunikation, for så vidt angår sikkerhed i net og tjenester).

10.1. Principper for implementering af erhvervsrettet EU-regulering

For så vidt angår princip nr. 1 om, at den nationale regulering som udgangspunkt ikke bør gå videre end minimumskravene i EU-reguleringen, bemærkes det, at loven indeholder nationale særregler, der på visse områder går videre end de krav, der følger af NIS 2-direktivet. Det er Ministeriet for

Samfundssikkerhed og Beredskabs vurdering, at der er væsentlige hensyn, der taler for, at der med lovforslaget sker en videreførelse af de eksisterende skærpede nationale særregler med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren. Dette skal set i lyset af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet. Ministeriet for Samfundssikkerhed og Beredskab vurderer således, at lovforslaget fraviger princip nr. 1, idet ministeriet i forbindelse med implementeringen af NIS 2-direktivet fastholder de allerede eksisterende skærpede nationale særregler.

For så vidt angår princip 2 om, at danske virksomheder ikke bør stilles dårligere i den internationale konkurrence, hvorfor implementeringen ikke bør være mere byrdefuld end den forventede implementering i sammenlignelige lande, er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at implementeringen lever op til dette princip. Med lovforslaget foretages en minimumsimplementering af de nye cybersikkerhedskrav samt oplysnings- og underretningspligter, der følger af NIS 2-direktivet. Samtidig er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der er særlige hensyn, der taler for, at der med lovforslaget sker en videreførelse af de eksisterende skærpede nationale særregler med henblik på at sikre en opretholdelse af det nuværende høje sikkerhedsniveau for telesektoren. Dette skal set i lyset af det generelt høje trusselsbillede på cyberområdet og telesektorens samfundsmæssige kritikalitet, jf. afsnit 2.1.3.

For så vidt angår princip 3 om, at fleksibilitet og undtagelsesmuligheder i EU-reguleringen bør udnyttes, skal det bemærkes, at Ministeriet for Samfundssikkerhed og Beredskab har afsøgt mulighederne herfor. NIS 2-direktivet indeholder imidlertid ikke sådanne muligheder i relation til telesektoren.

For så vidt angår princip 4 om, at EU-regulering – i det omfang det er muligt og hensigtsmæssigt, bør implementeres gennem alternativer til regulering, har Ministeriet for Samfundssikkerhed og Beredskab overvejet, om det er muligt og hensigtsmæssigt, at NIS 2-direktivet implementeres gennem alternativer til regulering. Ministeriet for Samfundssikkerhed og Beredskab vurderer imidlertid, at der er tale om et direktiv, der skal implementeres ved lovgivning.

For så vidt angår princip 5 om, at byrdefuld EU-regulering bør træde i kraft senest muligt og under hensyntagen til de fælles ikrafttrædelsesdatoer, er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at den foreslåede ikrafttrædelsesdato i § 37 lever op til dette princip.

10. Hørte myndigheder og organisationer mv.

Et udkast til lovforslag har i perioden fra [X] til den [X] været sendt i høring hos følgende myndigheder og organisationer mv.:

Advokatrådet, Amnesty International, Bauer Media, Borch Teknik, Cibicom A/S, Danmarks Radio, Dansk Beredskabskommunikation A/S, Dansk Energi, Dansk Erhverv, Dansk Industri (DI), DANSK IT, Dansk Kabel TV, Danske Advokater, Danske Regioner, Datatilsynet, DanPilot, Den Danske Dommerforening, DI Digital, Domstolsstyrelsen, Fibia A/S, Forenede Danske Antenneanlæg, GLOBALCONNECT A/S, Hi3G Denmark ApS, HORESTA, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, Justitia, KL, Norlys, Præsidenten for Vestre Landsret, Præsidenten for Østre Landsret, Retspolitisk Forening, Rigsrevisionen, Rådet for Digital Sikkerhed, Samtlige byretspræsidenter, TDC A/S, TeleDCIS Teleindustrien (TI), Telenor A/S, Telia Company Danmark A/S, TT-Netværket P/S, TV 2 DTT A/S og Waoo A/S.

11. Sammenfattende skema		
	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen.	De statsfinansielle konsekvenser til øgede aktiviteter afstedkommet af lovforslaget vurderes at være beskedne og vil blive afholdt inden for egen ramme.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Ingen.
Økonomiske konsekvenser for erhvervslivet mv.	Ingen.	Lovforslaget forventes at medføre negative de erhvervsøkonomiske konsekvenser for erhvervslivet, som forventes at være mindre end 10 mio. kr.
Administrative konsekvenser	Ingen.	Lovforslaget forventes at medføre negative administrative konsekvenser for

for erhvervslivet mv.		erhvervslivet, som forventes at være mindre end 4 mio. kr.
Administrative konsekvenser for borgerne	Ingen.	Ingen.
Klimamæssige konsekvenser	Ingen.	Ingen.
Miljø- og naturmæssige konsekvenser	Ingen.	Ingen.
Forholdet til EU-retten	Loven og de bekendtgørelser, der vil blive udstedt i medfør af loven, gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt 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). Der henvises til EU-tidende 2022, L nr. 333, side 80.	
Er i strid med de fem principper for implementering af erhvervsrettet EU-regulering (der i relevant omfang også gælder ved implementering af ikke-erhvervsrettet EU-regulering) (sæt X)	Ja [X]	Nej

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021, regulerer i dag informationssikkerhed og beredskab i telesektoren, og finder anvendelse for udbydere af elektroniske kommunikationsnet eller -tjenester.

Det følger af NIS 2-direktivets artikel 2, stk. 1, at direktivet bl.a. finder anvendelse på udbydere af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, jf. direktivets bilag I, pkt. 8. Det følger af derudover af NIS 2-direktivets artikel 26, stk. 1, litra a, at udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester anses for at henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres net eller tjenester.

Det følger af den foreslåede *§ 1, stk. 1*, at loven finder anvendelse for udbydere, der stiller offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed i Danmark.

Den foreslåede bestemmelse gennemfører NIS 2-direktivets artikel 2, stk.1, og artikel 26.

Det foreslås med *stk. 2,* at loven ikke finder anvendelse for kommuner og regioner, der stiller offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester til rådighed i Danmark.

Baggrunden herfor er, at det følger af bemærkningerne til § 1, stk. 2, i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, at 'i telesektoren vil enheder i enhedskategorierne »udbydere af offentlige elektroniske kommunikationsnet« og »udbydere af offentligt tilgængelige elektroniske kommunikationstjenester«, i sektoren »Digital infrastruktur« i bilag I til NIS 2-direktivet, som udgangspunkt blive omfattet af lov om sikkerhed og beredskab i telesektoren. I det omfang kommuner og regioner måtte udbyde offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, vil de imidlertid være omfattet af nærværende lov.'

I *stk. 3* foreslås det, at teleudbydere, uanset om de er omfattet af lovens anvendelsesområde, kan give frivillig underretning til Center for Cybersikkerhed og CSIRT'en efter § 11.

Efter den foreslåede bestemmelse i § 11 kan alle teleudbydere underrette CSIRT'en om hændelser, der negativt påvirker eller vurderes at kunne påvirke tilgængeligheden, integriteten eller fortroligheden af data, informationssystemer, digitale netværk eller digitale servicer.

Den foreslåede bestemmelse indebærer, at enheder, der ellers ikke ville være omfattet af lovens anvendelsesområde, har mulighed for at give frivillig underretning til CSIRT'en om hændelser.

Bestemmelsen svarer til den tilsvarende bestemmelse i § 1, stk. 6, i lov om foranstaltning til sikring af øget cybersikkerhedsniveau.

Den foreslåede bestemmelse vil delvist gennemføre NIS 2-direktivets artikel 29, stk. 2.

I *stk. 4* foreslås det, at § 17 i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau finder tilsvarende anvendelse for denne lov.

Det fremgår af § 1, stk. 2, 2. pkt., i forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, at lovens § 17 finder anvendelse for enheder, der er omfattet af telesektoren.

Den foreslåede bestemmelse § 17 i lov om forslag til lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau, fastsætter CSIRT'ens opgaver over for væsentlige og vigtige enheder.

Der henvises til bemærkningerne til henholdsvis § 1, stk. 2, og § 17 i forslag til lov om sikring af et højt cybersikkerhedsniveau.

Til § 2

Den foreslåede bestemmelse i *§ 2* indeholder definitioner af lovens centrale begreber.

Definitionerne bygger hovedsageligt på de tilsvarende definitioner i NIS 2-direktivet. Hertil kommer videreførelse af centrale definitioner i lov om sikkerhed i net og tjenester, som ophæves med nærværende lov.

Hertil kommer definitioner fra gældende ret, herunder lov om sikkerhed i net og tjenesters samt EU's telekodeks.

Det foreslås, at *nr. 1,* at » Beredskabssituationer og andre ekstraordinære situationer« defineres som situationer hvor der allerede er, eller hvor der kan opstå større ulykker, katastrofer eller hændelser, herunder krise eller krig og som kan påvirke udbuddet af net og tjenester.

Definitionen svarer til den gældende definition heraf i bekendtgørelse nr 259 af 22. februar 2021 om sikkerhed og beredskab i net og tjenester.

Det foreslås, at *nr. 2,* at »cybertrussel« defineres som enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer.

Efter NIS 2-direktivets artikel 6, nr. 10, skal cybertrussel forstås på samme måde som definitionen i artikel 2, nr. 8, i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed).

Den foreslåede bestemmelse svarer til definitionen i den nævnte forordning. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med denne definition.

Det foreslås med *nr. 3,* at »elektronisk kommunikationsnet« defineres som et transmissionssystem, uanset om det bygger på en permanent infrastruktur eller en centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs- og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, og kabel-tv-net, uanset hvilken type information der overføres.

NIS 2-direktivets artikel 6, nr. 1, litra a) definerer et elektronisk kommunikationsnet ved en henvisning til i artikel 2, nr. 1), i direktiv (EU) 2018/1972. Den foreslåede definition i nr. 3, svarer til definitionen af et elektronisk

kommunikationsnet i artikel 2, nr. 1, i direktiv 2018/1972 (EU's telekodeks), og skal fortolkes i overensstemmelse hermed.

Det foreslås med *nr. 4*, at »elektronisk kommunikationstjeneste« defineres som en tjeneste, som normalt ydes mod betaling via elektroniske kommunikationsnet, og som med undtagelse af tjenester, der består i tilrådighedsstillelse af eller udøvelse af redaktionel kontrol over indhold fremført via elektroniske kommunikationsnet og -tjenester omfatter følgende typer tjenester; internetadgangstjenester, interpersonelle kommunikationstjenester og tjenester, der udelukkende eller overvejende består i overføring af signaler, som f.eks. transmissionstjenester, der anvendes til levering af maskine-til-maskine-tjenester og til radio- og tv-spredning.

Med NIS 2-direktivets artikel 6, nr. 37, defineres en elektronisk kommunikationstjeneste ved en henvisning til i artikel 2, nr. 4), i direktiv (EU) 2018/1972. Den foreslåede definition i nr. 3, svarer til definitionen af en elektronisk kommunikationstjeneste i artikel 2, nr. 4, i direktiv 2018/1972 (EU's telekodeks), og skal fortolkes i overensstemmelse hermed.

Det foreslås med *nr. 5,* at en »hændelse« defineres som en begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 6. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås med *nr. 6,* at »håndtering af hændelser« defineres som enhver handling og procedure, der tager sigte på at forebygge, opdage, analysere og inddæmme eller at reagere på og reetablere sig efter en hændelse.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 8. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås med *nr. 7,* at »interpersonel kommunikationstjeneste« defineres som en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren el-

ler modtagerne skal være, undtaget tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

Definitionen svarer med enkelte sproglige justeringer til den tilsvarende definition i artikel 2, nr. 5, i EU's telekodeks, hvorefter der ved »interpersonel kommunikationstjeneste« forstås en tjeneste, som normalt ydes mod betaling, og som muliggør direkte interpersonel og interaktiv informationsudveksling via elektroniske kommunikationsnet mellem et afgrænset antal personer, hvor de personer, der indleder eller deltager i kommunikationen, bestemmer hvem modtageren eller modtagerne skal være, og omfatter ikke tjenester, der blot muliggør interpersonel og interaktiv kommunikation som en mindre støttefunktion, der er tæt knyttet til en anden tjeneste.

Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med den tilsvarende definition i EU's telekodeks.

Det foreslås med *nr. 8,* at »net- og informationssystem« defineres som a) et elektronisk kommunikationsnet, hvorved forstås transmissionssystemer, uanset om de bygger på en permanent infrastruktur eller centraliseret administrationskapacitet, og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, herunder netelementer, der ikke er aktive, som gør det muligt at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnet, jordbaserede fastnet (kredsløbs og pakkekoblede, herunder i internettet) og mobilnet, elkabelsystemer, i det omfang de anvendes til transmission af signaler, net, som anvendes til radio- og tv-spredning, samt kabel-tv-net, uanset hvilken type information der overføres, b) enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data, og c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a og b med henblik på deres drift, brug, beskyttelse og vedligeholdelse.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 1, litra a. Det forudsættes, at definitionen forstås og fortolkes i overensstemmelse med definitionen i direktivet. Det bemærkes, at NIS 2-direktivets artikel 6, nr. 1, litra a, henviser til definitionen i EU's telekodeks artikel 2, nr. 1. Det forudsættes således desuden, at definitionen forstås og fortolkes i overensstemmelse med definitionen i EU's telekodeks.

Det foreslås med *nr. 9,* at »nærvedhændelse« defineres som en begivenhed, der kunne have bragt tilgængeligheden, autenciteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare, men som det lykkedes at forhindre, eller som ikke indtraf.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 5. Det forudsættes, at bestemmelsen fortolkes i overensstemmelse med direktivets definition.

Det foreslås med *nr. 10,* at »offentligt elektronisk kommunikationsnet« defineres som et elektronisk kommunikationsnet, som udelukkende eller overvejende bruges til udbud af elektroniske kommunikationstjenester, der er tilgængelige for offentligheden, og som danner grundlag for overførsel af information mellem netterminerringspunkter.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 36, som henviser til definitionen i artikel 2, nr. 8, i EU's telekodeks.

Det foreslås med *nr. 11,* at »offentligt tilgængelige elektroniske kommunikationstjenester« defineres som: En elektronisk kommunikationstjeneste, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere.

Den foreslåede bestemmelse viderefører delvist definitionen i § 2, nr. 3, i lov om sikkerhed i net og tjenester, og svarer til definitionen af offentlig elektronisk kommunikationstjeneste i telelovens § 2, nr. 10, og den foreslåede nr. 4 skal forstås og fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevant praksis. Begrebet slutbruger skal forstås og fortolkes i overensstemmelse med definitionen heraf i telelovens § 2, nr. 3.

Det foreslås med *nr. 12,* at et »radiobaseret lokalnet« defineres som et trådløst adgangssystem med lav effekt og lille rækkevidde, der har en lav risiko for at skabe interferens med andre sådanne systemer etableret i nærheden af andre brugere, og som på et ikkeeksklusivt grundlag anvender harmoniserede radiofrekvenser (RLAN).

Den foreslåede bestemmelse svarer til definitionen i artikel 2, nr. 24, i EU's telekodeks, og skal fortolkes i overensstemmelse hermed.

Det foreslås med *nr. 13,* at »sikkerhed i net- og informationssystemer« defineres som net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå enhver begivenhed, der kan være til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller af de tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 2. Det forudsættes, at definitionen forstås og fortolkes i overensstemmelse med direktivets definition.

Det foreslås med *nr. 14,* at »teleudbyder« defineres som den, der med et kommercielt formål stiller produkter af offentlige elektroniske kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester til rådighed for andre.

Definitionen viderefører definitionen af en udbyder i § 2, nr. 4, i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Det foreslås med *nr. 15*, at »væsentlig cybertrussel« defineres som en cybertrussel, som på grundlag af sine tekniske karakteristika kan antages at have potentiale til at få alvorlig indvirkning på en udbyders net- og informationssystemer eller på brugerne af udbyderens tjenester ved at forårsage betydelig fysisk eller ikke fysisk skade.

Den foreslåede bestemmelse svarer til definitionen i NIS 2-direktivets artikel 6, nr. 11. Det forudsættes, at bestemmelsen forstås og fortolkes i overensstemmelse med direktivets definition.

Til § 3

Lov om sikkerhed i net og tjenester indeholder ikke en definition af væsentlige teleudbydere.

Efter NIS 2-direktivets artikel 3, stk. 1, litra a, anses enheder af en type, som er omhandlet i direktivets bilag I, og som overskrider tærsklerne for mellemstore virksomheder, der er fastsat i artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF, for at være væsentlige enheder.

Det følger af den foreslåede *§ 3, stk. 1,* at teleudbydere, der med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden, anses for at være væsentlige, hvis de opfylder mindst én af følgende betingelser: 1) udbyderen beskæftiger mere end 50 ansatte, eller 2) udbyderen har en årlig omsætning på over 10 mio. EUR og en årlig balance på over 10 mio. EUR.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra a, i NIS 2-direktivet.

Hvorvidt en enhed overskrider tærsklerne for mellemstore virksomheder efter den foreslåede bestemmelse, vil skulle vurderes ud fra de kriterier, der er fastsat i artikel 2, stk. 1, i bilaget til Europa-Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder. I artikel 2, stk. 1, i bilaget til henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder afgrænses kategorien af mikrovirksomheder, små og mellemstore virksomheder (SMV'er) som virksomheder, som beskæftiger under 250 personer, og har en årlig omsætning på ikke over 50 mio. EUR eller en årlig samlet balance på ikke over 43 mio. EUR.

Henstillingen må fortolkes således, at virksomheder falder inden for definitionen af mellemstore virksomheder, når virksomheden har 50 ansatte eller derover eller en årlig omsætning på 10 mio. EUR eller derover og en årlig balance på 10 mio. EUR eller derover. Der henvises i øvrigt til gennemgangen heraf i afsnit 3.1.3.

For at sikre, at enheder, der har partnervirksomheder eller er tilknyttede virksomheder, ikke betragtes som væsentlige enheder, hvor dette ville være uforholdsmæssigt, skal der i overensstemmelse med præambelbetragtning nr. 16 til NIS 2-direktivet tages hensyn til den grad af uafhængighed, som en enhed har i forhold til sine partnervirksomheder eller tilknyttede virksomheder. Der kan i denne forbindelse navnlig tages hensyn til, om en enhed er uafhængig af sine partnervirksomheder eller tilknyttede virksomheder med hensyn til de net- og informationssystemer, som enheden anvender i forbindelse med leveringen af sine tjenester og med hensyn til de tjenester, som enheden leverer.

På dette grundlag kan medlemsstaterne i overensstemmelse med præambelbetragtning nr. 16, hvor det er hensigtsmæssigt, anse en sådan enhed for ikke

at udgøre en mellemstor virksomhed i henhold til artikel 2, i bilaget til henstilling 2003/361/EF, eller for ikke at overskride tærsklerne for en mellemstor virksomhed fastsat i nævnte artikels stk. 1, hvis den pågældende enhed i betragtning af dennes grad af uafhængighed ikke ville være blevet anset for at udgøre en mellemstor virksomhed eller at overskride disse tærskler, hvis kun dens egne data var blevet taget i betragtning.

Det foreslås, at alene teleudbydere, der opfylder størrelseskravet, og som med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som deres hovedydelse, eller som en ikke-accessorisk del af virksomheden, anses for at være væsentlige.

Formålet med tilføjelsen af kravet om kommercielt formål og at udbuddet skal være en ikke accessorisk del af virksomheden er at sikre, at de nye skærpede regler efter NIS 2-direktivet ikke finder anvendelse for udbydere, der ikke meningsfuldt kan siges at falde ind under kategorien væsentlige teleudbydere efter NIS 2-direktivet.

Der henvises til den nærmere uddybning af lovens udbyderbegreb i afsnit 3.1.4.

Det foreslås i *stk. 2*¸ at uanset teleudbyderens størrelse, kan Center for Cybersikkerhed træffe afgørelse om, at følgende teleudbydere skal anses som væsentlige, hvis 1) teleudbyderen er den eneste udbyder i Danmark af et net eller en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter, 2) en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden., 3) en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne medføre en væsentlig systemisk risiko, herunder hvor en sådan forstyrrelse kan have en grænseoverskridende virkning, 4) teleudbyderen er kritisk på grund af udbyderens specifikke betydning på nationalt eller regionalt plan for sektoren eller typen af net eller tjeneste eller for andre indbyrdes afhængige sektorer i Danmark, 5) teleudbyderen er identificeret som en kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed.

Den foreslåede bestemmelse vil gennemføre artikel 3, stk. 1, litra c, litra e-f og artikel 2, stk. 2, litra b-e, i NIS 2-direktivet.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 3, stk. 1, litra c, litra e-f og artikel 2, stk. 2, litra b-e, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Formålet med bestemmelsen er, at det kan være svært for en teleudbyder selv at vurdere, om udbyderen af omfattet af kriterierne i de foreslående nr. 1)-5). Center for Cybersikkerhed kan derfor efter bestemmelsen træffe afgørelse herom.

Center for Cybersikkerhed kan således efter det foreslåede *nr. 1*, for det første lægge vægt på, om teleudbyderen, er den eneste udbyder i Danmark af et net eller en tjeneste, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter.

Bestemmelsen skal forstås således, at teleudbyderen skal være den reelt eneste udbyder i Danmark.

Center for Cybersikkerhed kan endvidere efter det foreslåede *nr. 2,* lægge vægt op, om en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne have væsentlig indvirkning på den offentlige sikkerhed eller folkesundheden.

Center for Cybersikkerhed kan efter det foreslåede *nr. 3,* lægge vægt på, om en forstyrrelse af det net eller den tjeneste, teleudbyderen leverer, vil kunne medføre en væsentlig systemisk risiko, herunder hvor en sådan forstyrrelse kan have en grænseoverskridende virkning.

Center for Cybersikkerhed kan efter det foreslåede *nr. 4,* lægge vægt på, om teleudbyderen er kritiske på grund af sin specifikke betydning på nationalt eller regionalt plan for sektoren eller type af net eller tjeneste eller for andre indbyrdes afhængige sektorer i Danmark.

Center for Cybersikkerhed skal efter det foreslåede *nr. 5,* lægge vægt på om teleudbyderen er identificeret som en kritisk enhed i henhold til lov om kritiske enheders modstandsdygtighed, anses for væsentlige teleudbydere.

Til § 4

Det følger af det foreslåede *stk. 1,* at teleudbydere, der ikke opfylder kriterierne for at være væsentlige udbydere efter lovens § 3, anses som vigtige teleudbydere, såfremt de med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske

kommunikationstjenester som deres hovedydelse, eller som en ikke accessorisk del af virksomheden.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 3, stk. 2, 1. pkt., som fastsætter, at enheder af en type omhandlet af direktivets bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til artikel 3, stk. 1, anses for at være vigtige enheder.

Teleudbydere, som med et kommercielt formål udbyder offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som en accessorisk del af virksomheden, herunder RLAN-udbydere, anses således ikke som vigtige teleudbydere.

Det følger af det foreslåede *stk. 2,* at Center for Cybersikkerhed efter en konkret vurdering kan træffe afgørelse om, at en teleudbyder, der er omfattet af § 3, stk. 2, nr. 1-4, skal anses som en vigtig teleudbyder.

Den foreslåede bestemmelse vil delvist gennemføre NIS 2-direktivets artikel 3, stk. 2, jf. artikel 3, stk. 1, litra e og g. Det følger af artikel 3, stk. 2, at enheder af en type omhandlet i direktivets bilag I eller II, der ikke opfylder kriterierne for at være væsentlige enheder i henhold til artikel 3, stk. 1, anses for at være vigtige enheder. Dette indbefatter enheder, som medlemsstaterne har identificeret som vigtige enheder i medfør af artikel 2, stk. 2, litra b-e.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerhed kan træffe afgørelse om, at en enhed, der er omfattet af loven på baggrund af de kvalitative kriterier i relation til deres samfundsmæssige betydning, jf. NIS 2-direktivets artikel 2, stk. 2, litra b-e, skal anses for at være en vigtig teleudbyder uanset udgangspunktet i det foreslåede § 3, stk. 2, nr. 1-4.

Såfremt en enhed i medfør af øvrige dele af lovforslagets § 3, herunder stk. 1, eller stk. 2, nr. 5, må anses for at være en væsentlig teleudbyder, vil der ikke kunne ske ændring af enhedens status fra væsentlig til vigtig efter den foreslåede bestemmelse.

Der henvises i øvrigt til afsnit 3.1 i lovforslagets almindelige bemærkninger.

Til § 5

Det følger af § 3, stk. 1, i lov om sikkerhed i net og tjenester, at Center for Cybersikkerhed fastsætter regler om minimumskrav til sikkerhed i net og tjenester for udbydere af offentligt tilgængelige elektroniske kommunika-

tionsnet og -tjenester og udbydere af NUIK-tjenester, herunder krav om passende tekniske, processuelle og organisatoriske foranstaltninger med henblik på risikostyring i forhold til sikkerhed i net og tjenester og opretholdelse af et passende sikkerhedsniveau, herunder krav om, at sådanne foranstaltninger gennemføres på baggrund af dokumenterede og ledelsesforankrede processer.

Det følger af den foreslåede *stk. 1,* at væsentlige og vigtige teleudbydere skal træffe passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal som minimum omfatte eller tage højde for: 1) politikker for risikoanalyse og informationssystemsikkerhed, 2) håndtering af hændelser, 3) driftskontinuitet, eksempelvis backup-styring og reetablering efter en katastrofe, og krisestyring, 4) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed 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 hos enheden, hvor det er relevant.

Den foreslåede bestemmelse vil gennemføre artikel 21, stk. 1-3, i NIS 2-direktivet.

Det fremgår af NIS 2-direktivets artikel 21, stk. 1, at medlemsstaterne skal sikre, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske, operationelle og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til deres operationer eller til at levere deres tjenester, og for at forhindre hændelser eller minimere deres indvirkning på modtagere af deres tjenester og på andre tjenester. Foranstaltningerne skal under hensyntagen til det aktuelle teknologiske stade og i givet fald til relevante europæiske og

internationale standarder samt gennemførelsesomkostningerne tilvejebringe et sikkerhedsniveau i net- og informationssystemer, der står i forhold til risiciene. Ved vurderingen af proportionaliteten af disse foranstaltninger skal der tages behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning.

Det fremgår af NIS 2-direktivets artikel 21, stk. 2, at de i stk. 1 omhandlede foranstaltninger skal baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatte følgende: a) Politikker for risikoanalyse og informationssystemsikkerhed, b) håndtering af hændelser, c) driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring, d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere, e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder, f) politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici, g) grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse, h) politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering, i) personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver og j) brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

Efter NIS 2-direktivets artikel 21, stk. 3, skal medlemsstaterne sikre, at enhederne, når de overvejer hvilke foranstaltninger efter artikel 21, stk. 2, litra d, om forsyningssikkerhed der er passende, 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 deres sikre udviklingsprocedurer. Enhederne skal desuden tage hensyn til resultaterne af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der kan foretages af Samarbejdsgruppen i samarbejde med Europa-Kommissionen og ENISA i overensstemmelse med NIS 2-direktivets artikel 22, stk. 1.

I overensstemmelse med direktivets forudsætninger, som udtrykt i præambelbetragtning nr. 83, 2. pkt., vil forpligtelsen til at indføre foranstaltninger til styring af cybersikkerhedsrisici finde anvendelse på væsentlige og vigtige

enheder, uanset om de selv vedligeholder deres net- og informationssystemer eller outsourcer vedligeholdelsen deraf.

I overensstemmelse med præambelbetragtning nr. 79 skal foranstaltningerne omfatte alle farer og sigte på at beskytte net- og informationssystemer og de pågældende systemers fysiske miljø mod enhver begivenhed såsom tyveri, brand, oversvømmelse, telekommunikations- eller strømsvigt, eller uautoriseret fysisk adgang til, beskadigelse af eller indgreb i en væsentlig eller vigtig enheds informations- og informationsbehandlingsfaciliteter, som kan kompromittere tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemerne. Foranstaltningerne bør derfor også adressere den fysiske og miljømæssige sikkerhed i net- og informationssystemerne ved at inkludere foranstaltninger til beskyttelse af sådanne systemer mod systemsvigt, menneskelige fejl, ondsindede handlinger eller naturfænomener i overensstemmelse med europæiske og internationale standarder såsom dem, der indgår i ISO/IEC 27000-serien.

Det følger af det foreslåede *stk. 2,* at en væsentlig eller vigtig teleudbyder, der finder, at den ikke overholder krav til foranstaltningerne i stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af stk. 3, uden unødigt ophold skal træffe alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 21, stk. 4. Efter NIS 2-direktivets artikel 21, stk. 4, skal medlemsstaterne sikre, at en enhed, der finder, at den ikke overholder foranstaltningerne i artikel 21, stk. 2, uden unødigt ophold træffer alle nødvendige, passende og forholdsmæssige korrigerende foranstaltninger.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 21, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse i stk. 2, understreger, at enheder skal handle på eventuelle konstateringer af mangler i overholdelsen af de krav til foranstaltninger, der følger af det foreslåede stk. 1, og regler om krav til foranstaltninger udstedt i medfør af det foreslåede stk. 3. Dette skal ses i sammenhæng med den foreslåede § 6 om ledelsens ansvar.

Det følger af det foreslåede *stk. 3*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om krav til foranstaltninger efter stk. 1, samt krav om yderligere foranstaltninger for teleudbydere omfattet af denne lov.

Den foreslåede bestemmelse indebærer, at ministeren for samfundssikkerhed og beredskab kan fastsættes nærmere regler om krav til de foranstaltninger til styring af sikkerhedsrisici, som væsentlige og vigtige teleudbydere skal træffe. Reglerne vil kunne stille mere konkretiserede krav til de foranstaltninger, som teleudbyderne skal træffe i medfør af den foreslåede bestemmelse i stk. 1, herunder fastsatte krav om yderligere foranstaltninger i telesektoren.

Dette omfatter bl.a. krav om foranstaltninger for i videst muligt omfang at sikre elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. Bestemmelsen viderefører således § 5, stk. 1, i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Bemyndigelsesbestemmelsen giver ministeren for samfundssikkerhed og beredskab mulighed for at fastsætte nærmere krav om foranstaltninger for samtlige teleudbydere, der er omfattet af lovens anvendelsesområde.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 21, stk. 5, 2. led, at Europa-Kommissionen kan vedtage gennemførelsesretsakter, der fastsætter de tekniske og metodologiske, samt om nødvendigt sektorspecifikke, krav til de i direktivets artikel 21, stk. 2, omhandlede foranstaltninger. Det vides endnu ikke, om Europa-Kommissionen vil vælge at vedtage gennemførelsesretsakter i medfør af artikel 21, stk. 5, 2. led, samt i givet fald indholdet heraf.

Det vil til enhver tid skulle sikres, at bekendtgørelser i medfør af det foreslåede stk. 3, harmonerer med eventuelle gennemførelsesretsakter fra Europa-Kommissionen. Såfremt der måtte være udstedt bekendtgørelser på et tidspunkt, hvor Europa-Kommissionen vedtager gennemførelsesretsakter, vil disse bekendtgørelser i relevant omfang skulle tilpasses eller efter omstændighederne ophæves.

Til § 6

Det foreslås i *stk. 1,* at de foranstaltninger, som en væsentlig eller en vigtig teleudbyder træffer på baggrund af forpligtelserne i § 5, stk. 1 og 2, samt

regler fastsat i medfør af § 5, stk. 3, skal være godkendt af teleudbyderens ledelsesorgan, samt at ledelsesorganet fører tilsyn med foranstaltningernes gennemførelse og sikrer, at foranstaltningerne har den fornødne effekt.

Den foreslåede bestemmelse i stk. 1, vil delvist gennemføre NIS 2-direktivets artikel 20, stk. 1. Det følger af NIS 2-direktivets artikel 20, stk. 1, at medlemsstaterne skal sikre, at de væsentlige og vigtige enheders ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med deres gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i den nævnte artikel. Dette berører dog ikke national ret for så vidt angår de ansvarsregler, der gælder for offentlige institutioner, samt ansvaret for embedsmænd og personer valgt eller udnævnt til offentlige hverv.

Den foreslåede bestemmelse i stk. 1 fastslår, at overholdelsen af forpligtelserne i den foreslåede § 5, stk. 1-3, er et ledelsesmæssigt ansvar.

Det følger af det foreslåede *stk. 2,* at medlemmerne af ledelsesorganet i en væsentlig eller vigtig teleudbyder skal deltage i relevante kurser om styring af informationssikkerhedsrisici og tilskynde til, at tilsvarende kurser tilbydes til ansatte i den væsentlige- eller en vigtige teleudbyder.

Den foreslåede bestemmelse i stk. 2 vil gennemføre NIS 2-direktivets artikel 20, stk. 2.

Det fremgår af NIS 2-direktivets artikel 20, stk. 2, at medlemsstaterne skal sikre, at medlemmerne af væsentlige og vigtige enheders ledelsesorganer er forpligtet til at følge kurser, og skal tilskynde væsentlige og vigtige enheder til løbende at tilbyde tilsvarende kurser til deres ansatte, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.

Henset til, at formålet med nærværende lov er at implementere NIS 2-direktivet gennem en integration med den eksisterende regulering på området, herunder navnlig lov om sikkerhed i net og tjenester, vurderes det, at kravet bør omfatte relevante kurser om styring af informationssikkerhedsrisici, og ikke kun cybersikkerhedsrisici, som forudsat i NIS 2-direktivet.

Til § 7

Det foreslås med *stk. 1,* at Center for Cybersikkerhed kan fastsætte regler om, at væsentlige- og vigtige teleudbydere skal anvende særlige IKT-produkter, -tjenester og -processer, som er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning for at påvise overensstemmelse med bestemte krav i § 6, stk. 1, eller regler om krav til foranstaltninger fastsat i medfør af § 6, stk. 3.

Bestemmelsen vil gennemføre artikel 24, stk. 1, i 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). Det følger af artikel 24, stk. 1, at for at påvise overensstemmelse med bestemte krav i direktivets artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici), kan medlemsstaterne kræve, at væsentlige og vigtige enheder bruger særlige IKT-produkter, -tjenester og -processer, der er udviklet af den væsentlige eller vigtige enhed, eller indkøbt fra tredjeparter, og som er certificeret i henhold til europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed). Endvidere skal medlemsstaterne tilskynde væsentlige og vigtige enheder til at anvende kvalificerede tillidstjenester.

Artikel 49 i nævnte forordning fastsætter nærmere regler om udarbejdelse, vedtagelse og revision af en europæisk cybersikkerhedscertificeringsordning.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 24, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger. De nærmere regler, der kan fastsættes i medfør af bestemmelsen, vil således skulle udarbejdes inden for denne ramme. Det indebærer bl.a., at reglerne vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at bestemmelsen i NIS 2-direktivets artikel 24, stk. 1, hvorefter IKT-produkter, -tjenester og -processer skal være udviklet af enhederne eller »indkøbt fra tredjeparter«, ikke er til hinder for, at der kan fastsættes regler om, at enhe-

derne skal bruge IKT-produkter, -tjenester og -processer, som stilles gratis til rådighed af tredjeparter.

Bestemmelsen skal i øvrigt ses i lyset af, at Europa-Kommissionen efter artikel 24, stk. 2, tillægges beføjelser til at vedtage delegerede retsakter for at supplere direktivet ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder, der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning. De delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer. I givet fald forudsættes det, at eventuelle allerede udstedte bekendtgørelser i relevant omfang tilpasses eller ophæves.

Til § 8

Det foreslås med *stk. 1,* at væsentlige- og vigtige teleudbydere skal registrere sig hos Center for Cybersikkerhed og i den forbindelse oplyse: 1) teleudbyderens navn, 2) adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre og 3) i givet fald en liste over de øvrige medlemsstater i Den Europæiske Union, hvor teleudbyderen leverer tjenester, der er omfattet af anvendelsesområdet i artikel 2 i Europa-Parlamentets og Rådets direktiv 2022/2555/EU 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).

Den foreslåede bestemmelse vil gennemføre artikel 27, stk. 2, i 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). Artikel 27, stk. 2, fastsætter bl.a., at medlemsstaterne pålægger DNS-tjenesteudbydere, topdomænenavneadministratorer, enheder, der leverer domænenavneregistreringstjenester og udbydere af cloudcomputingtjenester, af datacentertjenester, af indholdsleveringsnetværk, af administrerede tjenester, af administrerede sikkerhedstjenester, af onlinemarkedspladser, af onlinesøgemaskiner og af platforme for sociale netværkstjenester at indgive følgende oplysninger til de kompetente myndigheder: a) Enhedens navn, b) den relevante sektor og delsektor og typen af enhed, som i givet fald er omhandlet i direktivets bilag I eller II, c) adressen på enhedens hovedforretningssted og dens andre retlige forretningssteder i Unionen eller, hvis den

ikke er etableret i Unionen, på den repræsentant, der er udpeget i henhold til direktivets artikel 26, stk. 3, d) ajourførte kontaktoplysninger, herunder e-mailadresser og telefonnumre på enheden og i givet fald dens repræsentant udpeget i henhold til direktivets artikel 26, stk. 3, e) de medlemsstater, hvor enheden leverer tjenester og f) enhedens IP-intervaller.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 27, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der vil være tale om en oplysningspligt omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter finder anvendelse. Dette indebærer, at retten til ikke at inkriminere sig selv, jf. kapitel 4 i nævnte lov, skal overholdes. Det bemærkes dog, at det af bemærkningerne til § 10 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter fremgår, at »[b]estemmelsen [om forbud mod selvinkriminering] er ikke til hinder for, at den mistænkte kan pålægges at give (faktuelle) oplysninger, som er uden betydning for bedømmelsen af, hvorvidt den pågældende har begået en lovovertrædelse, der kan medføre straf. Bestemmelsen vil således ikke være til hinder for at anvende en oplysningspligt til at kræve oplysninger om navn, adresse mv., jf. herved også retsplejelovens § 750, hvorefter enhver på forlangende er forpligtet til over for politiet at opgive navn, adresse og fødselsdato.« Der henvises til Folketingstidende 2003-04, tillæg A, side 3097. Der vil med den foreslåede bestemmelse være tale om en registreringspligt, hvorved enheder skal afgive en række helt overordnede oplysninger om bl.a. navn, adresse og enhedstype. Det er derfor Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter alene vil være relevant i praksis i yderst sjældne tilfælde.

Det foreslås i *stk. 2*, at oplysningerne efter stk. 1, skal indgives senest den 1. oktober 2025. En væsentlig eller en vigtig teleudbyder, der omfattes af lovens anvendelsesområde efter denne dato, skal indgive oplysningerne senest to uger efter, at teleudbyderen omfattes af loven.

Bestemmelsen vil gennemføre dele af artikel 27, stk. 2, i NIS 2-direktivet, som bl.a. fastslår, at oplysningerne skal indgives til de kompetente myndigheder senest den 17. januar 2025. Det bemærkes dog, at den seneste dato for

registreringspligten foreslås at være den 1. oktober 2025. Dette vil sikre, at den seneste dato for registreringspligten ligger efter, at loven er trådt i kraft.

Det foreslås i *stk. 3,* at tilfælde af ændring i de oplysninger, der er afgivet i medfør af stk. 1, skal den væsentlige- eller vigtige teleudbyder give Center for Cybersikkerhed underretning herom senest to uger efter datoen for ændringen.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 27, stk. 3, som fastsætter en forpligtelse for medlemsstaterne til at sikre, at de nævnte enheder straks og under alle omstændigheder senest tre måneder efter den dato, hvor ændringen trådte i kraft, underretter den kompetente myndighed om enhver ændring af de oplysninger, de har indsendt i henhold til artikel 27, stk. 2.

Den foreslåede bestemmelse svarer indholdsmæssigt til dele af NIS 2-direktivets artikel 27, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *stk. 4,* at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om hvilke yderligere oplysninger væsentlige og vigtige teleudbydere skal afgive ved registrering.

Bestemmelsen har til formål at give ministeren for samfundssikkerhed og beredskab mulighed for at fastsætte nærmere regler om oplysningspligter, herunder eksempelvis oplysningspligter i forbindelse med bl.a. beredskabskontakt og operative hændelser.

Det foreslås i *stk. 5*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige og vigtige teleudbydere, herunder krav om 1) afgivelse af oplysninger om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf og 2) krav om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, herunder regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

Bestemmelsen viderefører § 4, nr. 1-2, i lov om sikkerhed i net og tjenester, og skal fortolkes i overensstemmelse hermed.

Den foreslåede oplysningspligt vil indebære, at teleudbydere efter anmodning skal afgive oplysninger om de dele af deres net eller tjenester – eller driften heraf – der anses som væsentlige. Det kan f.eks. være oplysninger om, hvilke leverandører som teleudbyderen anvender. Dermed sikres det, at Center for Cybersikkerhed kan få det nødvendige overblik over de centrale dele af teleinfrastrukturen.

Oplysningspligten foreslås – ligesom tilfældet er i dag – suppleret af en underretningspligt, som indebærer, at teleudbydere skal underrette Center for Cybersikkerhed i forbindelse med påtænkte indgåelser af visse større aftaler om leverancer af hardware, firmware eller software samt driften heraf. Teleudbyderne skal endvidere indsende det endelige aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelsen af aftalen. I den forbindelse påtænkes der indført en kort standstill-periode, således at Center for Cybersikkerhed kan foretage en vurdering af aftaleudkastet. Standstill-periodens korte varighed sikrer, at aftaleindgåelsen ikke forsinkes unødigt.

Formålet med ordningen er at give Center for Cybersikkerhed mulighed for at rådgive teleudbyderen om særlige trusler mod informationssikkerheden samt om mulighederne for at imødegå de trusler, som det pågældende aftaleudkast vurderes at indebære. Det vurderes, at dette ville bidrage til, at teleudbyderne får bedre forudsætninger for at vurdere mulige risici ved den påtænkte aftale, således at teleudbyderne kan tage højde herfor inden aftaleindgåelsen.

Til § 9

Det foreslås i *stk. 1*, at teleudbydere uden unødigt ophold skal underrette Center for Cybersikkerhed og CSIRT'en om enhver væsentlig hændelse. En underretning skal indeholde oplysninger, der gør det muligt at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Den foreslåede bestemmelse vil gennemføre artikel 23, stk. 1, i NIS 2-direktivet.

Det følger bl.a. af NIS 2-direktivets artikel 23, stk. 1, at hver medlemsstat sikrer, at væsentlige og vigtige enheder uden unødigt ophold underretter dens CSIRT eller i givet fald dens kompetente myndighed om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester. Hver medlemsstat sikrer, at enhederne indberetter alle oplysninger, der gør det muligt for CSIRT'en eller den kompetente myndighed at fastslå eventuelle grænseoverskridende virkninger af hændelsen.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 23, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at samtlige teleudbydere, der er omfattet af lovens anvendelsesområde, skal underrette både Center for Cybersikkerhed og CSIRT'en i tilfælde af hændelser, der har en væsentlig indvirkning på levering af deres tjenester. Dermed sikres det, at både Center for Cybersikkerhed og CSIRT'en hurtigt og effektivt vil kunne varetage sine myndighedsopgaver.

I overensstemmelse med præambelbetragtning nr. 83 vil den foreslåede forpligtelse til at foretage underretning ved hændelser finde anvendelse på de væsentlige og vigtige teleudbydere, uanset om disse teleudbydere selv vedligeholder deres net- og informationssystemer eller outsourcer vedligeholdelsen deraf. Såfremt der måtte ske en hændelse i et net- og informationssystem, som eksempelvis er outsourcet, vil det derfor fortsat være den væsentlige eller vigtige teleudbyders ansvar, at der sker underretning i fornødent omfang.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der vil være tale om en oplysningspligt omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter finder anvendelse. Dette indebærer bl.a., at kapitel 4 (om retten til ikke at inkriminere sig selv mv.) vil gælde i tilfælde, hvor der måtte være en konkret mistanke om, at en enhed har begået en overtrædelse af lovgivningen, der kan medføre straf. Der henvises i øvrigt til kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter og bemærkningerne hertil. Der henvises til Folketingstidende 2003-04, tillæg A, side 3075-3078 og side 3096-3099.

Såfremt en væsentlig hændelse, der underrettes om i medfør af bestemmelsen, måtte have grænseoverskridende virkning, vil CSIRT'en i ovenstemmelse med forudsætningen i NIS 2-direktivets artikel 23, stk. 6, via det centrale kontaktpunkt uden unødigt ophold skulle underrette de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse, navnlig hvor den væsentlige hændelse berører to eller flere medlemsstater. Efter samme bestemmelse vil en sådan information omfatte den type af oplysninger, der er modtaget i overensstemmelse med artikel 23, stk. 4, og CSIRT'en vil i den forbindelse – i overensstemmelse med EU-retten eller national ret – sikre

enhedens sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

Det følger af det foreslåede *stk. 2,* at en hændelse anses for at være væsentlig, hvis den 1) har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af net eller tjenester eller økonomiske tab for den berørte udbyder, eller 2) har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig fysisk eller ikke fysisk skade.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 3, som fastslår, at en hændelse anses for at være væsentlig, hvis: a) den har forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller b) den har påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

Den foreslåede bestemmelse svarer med en enkelt sproglig konsekvensrettelse uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det følger af det foreslåede *stk. 3,* at Center for Cybersikkerhed kan fastsætte nærmere regler om, hvornår en hændelse anses for at være væsentlig samt hvilke oplysninger, der skal gives i forbindelse med underretningen.

Henset til at kriterierne for, hvornår en hændelse anses for at være væsentlig efter det foreslåede stk. 2, har en kvalitativ og skønspræget karakter, vurderes det hensigtsmæssigt, at Center for Cybersikkerhed kan fastsættes nærmere regler, som præciserer, hvornår en hændelse anses for at være væsentlig i telesektoren.

Til § 10

Det foreslås i *stk. 1*, at underretningen efter § 9, stk. 1, skal ske på følgende måde 1) en tidlig varsling, som skal angive, om den væsentlige hændelse mistænkes at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, sendes uden unødigt ophold og under alle omstændigheder inden for 24 timer efter, at enheden har fået kendskab til den væsentlige hændelse, 2) en hændelsesunderretning, som skal ajourføre oplysningerne fra den tidlige varsling, jf. nr. 1, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger,

sendes uden unødigt ophold og under alle omstændigheder inden for 72 timer efter, at enheden har fået kendskab til den væsentlige hændelse, jf. dog stk. 2, 3) en foreløbig rapport med relevante statusopdateringer sendes efter anmodning fra CSIRT'en, 4) en endelig rapport sendes senest en måned efter fremsendelsen af den hændelsesunderretning, der er omhandlet i nr. 2. Rapporten skal indeholde 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 og d) de eventuelle grænseoverskridende virkninger af hændelsen, og 5) såfremt hændelsen fortsat pågår på tidspunktet for fremsendelsen af den endelige rapport, jf. nr. 4, skal den berørte enhed forelægge en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter, at hændelsen er håndteret.

Bestemmelsen vil gennemføre artikel 23, stk. 4, i NIS 2-direktivet.

Artikel 23, stk. 4, fastsætter, at medlemsstaterne sikrer, at de berørte enheder med henblik på den i artikel 23, stk. 1, omhandlede underretning fremsender følgende til CSIRT'en eller i givet fald den kompetente myndighed: a) Uden unødigt ophold og under alle omstændigheder inden for 24 timer efter at have fået kendskab til den væsentlige hændelse en tidlig varsling, som i givet fald skal angive, om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger eller kunne have en grænseoverskridende virkning, b) uden unødigt ophold og under alle omstændigheder inden for 72 timer efter at have fået kendskab til den væsentlige hændelse, en hændelsesunderretning, som i givet fald skal ajourføre de oplysninger, der er omhandlet under litra a, og give en indledende vurdering af den væsentlige hændelse, herunder dens alvor og indvirkning samt kompromitteringsindikatorerne, hvor sådanne foreligger, c) efter anmodning fra en CSIRT eller den kompetente myndighed en foreløbig rapport om relevante statusopdateringer, d) en endelig rapport senest en måned efter forelæggelsen af den i litra b omhandlede hændelsesunderretning, der skal omfatte følgende: i) En detaljeret beskrivelse af hændelsen, herunder dens alvor og indvirkning, ii) den type trussel eller grundlæggende årsag, der sandsynligvis har udløst hændelsen, iii) anvendte og igangværende afbødende foranstaltninger og iv) i givet fald de grænseoverskridende virkninger af hændelsen og e) i tilfælde af at en hændelse pågår på tidspunktet for indgivelsen af den i litra d, omhandlede endelige rapport, sikrer medlemsstaterne, at berørte enheder forelægger en statusrapport på det pågældende tidspunkt og en endelig rapport senest en måned efter deres håndtering af hændelsen.

Den foreslåede bestemmelse svarer med enkelte sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 4, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Med den foreslåede bestemmelse fastlægges der en flertrinstilgang for underretninger om væsentlige hændelser.

Væsentlige og vigtige teleudbydere vil indledningsvist være forpligtet til at indgive en tidlig varsling uden unødigt ophold og under alle omstændigheder inden for 24 timer efter, at de bliver opmærksomme på en væsentlig hændelse.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 102 vil den tidlige varsling alene skulle indeholde de oplysninger, der er nødvendige for at gøre CSIRT'en og den relevante kompetente myndighed opmærksom på den væsentlige hændelse og give enheden mulighed for om nødvendigt at anmode om assistance. En sådan tidlig varsling bør endvidere, hvis det er relevant, angive om den væsentlige hændelse mistænkes for at være forårsaget af ulovlige eller ondsindede handlinger, og om den sandsynligvis vil have grænseoverskridende virkninger.

Den tidlige varsling vil skulle efterfølges af en hændelsesunderretning, som bl.a. skal ajourføre oplysningerne fra den tidlige varsling. Denne hændelsesunderretning skal sendes uden unødigt ophold og senest inden for 72 timer efter, at en enhed har fået kendskab til den væsentlige hændelse.

CSIRT'en kan på baggrund af hændelsesunderretningen anmode om en foreløbig rapport med relevante statusopdateringer. Indholdet i den foreløbige rapport vil afhænge af hændelsens nærmere omstændigheder.

Den berørte teleudbyder vil skulle sende en endelig rapport senest en måned efter forelæggelsen af hændelsesunderretningen efter den foreslåede § 10, stk. 1, nr. 2. I tilfælde af at hændelsen fortsat er igangværende på tidspunktet for indgivelsen af den endelige rapport, skal den berørte teleudbyder forelægge en statusrapport for CSIRT'en og Center for Cybersikkerhed. Den endelige rapport vil i så fald skulle indgives senest en måned efter, at enheden har håndteret den væsentlige hændelse.

Efter NIS 2-direktivets præambelbetragtning nr. 101 er formålet med denne flertrinstilgang at finde den rette balance mellem på den ene side hurtig underretning, der vil bidrage til at afbøde den potentielle spredning af væsentlige hændelser og give væsentlige og vigtige enheder mulighed for at søge

assistance, og på den anden side en dybdegående underretning, der gør det muligt at høste erfaringer af individuelle hændelser.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at der vil være tale om en oplysningspligt omfattet af lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter finder anvendelse. Dette indebærer bl.a., at kapitel 4 (om retten til ikke at inkriminere sig selv mv.) vil gælde i tilfælde, hvor der måtte være en konkret mistanke om, at en enhed har begået en overtrædelse af lovgivningen, der kan medføre straf. Der henvises i øvrigt til kapitel 4 i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter og bemærkningerne hertil. Der henvises til Folketingstidende 2003-04, tillæg A, side 3075-3078 og side 3096-3099.

I overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 102 vil det skulle sikres, at forpligtelsen til at indgive den tidlige varsling eller den efterfølgende hændelsesunderretning ikke medfører, at den underrettende enhed skal bruge færre ressourcer på aktiviteter vedrørende håndtering af hændelsen. Enhedens ressourcer bør således prioriteres, så det forhindres, at forpligtelser vedrørende hændelsesrapportering enten omdirigerer ressourcer fra håndtering af væsentlige hændelser eller på anden måde kompromitterer enhedens indsats i denne henseende.

Det forudsættes på denne baggrund, at det sikres, at underretningen kan ske på en så ressourcebesparende måde som muligt, eksempelvis ved at anvende én fælles digital løsning, jf. den foreslåede bestemmelse i § 32.

Det følger af det foreslåede *stk. 2,* at Center for Cybersikkerhed og CSIRT'en sikrer, at den underrettende teleudbyder uden unødigt ophold og, hvor det er muligt, inden for 24 timer efter modtagelsen af den tidlige varsling, gives et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse. Efter anmodning fra teleudbyderen skal CSIRT'en desuden yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger og supplerende teknisk bistand.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 23, stk. 5, som bl.a. fastsætter, at CSIRT'en eller den relevante kompetente myndighed uden unødigt ophold, og hvor det er muligt, inden for 24 timer efter modtagelsen af den i stk. 4, litra a, omhandlede tidlige varsling giver den underrettende enhed et svar, herunder indledende tilbagemeldinger om den væsentlige hændelse og, efter anmodning fra enheden, vejledning eller operativ rådgivning om gennemførelsen af mulige afbødende foranstaltnin-

ger. CSIRT'en yder supplerende teknisk bistand, hvis den berørte teleudbyder anmoder herom. Hvor den væsentlige hændelse mistænkes for at være af strafferetlig karakter, giver CSIRT'en eller Center for Cybersikkerhed også vejledning om underretning om den væsentlige hændelse til retshåndhævende myndigheder.

Den foreslåede bestemmelse svarer med enkelte sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indeholder en forpligtelse for CSIRT'en til at sikre, at der hurtigt gives svar på de tidlige varslinger, som den modtager fra teleudbydere, og i denne forbindelse give indledende tilbagemeldinger om den væsentlige hændelse.

Svar og tilbagemeldinger vil kunne gives af CSIRT'en selv eller Center for Cybersikkerhed. Svar og tilbagemeldinger vil bl.a. kunne bestå i, at der gives vejledning om mulige afværgeforanstaltninger, om anden relevant viden, som CSIRT'en eller Center for Cybersikkerhed er i besiddelse af, eller om anmeldelse til politiet, såfremt den væsentlige hændelse mistænkes for at udgøre en strafbar handling. Derimod er det ikke hensigten, at CSIRT'en eller Center for Cybersikkerhed, som afgiver svaret, skal tilvejebringe oplysninger fra tredjemand.

Efter bestemmelsen vil CSIRT'en desuden efter anmodning fra teledbyderen skulle yde vejledning, operativ rådgivning om gennemførelsen af mulige afbødende foranstaltninger eller supplerende teknisk bistand.

Det bemærkes i den forbindelse, at hvis en hændelse efterforskes som et strafbart forhold, vil der skulle tages højde for, at de opfølgende oplysninger ikke må vanskeliggøre eller forhindre efterforskningen.

Til § 11

Det følger af den foreslåede bestemmelse i *stk. 1*, at teleudbydere kan underrette Center for Cybersikkerhed og CSIRT'en om hændelser, der ikke er omfattet af lovens § 9, nærvedhændelser og cybertrusler.

Bestemmelsen vil gennemføre artikel 30, stk. 1, i NIS 2-direktivet, som fastsætter en forpligtelse for medlemsstaterne til at sikre, at der ud over underretningsforpligtelsen i artikel 23 kan indgives underretninger til CSIRT'en eller i givet fald de kompetente myndigheder på frivillig basis af: a) væsent-

lige og vigtige enheder for så vidt angår hændelser, cybertrusler og nærvedhændelser og 2) enheder, udover dem der er omhandlet i litra a), uanset om de er omfattet af dette direktivs anvendelsesområde, for så vidt angår væsentlige hændelser, cybertrusler og nærvedhændelser.

Den foreslåede bestemmelse svarer indholdsmæssigt til bestemmelsen i NIS 2-direktivets artikel 30, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Underretning af CSIRT'en og Center for Cybersikkerhed ved større sikkerhedshændelser skaber gode forudsætninger for, at CSIRT'en og Center for Cybersikkerhed kan udnytte erfaringer med cybertrusler og sikkerhedsrisici på tværs af samfundet – og dermed skabe et samlet overblik over den aktuelle sikkerhedstilstand på den danske del af internettet. Underretninger sætter således CSIRT'en og Center for Cybersikkerhed i stand til at varsle hurtigere om trusler og styrke grundlaget for rådgivningen om risici og passende sikkerhedstiltag.

Den foreslåede bestemmelse indebærer, at alle teleudbydere kan underrette Center for Cybersikkerhed og CSIRT'en om hændelser, nærvedhændelser og cybertrusler.

Det følger af den foreslåede *stk. 2,* at Center for Cybersikkerhed og CSIRT'en behandler underretninger efter stk. 1 på samme måde som underretninger modtaget i medfør af § 10. CSIRT'en kan prioritere håndteringen af underretninger, der er modtaget i medfør af § 9.

Bestemmelsen vil gennemføre artikel 30, stk. 2, i NIS 2-direktivet. Det følger af NIS 2-direktivets artikel 30, stk. 2, at medlemsstaterne behandler de i artiklens stk. 1 omhandlede underretninger i overensstemmelse med proceduren, der er fastsat i artikel 23. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger. Hvor det er nødvendigt, giver CSIRT'erne og i givet fald de kompetente myndigheder det centrale kontaktpunkt de oplysninger om underretninger, de har modtaget i medfør af denne artikel, samtidig med at de sikrer fortroligheden og passende beskyttelse af de oplysninger, der er afgivet af den underrettende enhed. Uden at det berører forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, må frivillig rapportering ikke medføre, at den underrettende enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde foretaget underretningen.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til bestemmelsen i NIS 2-direktivets artikel 30, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at CSIRT'en og Center for Cybersikkerhed vil skulle behandle frivillige underretninger, der er indgivet i medfør af den foreslåede bestemmelse i § 11, stk. 1, efter procedurebestemmelsen i den foreslåede § 10. De forpligtelser for myndigheder, der er angivet i § 10 og bemærkningerne hertil, vil således også gælde for underretninger, der indgives i medfør af den foreslåede bestemmelse i § 11, stk. 1.

Det bemærkes, at den foreslåede bestemmelse ikke indebærer, at teleudbyderen er forpligtet til at følge proceduren efter den foreslåede bestemmelse i § 10, når der indgives underretning efter den foreslåede § 11, stk. 1.

Den foreslåede bestemmelse indebærer desuden, at CSIRT'en kan prioritere at håndtere de underretninger, der er modtaget i medfør af § 11, før CSIRT'en og Center for Cybersikkerhed behandler de underretninger, der er modtaget i medfør af § 9, stk. 1.

Til § 12

Det følger af det foreslåede *stk. 1,* at teleudbydere i relevant omfang uden unødigt ophold underretter modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af deres tjenester negativt.

Bestemmelsen vil gennemføre artikel 23, stk. 1, 2. pkt., i NIS 2-direktivet, som fastsætter en forpligtelse for medlemsstaterne til at sikre, at væsentlige og vigtige enheder i relevant omfang underretter modtagerne af deres tjenester om væsentlige hændelser, der sandsynligvis vil påvirke leveringen af disse tjenester negativt.

Den foreslåede bestemmelse svarer indholdsmæssigt til bestemmelsen i NIS 2-direktivets artikel 23, stk. 1, 2. pkt., og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog med den ændring, at kravet om underretning ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og informationer finder anvendelse for samtlige teleudbydere. Henset til det ak-

tuelle trusselsbillede, vurderer ministeriet for samfundssikkerhed og beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Bestemmelsen indebærer en forpligtelse for teleudbydere til at underrette modtagerne af deres tjenester om en væsentlig hændelse. Underretning af modtagerne vil alene skulle ske i relevant omfang. Det indebærer, at teleudbyderne vil kunne undlade at foretage underretning af modtagerne ud fra en konkret vurdering af, at underretningen ikke vil være i modtagernes interesse.

Om en hændelse er at anse for væsentlig vurderes ud fra den foreslåede bestemmelse i § 9, stk. 2, og ud fra regler, der måtte være udstedt i en given sektor i medfør af § 9, stk. 3.

Der stilles ingen formkrav til underretningen, og de pågældende teleudbydere vil derfor have metodefrihed i forhold til, hvordan underretningen af modtagerne vil skulle ske, idet det dog forudsættes, at underretningen skal være umiddelbart tilgængelig for de relevante modtagere og kommunikeres på et letforståeligt sprog.

Det følger af det foreslåede *stk. 2,* at teleudbydere oplyser uden unødigt ophold modtagerne af deres tjenester, som potentielt er berørt af en væsentlig hændelse, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende hændelse. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om den væsentlige hændelse.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 23, stk. 2, der fastsætter en forpligtelse for medlemsstaterne til at sikre, at væsentlige og vigtige enheder i givet fald uden unødigt ophold meddeler modtagerne af deres tjenester, som potentielt kan være berørt af en væsentlig cybertrussel, eventuelle foranstaltninger eller modforholdsregler, som disse modtagere kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal enhederne også informere de pågældende modtagere om selve den væsentlige trussel.

Den foreslåede bestemmelse svarer indholdsmæssigt til bestemmelsen i NIS 2-direktivets artikel 23, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog med den ændring, at kravet om underretning ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og informationer finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer ministeriet for samfundssikkerhed og beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Den foreslåede bestemmelse indebærer i overensstemmelse med NIS 2-direktivets præambelbetragtning nr. 103, bl.a. at væsentlige og vigtige enheder uden unødigt ophold vil skulle underrette modtagerne af deres tjenester om enhver foranstaltning eller modforholdsregel, som modtagerne kan træffe for at afbøde risici fra en væsentlig hændelse. Teleudbyderen vil desuden, hvor det er hensigtsmæssigt skulle informere deres tjenestemodtagere om selve hændelsen. Kravet om at informere modtagerne bør opfyldes efter bedste evne, men vil ikke fritage teleudbyderne for forpligtelsen til at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe enhver hændelse og genoprette tjenestens normale sikkerhedsniveau.

I overensstemmelse med præambelbetragtning nr. 103 indebærer bestemmelsen endvidere, at oplysninger om væsentlige cybertrusler skal stilles gratis til rådighed for modtagerne i et let forståeligt sprog

Der stilles i øvrigt ingen formkrav til oplysningen, og de pågældende teleudbyderne vil derfor have metodefrihed i forhold til, hvordan underretningen af modtagerne vil skulle ske.

Til § 13

Det foreslås i *stk. 1,* at Center for Cybersikkerhed efter høring af en teleudbyder, der er ramt af en væsentlig hændelse, jf. § 9, kan informere offentligheden om den væsentlige hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse.

Bestemmelsen vil delvist gennemføre artikel 23, stk. 7, i NIS 2-direktivet.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer – med visse sproglige tilpasninger uden indholdsmæssig betydning – til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog således, at bestemmelsen ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og informationer finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer ministeriet for samfundssikkerhed og beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerhed kan informere offentligheden om en væsentlig hændelse, hvis offentliggørelsen er nødvendig for at forebygge eller håndtere hændelsen, eller hvor offentliggørelsen af hændelsen på anden vis er i offentlighedens interesse.

Center for Cybersikkerhed vil i medfør af bestemmelsen skulle høre den berørte enhed, før der sker offentliggørelse af hændelsen.

Formålet med høringen vil være at sikre, at Center for Cybersikkerhed kan træffe afgørelse om offentliggørelse på et oplyst grundlag, herunder foretage en afvejning af hensynet til den konkrete enhed over for hensynet til orientering af offentligheden.

Det vil være op til Center for Cybersikkerhed at tage stilling til formen for orienteringen. Orientering af offentligheden kan således ske på den måde, som Center for Cybersikkerhed finder bedst egnet under hensyn til den berørte enhed, hændelsens karakter, den geografiske udstrækning, den forventede betydning for bestemte dele af offentligheden mv.

Det vil i den forbindelse skulle sikres, at offentligheden informeres på en ansvarlig måde, som ikke kompromitterer fortrolige oplysninger. Det bemærkes, at den kompetente myndighed vil skulle sikre, at de hensyn til fortrolighed, der fremgår af i forvaltningslovens § 27 om offentligt ansattes tavshedspligt, iagttages. Dette omfatter bl.a. hensynet til enkeltpersoners private forhold, forretningshemmeligheder samt hensynet til forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Det foreslås, at det som udgangspunkt er Center for Cybersikkerhed, og ikke CSIRT'en, der foretager offentliggørelsen af en væsentlig hændelse, jf. dog det foreslåede stk. 3, idet Center for Cybersikkerhed vil være nærmest til at

foretage afvejningen af teleudbyderens eventuelle interesse i, at der ikke sker offentliggørelse, over for hensynet til offentligheden.

Det følger af den foreslåede bestemmelse i *stk. 2*, at den Center for Cybersikkerhed i de situationer, der er nævnt i stk. 1, kan kræve, at den relevante enhed informerer offentligheden om en væsentlig hændelse.

Bestemmelsen vil delvist gennemføre NIS 2-direktivets artikel 23, stk. 7.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger, dog med den ændring, at bestemmelsen ikke alene gælder for væsentlige og vigtige teleudbydere, men for samtlige teleudbydere, der er omfattet af nærværende lov.

Dette skal navnlig ses i lyset af, at den gældende lov om sikkerhed i net og informationer finder anvendelse for samtlige teleudbydere. Henset til det aktuelle trusselsbillede, vurderer ministeriet for samfundssikkerhed og beredskab, at det nuværende sikkerhedsniveau bør opretholdes.

Center for Cybersikkerhed vil skulle foretage høring af den berørte teleudbyder, før der træffes afgørelse om, at teleudbyderen skal offentliggøre hændelsen, i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåede stk. 1. I forbindelse med en afgørelse om offentliggørelse vil den kompetente myndighed endvidere skulle varetage de fortrolighedshensyn, der ligeledes er beskrevet i bemærkningerne til det foreslåede stk. 1.

Det følger af det foreslåede *stk. 3,* at CSIRT'en efter samme kriterier som i stk. 1, kan informere offentligheden om væsentlige hændelser, der kan påvirke mere end én sektor.

Bestemmelsen vil delvist gennemføre NIS 2-direktivets artikel 23, stk. 7.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at det vil være CSIRT'en, der informerer offentligheden om væsentlige hændelser, når disse kan påvirke flere sektorer, idet det typisk vil være CSIRT'en, der har viden om, at en hændelse rammer flere sektorer eller har potentialet til at ramme flere sektorer.

CSIRT'en vil skulle foretage høring af den berørte teleudbyder, før der træffes afgørelse om, at teleudbyderen skal offentliggøre hændelsen, i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåede stk. 1. I forbindelse med en afgørelse om offentliggørelse vil CSIRT'en endvidere skulle varetage de fortrolighedshensyn, og forvaltningslovens regler om tavshedspligt der ligeledes er beskrevet i bemærkningerne til det foreslåede stk. 1.

Herudover forudsættes det, at der sker en tæt koordination mellem CSIRT'en og Center for Cybersikkerhed forud for eventuel offentliggørelse af en væsentlig hændelse.

Det følger af det foreslåede *stk. 4,* at CSIRT'en efter samme kriterier som i stk. 1, kan informere offentligheden om væsentlige hændelser i andre medlemsstater.

Bestemmelsen vil delvist gennemføre NIS 2-direktivets artikel 23, stk. 7.

Det fremgår af NIS 2-direktivets artikel 23, stk. 7, at hvor offentlighedens kendskab er nødvendig for at forebygge en væsentlig hændelse eller for at håndtere en igangværende hændelse, eller hvor offentliggørelse af den væsentlige hændelse på anden vis er i offentlighedens interesse, kan en medlemsstats CSIRT eller i givet fald dens kompetente myndighed, og hvor det er relevant CSIRT'erne eller de kompetente myndigheder i andre berørte

medlemsstater, efter høring af den berørte enhed informere offentligheden om den væsentlige hændelse eller kræve, at enheden gør det.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydningtil NIS 2-direktivets artikel 23, stk. 7, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at CSIRT'en efter høring af en enhed i en anden medlemsstat, hvor teleudbyderen er ramt af en væsentlig hændelse, kan informere offentligheden i Danmark om den væsentlige hændelse.

Det er et krav, at offentliggørelsen er nødvendig for at forebygge eller håndtere en lignende hændelse i Danmark, eller at offentliggørelsen på anden vis er i den danske offentligheds interesse. En sådan situation vil eksempelvis foreligge, hvis CSIRT'en vurderer, at den konkrete væsentlige hændelse kan have grænseoverskridende virkning, og at det derfor er nødvendigt at orientere offentligheden, således at der i Danmark kan træffes de fornødne forebyggende foranstaltninger eller modforholdsregler.

Før der træffes afgørelse om, at teleudbyderen skal offentliggøre hændelsen, vil CSIRT'en skulle foretage høring af den berørte teleudbyder i overensstemmelse med proceduren beskrevet i bemærkningerne til det foreslåedes stk. 1. Det forudsættes dog, at høringen af teleudbyderen vil ske via det centrale kontaktpunkt i den pågældende medlemsstat. I forbindelse med en afgørelse om offentliggørelse vil CSIRT'en endvidere skulle varetage de fortrolighedshensyn og forvaltningslovens regler om tavshedspligt, der er beskrevet i bemærkningerne til det foreslåede stk. 1.

Til § 14

Det foreslås i *stk. 1,* at Center for Cybersikkerhed koordinerer og prioriterer beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer.

Bestemmelsen viderefører indholdet af § 5, stk. 3, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med vi-

dereførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Bemyndigelsen i § 5, stk. 3, er udmøntet i bekendtgørelse nr. 261 af 22. februar 2021 om beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer mv.

Bestemmelsen i § 5, stk. 3, gennemfører i øvrigt delvist artikel 108 i EU's telekodeks. Artikel 108 berøres ikke af NIS 2-direktivet.

Ordningen er en del af den samlede beredskabsplanlægning inden for den civile sektor. Det følger således af § 24, stk. 1, i beredskabsloven, jf. lovbekendtgørelse nr. 314 af 3. april 2017 med senere ændringer, at hver enkelt minister inden for sit område skal planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, herunder udarbejde beredskabsplaner.

Bestemmelsens anvendelsesområde omfatter beredskabssituationer samt andre ekstraordinære situationer. Dette omfatter såvel situationer med krigshandlinger som situationer, hvor det som følge af en større ulykke, katastrofe eller anden ekstraordinær hændelse eller krise er nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at opretholde samfundets funktioner. Bestemmelsens anvendelsesområde omfatter således både naturskabte og menneskeskabte ulykker og katastrofer, herunder eksempelvis orkan- og stormflodssituationer og alvorlige cyberangreb.

Den foreslåede bestemmelse vedrører koordinering og prioritering af de forskellige beredskabsaktørers behov for elektronisk kommunikation i beredskabssituationer og i andre ekstraordinære situationer. En sådan koordinering og prioritering vil ofte være nødvendigt i beredskabssituationer og i andre ekstraordinære situationer, hvor der kan opstå kapacitetsproblemer eller beskadigelse af teleinfrastrukturen.

Ved beredskabsaktører forstås myndigheder, virksomheder og institutioner som skal bidrage til opretholdelse af samfundets funktioner i en beredskabssituation eller i en anden ekstraordinær situation.

Bestemmelsen indebærer, at Center for Cybersikkerhed fortsat varetager den overordnede krisestyring i forhold til telesektoren. Center for Cybersikkerhed skal i den forbindelse i beredskabssituationer eller i andre ekstraordinære situationer være bindeled mellem beredskabsaktører og væsentlige

teleudbydere samt vigtige erhvervsmæssige teleudbydere og søge at tilgodese eller prioritere mellem beredskabsaktørernes behov for elektronisk kommunikation. Center for Cybersikkerhed skal i den forbindelse koordinere teleberedskabet med beredskabsindsatsen i de øvrige samfundssektorer.

Det foreslås med *stk. 2,* at Center for Cybersikkerhed kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal sikre, at de foretagne prioriteringer gennemføres i net og tjenester.

Center for Cybersikkerhed bemyndiges til at fastsætte regler om, at væsentlige teleudbydere og vigtige teleudbydere skal foretage visse forberedende tiltag med henblik på at kunne tilgodese beredskabsaktørernes behov for elektronisk kommunikation i beredskabssituationer eller i andre ekstraordinære situationer. Sådanne forberedende tiltag kan eksempelvis være planlægning og forberedelse af prioriteringer i net og tjenester med henblik på, at beredskabsaktørerne kan få forrang til anvendelse af disse, herunder til kald i fastnet og mobilnet i tilfælde af overbelastning eller ved beskadigelse af teleinfrastrukturen. Et forberedende tiltag kan i den forbindelse endvidere være tilvejebringelse og opretholdelse af faste kredsløb til beredskabsmæssige formål. Ved faste kredsløb til beredskabsmæssige formål forstås permanent etablerede fysiske eller logiske forbindelser eller netværk, hvor der stilles nærmere defineret transmissionskapacitet til rådighed for beredskabsaktørerne i forbindelse med varetagelsen af opgaver, som bidrager til opretholdelse af samfundets funktioner i en beredskabssituation.

Der kan desuden med hjemmel i bestemmelsen fastsættes regler om, at væsentlige teleudbydere og vigtige teleudbydere i beredskabssituationer eller andre ekstraordinære situationer efter påbud fra Center for Cybersikkerhed skal foretage visse foranstaltninger med henblik på, at prioriteringerne i net og tjenester kan gennemføres. Der kan i den forbindelse fastsættes nærmere regler om, at Center for Cybersikkerhed kan give påbud om, at væsentlige teleudbydere og vigtige teleudbydere skal prioritere retablering af bestemte dele af en udbyders beskadigede infrastruktur. Behovet for prioritering vil være situationsbestemt og afledt af centerets samarbejde med andre sektorer. Prioriteringen kan både omfatte bestemte beredskabsaktørers kommunikation, geografiske områder, bestemte forbindelser og net eller tjenester, alt efter hvad den konkrete situation tilsiger.

Herudover kan der efter bestemmelsen fastsættes regler om, at væsentlige teleudbydere og vigtige teleudbydere i beredskabssituationer eller andre ek-

straordinære situationer efter påbud fra Center for Cybersikkerhed skal prioritere fremførsel i nettene af bestemte forbindelser eller tjenester i tilfælde af kapacitetsproblemer. En væsentlig eller vigtig teleudbyder kan i den forbindelse være nødsaget til at afbryde andre forbindelser eller tjenester helt eller delvis med henblik på at sørge for, at en bestemt forbindelse eller tjeneste opretholdes. Reglerne kan endvidere indeholde krav om, at væsentlige og vigtige teleudbydere i beredskabssituationer eller andre ekstraordinære situationer efter påbud fra Center for Cybersikkerhed skal iværksætte de forberedte prioriteringsordninger ved eksempelvis at indføre generel eller delvis begrænsning af teletrafikken med henblik på at give beredskabsaktører forrang til kald i fastnet og mobilnet.

Det foreslås i *stk. 3,* at Center for Cybersikkerhed kan fastsætte regler om, at væsentlige- og vigtige teleudbydere skal underrette Center for Cybersikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder, herunder regler om, hvordan underretningen skal foretages.

Den foreslåede bestemmelse videreføre delvist indholdet af § 5, stk. 2, i lov om sikkerhed i net og tjenester.

Det følger således bl.a. af bemærkningerne til § 5, stk. 2, i lov om sikkerhed i net og tjenester, at de regler, som Center for Cybersikkerhed med hjemmel i bestemmelsen kan fastsætte for erhvervsmæssige udbydere af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, kan omfatte krav om, at en erhvervsmæssig udbyder skal underrette Center for Cybersikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for udbyderen selv eller for en anden udbyder.

Ministeriet for Samfundssikkerhed og Beredskab finder det henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau i telesektoren.

Det foreslås i *stk. 4,* at Center for Cybersikkerhed kan fastsætte regler om, at udbydere, som i medfør af lov om elektroniske kommunikationsnet og -tjenester skal udsende offentlige advarsler om overhængende eller truende

alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede bestemmelse er en uændret videreførelse af § 5 a i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021. Bemyndigelsen til at fastsætte regler er ikke udmøntet i dag.

Der vil med hjemmel i den foreslåede bestemmelse kunne fastsættes regler om, at udbydere, som i medfør af teleloven skal udsende offentlige advarsler om overhængende eller truende alvorlige nødsituationer og katastrofer, skal træffe alle nødvendige foranstaltninger til at sikre uafbrudt transmission af advarslerne.

Den foreslåede bestemmelse gennemfører den del af artikel 108, 2. pkt., i EU's telekodeks, hvorefter medlemsstaterne sikrer, at udbydere af talekommunikationstjenester træffer alle nødvendige foranstaltninger til at sikre uafbrudt transmission af offentlige advarsler. Artikel 108, 2 pkt. berøres ikke af NIS 2-direktivet.

Den pågældende del af bestemmelsen i artikel 108, 2. pkt., i EU's telekodeks skal ses i sammenhæng med artikel 110, der pålægger medlemsstater, der allerede har etableret offentlige varslingssystemer, at sørge for, at udbydere af mobile nummerbaserede interpersonelle kommunikationstjenester udsender offentlige advarsler til berørte slutbrugere (mobilbaseret varsling).

Forpligtelsen i artikel 110 er implementeret ved telelovens § 62, stk. 1 da forpligtelsen har nær sammenhæng med eksisterende forpligtelser i teleloven i relation til bl.a. alarm- og beredskabsforhold. Det mobilbaserede varslingssystem, der er etableret i medfør af artikel 110 i EU's telekodeks og implementeret i dansk ret ved telelovens § 62, blev taget i brug i foråret 2023.

Forpligtelsen til at udsende offentlige advarsler, der følger af telelovens § 62, stk. 1, påhviler de såkaldte mobiloperatører, som omfatter udbydere af elektroniske kommunikationstjenester i mobilnet og udbydere af mobilnet.

Den foreslåede bestemmelse har til formål at sikre, at mobiloperatørerne træffer alle nødvendige foranstaltninger for at undgå, at udstyr og systemer, der anvendes i forbindelse med transmission af offentlige advarsler, afbrydes. Mobiloperatørerne vil i forlængelse af eksisterende forpligtelser til at sikre en robust teleinfrastruktur skulle planlægge og sørge for opretholdel-

sen af uafbrudt transmission af offentlige advarsler, herunder i relation til udstyr og systemer, der anvendes til transmission af offentlige advarsler, bl.a. tage stilling til fremskaffelse af det nødvendige reserveudstyr, og sikring af redundans og nødstrømsforsyning.

Det foreslås i *stk. 5,* at i beredskabssituationer og i andre ekstraordinære situationer kan Center for Cybersikkerhed påbyde væsentlige og vigtige teleudbydere uden unødigt ophold at iværksætte nærmere angivne sikkerhedsforanstaltninger i tilfælde af en hændelse eller trussel, der i betydeligt omfang påvirker eller kan påvirke udbuddet af net eller tjenester negativt.

Den foreslåede bestemmelse viderefører indholdet af § 5, stk. 4, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Den gældende bestemmelse i § 5, stk. 4, i lov om sikkerhed i net og tjenester gennemfører i øvrigt delvist artikel 108 i EU's telekodeks. Artikel 108 berøres ikke af NIS 2-direktivet.

Ordningen er en del af den samlede beredskabsplanlægning inden for den civile sektor. Det følger således af § 24, stk. 1, i beredskabsloven, jf. lovbekendtgørelse nr. 314 af 3. april 2017 med senere ændringer at hver enkelt minister inden for sit område skal planlægge for opretholdelse og videreførelse af samfundets funktioner i tilfælde af større ulykker og katastrofer, herunder udarbejde beredskabsplaner.

Bestemmelsens anvendelsesområde omfatter beredskabssituationer samt andre ekstraordinære situationer. Dette omfatter såvel situationer med krigshandlinger som situationer, hvor det som følge af en større ulykke, katastrofe eller anden ekstraordinær hændelse eller krise er nødvendigt at indføre særlige foranstaltninger vedrørende net og tjenester med henblik på at opretholde samfundets funktioner. Bestemmelsens anvendelsesområde omfatter således både naturskabte og menneskeskabte ulykker og katastrofer, herunder eksempelvis orkan- og stormflodssituationer og alvorlige cyberangreb.

Center for Cybersikkerhed kan efter bestemmelsen påbyde væsentlige og vigtige teleudbydere at iværksætte akutte sikkerhedsforanstaltninger, forudsat at der er en hændelse eller trussel, der i betydeligt omfang påvirker, eller kan påvirke, udbuddet af net og tjenester negativt. En hændelse, der i betydeligt omfang påvirker udbuddet af net og informationssystemer, kan eksempelvis være et alvorligt cyberangreb eller et terrorangreb, som medfører, at net eller informationssystemer i en periode ikke er tilgængelige for slutbrugerne. Sådanne hændelser kan endvidere være kraftige vejrfænomener såsom orkaner eller skybrud, der medfører, at større dele af teleinfrastrukturen beskadiges. En trussel, der vurderes i betydeligt omfang at kunne påvirke udbuddet af net eller tjenester, vil eksempelvis være, hvis der foreligger oplysninger om et nært forestående sabotageforsøg eller terrorangreb mod kritiske dele af teleinfrastrukturen.

For at anvende bestemmelsen skal der foreligge en beredskabssituation eller en anden ekstraordinær situation. Det bemærkes i den forbindelse, at en hændelse eller trussel, der i betydeligt omfang påvirker, eller kan påvirke, udbuddet af net eller informationssystemer negativt, i sig selv kan udgøre en beredskabssituation.

Center for Cybersikkerhed kan i sådanne situationer påbyde væsentlige og vigtige teleudbydere at iværksætte akutte sikkerhedsforanstaltninger såsom indførelse af særlige adgangskontroller til udbyderens lokaliteter, begrænsning af adgangsveje til og parkeringsrestriktioner på udbyderens arealer samt eftersyn med udbyderens arealer og bygninger. Center for Cybersikkerhed kan endvidere påbyde de væsentlige og de vigtige teleudbydere foranstaltninger ved håndteringen af postforsendelser, f.eks. gennemlysning af breve og pakker. Desuden kan centeret påbyde udbyderne at udpege særligt kritiske eller aktuelt truede dele af deres teleinfrastruktur og sørge for vagtrundering, kontrol med sikringsforanstaltninger og eventuelt bevogtning af de pågældende dele af teleinfrastrukturen i samarbejde med relevante beredskabsaktører. Center for Cybersikkerhed kan i øvrigt påbyde de væsentlige og de vigtige teleudbydere at foranstalte akutte sikkerhedsforanstaltninger til begrænsning af skadevirkningen af eksempelvis naturskabte hændelser. I beredskabssituationer eller i andre ekstraordinære situationer kan Center for Cybersikkerhed i forhold til cyberangreb eksempelvis påbyde logning eller blokering af IP-adresser, der anvendes som led i et angreb. Centeret kan desuden påbyde udbyderne at gennemgå deres beredskabsplaner med henblik på at kunne iværksatte de forberedte tiltag til sikring af teleinfrastrukturen.

Det forudsættes, at udbyderne skal foretage de pågældende foranstaltninger uden omkostninger for staten, hvilket svarer til, at der heller ikke på andre områder udtrykkeligt er angivet, at de påkrævede foranstaltninger skal foretages uden omkostninger for staten.

Til § 15

Det foreslås i *stk. 1,* at underretninger modtaget i medfør af § 9, stk. 1-2, og § 11 er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Bestemmelsen viderefører indholdet af § 7, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Bemyndigelsen til at fastsætte regler om aktindsigt er i dag udmøntet i bekendtgørelse nr. 258 af 22. februar 2021 om oplysnings- og underretningspligter vedrørende sikkerhed i net og tjenester.

Det følger af den foreslåede § 9, stk. 1, 1. pkt., at teleudbydere uden unødigt ophold skal underrette Center for Cybersikkerhed og CSIRT'en om enhver væsentlig hændelse. Det følger derudover af den foreslåede § 11, at teleudbydere kan underrette Center for Cybersikkerhed og CSIRT'en om en hændelse, nærvedhændelser og cybertrusler.

Undtagelsen fra aktindsigt vil også gælde i de tilfælde, hvor oplysningerne videregives til Kommissionen, Det Europæiske Agentur for Net- og Informationssikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Undtagelsen fra aktindsigt omfatter ikke teleudbydernes adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold.

Til § 16

Det foreslås i *stk. 1,* at det i regler udstedt i medfør af § 8, stk. 5, og § 14, stk. 3, kan fastsættes, at underretninger og afgivelse af oplysninger efter disse bestemmelser er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Det følger af den foreslåede § 8, stk. 5, at Center for Cybersikkerhed kan fastsætte nærmere regler om oplysnings- og underretningspligter for væsentlige- og vigtige teleudbydere, herunder krav om: 1) afgivelse af oplys-

ninger om væsentlige dele teleudbyderens net eller tjenester eller driften heraf og 2) krav om underretning ved påtænkt indgåelse af aftaler om leverancer, der vedrører væsentlige dele af udbyderens net eller tjenester eller driften heraf, herunder regler om, at teleudbyderen skal indsende et endeligt aftaleudkast til Center for Cybersikkerhed umiddelbart forud for indgåelse af aftalen, og at aftalen først kan indgås op til 25 arbejdsdage efter centerets modtagelse af dette udkast.

Det foreslås, at der ikke skal være mulighed for aktindsigt i teleudbyderes afgivelse af oplysninger om væsentlige dele af teleudbyderens net eller tjenester eller driften heraf. De oplysninger, som Center for Cybersikkerhed som led i den foreslåede § 8, stk. 5, nr. 1, modtager fra og sender til teleudbydere vedrørende væsentlige dele af udbyderens net og tjenester eller varetagelsen af driften heraf, vil ofte indeholde oplysninger om fejl eller sårbarheder i net eller tjenester, som kan misbruges af potentielle angribere, hvis de kommer til uvedkommendes kendskab. Det foreslås derfor, at oplysningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven, således at aktindsigtsanmodninger ikke – som det ellers ville være tilfældet – behandles efter principperne i offentlighedsloven.

Det foreslås endvidere, at der ikke er adgang til aktindsigt i de udkast til aftaler, som væsentlige og vigtige teleudbydere indsender til Center for Cybersikkerhed i medfør af regler fastsat efter den foreslåede § 8, stk. 5, nr. 2. Aftalerne vil ofte indeholde en lang række oplysninger om udbydernes net og tjenester samt aftaleforhold, som dels er kommercielt fortrolige, dels kan misbruges af potentielle angribere. Reglerne svarer til den gældende § 7, stk. 1, i lov om sikkerhed i net og tjenester. Der tilsigtes ikke en ændring af denne praksis.

Det følger af den foreslåede § 14, stk. 3, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om, at væsentlige og vigtige teleudbydere skal underrette Center for Cybersikkerhed i tilfælde, hvor udbyderen aktiverer sit beredskab, eller hvor udbyderen bliver bekendt med en hændelse, som vurderes at kunne føre til en beredskabssituation eller en anden ekstraordinær situation for teleudbyderen selv eller for en anden udbyder, herunder regler om, hvordan underretningen skal foretages.

Det foreslås, at sådanne underretninger er undtaget fra aktindsigt. Oplysninger om, at der f.eks. er gennemført et vellykket hackerangreb, hvor en virksomhed har mistet data, kan imidlertid i høj grad skade virksomhedens om-

dømme, og risikoen for, at oplysningerne via aktindsigt bliver offentligt tilgængelige, kan i praksis afholde mange virksomheder fra at underrette Center for Cybersikkerhed om et sådant hackerangreb. Derfor bør også disse særlige underretninger være undtaget fra aktindsigt

Til § 17

Den foreslås i *stk. 1*, at medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse udbydere skal sikkerhedsgodkendes af Center for Cybersikkerhed, når 1) det er nødvendigt i forhold til den pågældendes adgang til klassificeret information eller til de funktioner, som den pågældende skal varetage eller 2) den pågældende varetager kontakten til Center for Cybersikkerhed i relation til beredskabet i henhold til regler, der er udstedt i medfør af § 14, stk. 3.

Bestemmelsens viderefører delvist indholdet af den gældende § 6, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Bestemmelsen indebærer, at personkredsen nævnt i bestemmelsens stk. 1, skal sikkerhedsgodkendes af Center for Cybersikkerhed.

Afgørelsen baseres på en sikkerhedsundersøgelse foretaget af Politiets Efterretningstjeneste og træffes ud fra en konkret vurdering af alle foreliggende oplysninger om den pågældende person. I overensstemmelse med ordningen efter sikkerhedscirkulærets § 14 vil der ved afgørelsen om sikkerhedsgodkendelse blive lagt vægt på, om vedkommende har udvist ubestridt loyalitet og har en sådan adfærd og karakter, herunder vaner, forbindelser og diskretion, at der ikke kan være tvivl om den pågældendes pålidelighed i forbindelse med håndtering af klassificerede informationer eller andre beskyttelsesværdige informationer. Der kan ved afgørelsen tilsvarende lægges vægt på oplysninger om en ægtefælles, samlevers, registreret partners eller samboendes adfærd, karakter og forhold i øvrigt.

Den foreslåede bestemmelse i *stk. 2*, hvoraf følger, at ministeren for samfundssikkerhed og beredskab efter forhandling med justitsministeren kan fastsætte regler om ansøgninger vedrørende sikkerhedsgodkendelser, herunder betingelser for indgivelse af sådanne ansøgninger samt meddelelse og tilbagekaldelse af sikkerhedsgodkendelser.

Med den foreslåede bestemmelse vil der således i loven være en særskilt hjemmel til fastsættelse af regler om sikkerhedsgodkendelse af medarbejdere hos væsentlige og vigtige teleudbydere og repræsentanter for disse.

Det forventes, at der fastsættes nærmere regler om ansøgning og afgørelser om sikkerhedsgodkendelser, samt meddelelse om og tilbagekaldelse af afgørelser om sikkerhedsgodkendelser. Dette omfatter bl.a. administrative krav i forbindelse med indgivelse af en ansøgning, krav om afmelding, hvis en person ikke længere har en funktion, som forudsætter en sikkerhedsgodkendelse, og bestemmelser om, at afgørelsen tilbagekaldes, hvis en person ikke længere opfylder kravene til godkendelsen.

Til § 18

Det foreslås med *§ 18,* at Center for Cybersikkerhed fører tilsyn med overholdelsen af denne lov og regler, der er udstedt i medfør af loven.

Der er således ikke forudsat en ændring af tilsynsmyndigheden på teleområdet.

De nærmere regler om Center for Cybersikkerheds kompetencer og regler for håndhævelse af fastsat i forslagets §§ 19-27.

Til § 19

Det foreslås i *stk. 1*, at såfremt det er nødvendigt af hensyn til sikkerheden i net- og informationssystemer, har Center for Cybersikkerhed efter et skriftligt varsel på mindst syv arbejdsdage uden retskendelse mod behørig legitimation adgang til forretningslokaler hos væsentlige- og vigtige teleudbydere samt deres samarbejdspartnere, leverandører eller underleverandører med henblik på at påse overholdelsen af loven og regler, der er udstedt i medfør af loven, herunder i relation til outsourcet aktivitet.

Bestemmelsen viderefører § 9, stk. 6, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren, jf. afsnit 1 ovenfor, væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Formålet med dette tilsynsværktøj er at give Center for Cybersikkerhed mulighed for at konstatere, om væsentlige og vigtige teleudbydere i praksis har gennemført de nødvendige foranstaltninger med henblik på at sikre et passende informationssikkerheds- og beredskabsniveau.

Tilsynsbesøgene vil alene blive gennemført, hvis det er nødvendigt af hensyn til informationssikkerheden. Center for Cybersikkerheds adgang til at foretage tilsynsbesøg – der kun forudsættes anvendt, såfremt et tilsvarende resultat ikke kan opnås ved anvendelse af andre og mindre indgribende tilsynsmuligheder – kan derfor kun anvendes i forbindelse med centerets tilsynsvirksomhed.

Center for Cybersikkerheds tilsynsbesøg vil skulle varsles skriftligt, herunder via e-mail, mindst syv arbejdsdage forud for besøget, og centeret kan således ikke med hjemmel i bestemmelsen foretage uanmeldte tilsynsbesøg.

Det forudsættes endvidere, at Center for Cybersikkerhed i forbindelse med tilsynsbesøgene i videst muligt omfang tager hensyn til den væsentlige eller den vigtige udbyderes virksomhed og tilrettelægger besøgene således, at centeret alene skaffer sig kendskab til forhold, der er af betydning for gennemførelsen af centerets tilsynsvirksomhed. Tilsynsbesøgene vil typisk tage udgangspunkt i oplysninger og materiale fra udbyderne, herunder oplysninger om de iværksatte tekniske, operationelle og organisatoriske foranstaltninger.

Det foreslås i *stk. 2*, at Center for Cybersikkerhed ikke i forbindelse med adgang til forretningslokaler efter stk. 1, kan tilgå kommunikation til, fra eller mellem udbyderens kunder.

Center for Cybersikkerhed vil ikke i forbindelse med tilsynsbesøgene kunne få adgang til elektronisk kommunikation til, fra og mellem udbydernes kunder, ligesom centeret alene vil kunne foretage tilsynsbesøg i det omfang, udbyderens forretningslokaler er placeret i Danmark.

Til § 20

Det foreslås i *stk. 1*, at Center for Cybersikkerhed kan påbyde væsentlige og vigtige teleudbydere at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og informationssystemer i deres risikostyringsprocesser efter § 5.

Bestemmelsen viderefører indholdet af § 3, stk. 2, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Det foreslås derfor med bestemmelsen, at Center for Cybersikkerhed kan påbyde væsentlige og vigtige teleudbydere at inddrage nærmere angivne områder af deres virksomhed og nærmere angivne trusler mod sikkerheden i net og informationssystemer i deres risikostyringsprocesser efter § 5.

Der kan efter den foreslåede bestemmelse stilles krav om, at udbyderne i risikostyringsprocesserne skal tage højde for bestemte (konkrete eller generelle) trusler mod sikkerheden i net og informationssystemer efter påbud fra Center for Cybersikkerhed. Det kan eksempelvis ske på baggrund af de trusselsvurderinger, som løbende udarbejdes af Center for Cybersikkerhed og den øvrige del af Forsvarets Efterretningstjeneste.

Endvidere kan Center for Cybersikkerhed ved påbud bestemme, at visse områder af en udbyders virksomhed, der er nærmere specificeret i påbuddet, skal være omfattet af risikostyringsprocesserne, hvis dette ikke i forvejen er tilfældet.

Det foreslås i *stk. 2*, at Center for Cybersikkerhed, såfremt det er af væsentlig samfundsmæssige betydning, kan påbyde væsentlige og vigtige teleudbydere at træffe konkrete foranstaltninger med henblik på at sikre sikkerheden i net- og informationssystemer. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler herom.

Den foreslåede bestemmelse viderefører indholdet af § 3, stk. 4, i lov om sikkerhed i net og tjenester.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Det foreslås derfor med bestemmelsen, at Center for Cybersikkerhed skal kunne påbyde væsentlige og vigtige teleudbydere at træffe andre og konkrete foranstaltninger end de i stk. 1 nævnte med henblik på at sikre sikkerheden i net og informationssystemer, hvis sådanne foranstaltninger er af væsentlig samfundsmæssig betydning.

Foranstaltninger af væsentlig samfundsmæssig betydning kan i denne sammenhæng eksempelvis være tiltag, der skal reducere risikoen for, at uvedkommende får adgang til myndigheders elektroniske kommunikation. Det kan endvidere være foranstaltninger, der skal hindre uvedkommendes adgang via net og tjenester til infrastruktur, som er nødvendige, for at samfundsvigtige funktioner opretholdes. Dette kan være funktioner, som er særligt vigtige for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed, herunder funktioner inden for sundhed, energi, transport, forsyning, finans, forskning, medier og kommunikation samt funktioner, som har stor økonomisk betydning for samfundet.

Center for Cybersikkerhed vil desuden med hjemmel i bestemmelsen kunne påbyde væsentlige teleudbydere og vigtige erhvervsmæssige teleudbydere at sikre, at udstyr og systemer, som skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden – de såkaldte »lawful interception-funktionaliteter« – skal opsættes i og drives fra Danmark. Påbudsmuligheden forudsættes imidlertid ikke benyttet, såfremt en teleudbyder kan godtgøre, at der er et tilstrækkeligt sikkerhedsniveau på trods af, at lawful interception-funktionaliteterne opsættes og drives uden for Danmark. »Lawful interception-funktionaliteterne« vil i tilfælde af utilstrækkelige sikkerhedsforanstaltninger kunne benyttes af uvedkommende til at overvåge telekunders kommunikation, ligesom uvedkommende vil kunne få kendskab til politiets igangværende aflytninger. En tilstrækkelig sikkerhed i forhold til »lawful interception-funktionaliteterne« er derfor særligt vigtig for samfundets og demokratiets opretholdelse og sikkerhed samt borgernes tryghed.

Det bemærkes i den forbindelse, at Center for Cybersikkerhed alene vil kunne foretage tilsynsbesøg, såfremt »lawful interception-funktionaliteten« er placeret i Danmark. Opsættes udstyr og systemer, som skal anvendes i forbindelse med indgreb i meddelelseshemmeligheden, i udlandet, vil Center for Cybersikkerhed således ikke have mulighed for at konstatere, om udbyderne i praksis har gennemført de nødvendige foranstaltninger med henblik på at sikre et passende sikkerhedsniveau i net og informationssystemer. Det bemærkes desuden, at Center for Cybersikkerheds tilsyn alene vil omfatte de systemtekniske sikkerhedsforanstaltninger, og at centeret ikke i for-

bindelse med tilsyn vil få adgang til oplysninger om igangværende eller historiske aflytninger.

Et påbud efter den foreslåede bestemmelses stk. 2, vil i almindelighed have karakter af erstatningsfri regulering. Det kan imidlertid ikke udelukkes, at påbud udstedt i medfør af den foreslåede bestemmelse vil kunne ramme væsentlige og vigtige teleudbydere så økonomisk intensivt og atypisk hårdt, at der vil kunne være tale om et ekspropriativt indgreb mod den pågældende udbyder. Det vil bero på en konkret vurdering, om der i det enkelte tilfælde foreligger ekspropriation efter grundlovens § 73. Spørgsmålet om adgang til erstatning efter grundlovens § 73 henhører under domstolene.

De foreslåede bestemmelser indebærer ikke, at der ændres ved det grundlæggende princip om aftalefrihed. Der kan således ikke med hjemmel i bestemmelserne ske regulering af ejerforhold, fastsættes forbud mod at indgå aftale med bestemte leverandører eller forbud mod ejerskab af bestemte netværk eller produkter.

Til § 21

Det foreslås i *stk. 1,* at Center for Cybersikkerhed som led i sit tilsyn ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende følgende tilsynsforanstaltninger over for en væsentlig teleudbyder: 1) foretage kontrol på stedet og eksternt tilsyn, herunder foretage stikprøvekontroller, 2) foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Center for Cybersikkerhed, 3) foretage sikkerhedsaudits ad hoc, 4) foretage sikkerhedsscanninger, 5) kræve at få udleveret oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført, 6) kræve at få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven, 7) kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker og 8) kræve at få skriftlige udtalelser og redegørelser om faktiske forhold af betydning for Center for Cybersikkerheds tilsynsvirksomhed.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 1 og 2, i NIS 2-direktivet.

Det følger af NIS 2-direktivets artikel 32, stk. 1, at medlemsstaterne skal sikre, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væ-

sentlige enheder, for så vidt angår forpligtelserne fastsat i direktivet, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Efter bestemmelsen i artikel 32, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende væsentlige enheder, som minimum har beføjelse til at pålægge disse enheder a) kontrol på stedet og eksternt tilsyn, herunder stikprøvekontrol, som skal udføres af uddannede fagfolk, b) regelmæssige og målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed, c) ad hoc-audits, herunder hvor det er berettiget på grund af en væsentlig hændelse eller en overtrædelse af dette direktiv fra den væsentlige enheds side, d) sikkerhedsscanninger baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed, e) anmodninger om oplysninger, der er nødvendige for at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27 (om registreringspligt for bestemte typer af digitale tjenester), f) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver og g) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

Efter direktivets artikel 32, stk. 2, 2. led, baseres de målrettede sikkerhedsaudits, der er omhandlet i første led, litra b, på risikovurderinger foretaget af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger. Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde når den kompetente myndighed bestemmer andet.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *stk. 2*, at ved anvendelsen af tiltagene i stk. 1, nr. 5-8, skal Center for Cybersikkerhed angive formålet med kravet og præcisere, hvilke oplysninger der kræves udleveret.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 3, hvorefter de kompetente myndigheder ved udøvelsen af deres beføjelser i henhold til artikel 32, stk. 2, litra e, f eller g, skal angive formålet med anmodningen og præcisere, hvilke oplysninger der anmodes om.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 3, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det foreslås i *stk. 3,* at Center for Cybersikkerhed kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 5-8, skal afgives.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerhed i forbindelse med, at der stilles krav om udlevering af oplysninger eller materiale efter de foreslåede bestemmelser i stk. 1, nr. 5-8, samtidig kan kræve, at oplysningerne eller materialet udleveres på en bestemt måde, på et bestemt sprog og i en bestemt form.

Der vil eksempelvis kunne stilles krav om anvendelse af bestemte skemaer, eller at der skal foretages indtastninger på en hjemmeside.

Til § 22

Det foreslås i *stk. 1,* at Center for Cybersikkerhed ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende følgende håndhævelsesforanstaltninger over for en væsentlig teleudbyder 1) udstede advarsler om teleudbyderens overtrædelse af denne lov, 2) udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov, 3) påbyde teleudbyderen at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, 4) meddele teleudbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 5) påbyde teleudbyderen at underrette de fysiske eller juridiske personer, som teleudbyderen leverer tjenester til eller udfører aktiviteter for, og som potentielt kan være berørt af

en væsentlig trussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel, 6) påbyde teleudbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit, 7) udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med teleudbyderens overholdelse af lovens kapitel 2 og 3 samt regler udstedt i medfør heraf og 8) påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 4, litra a-h, i NIS 2-direktivet, for så vidt angår telesektoren.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 4, litra a-h, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Efter bestemmelsen får Center for Cybersikkerhed mulighed for at udstede advarsler, bindende instrukser, påbud og forbud.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 32, stk. 1, at de håndhævelsesforanstaltninger, der anvendes overfor væsentlige teleudbydere i medfør af den foreslåede bestemmelse, skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det følger af den foreslåede bestemmelse, at Center for Cybersikkerhed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når centret anvender håndhævelsesforanstaltningerne over for væsentlige teleudbydere, således at proportionalitetsprincippet overholdes ved valg mellem de oplistede håndhævelsesmuligheder.

Center for Cybersikkerhed skal derfor i overensstemmelse med NIS 2-direktivets artikel 32, stk. 7, litra a, tage hensyn til 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 Center for Cybersikkerhed, d) hindringer for audits eller overvåg-

ningsaktiviteter beordret af Center for Cybersikkerhed efter konstatering af en overtrædelse, og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, 2) overtrædelsens varighed, 3) den pågældende udbyders relevante tidligere overtrædelser, 4) enhver fysisk eller ikke fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af udbyderen for at forebygge eller afbøde den fysisk eller ikke fysisk skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med Center for Cybersikkerhed.

Det følger endvidere af NIS 2-direktivets artikel 32, stk. 7, at den kompetente myndighed ved anvendelsen af håndhævelsesforanstaltninger skal overholde retten til forsvar. Dette sikres ved, at et påbud eller forbud efter den foreslåede § 22 vil være omfattet af forvaltningslovens almindelige regler, herunder bestemmelserne i kapitel 3 (om vejledning og repræsentation mv.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse mv.) og kapitel 7 (om klagevejledning).

Derudover vil der være mulighed for at indbringe afgørelserne for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 22 blive fastsat en frist, inden for hvilken udbyderen skal efterkomme indholdet i afgørelsen.

En væsentlig teludbyder, der modtager en afgørelse om påbud eller forbud efter den foreslåede § 22, vil også kunne ifalde straf for en eventuel overtrædelse af denne lov eller regler udstedt i medfør af loven.

Det følger af det foreslåede *nr. 1,* at Center for Cybersikkerhed kan udstede advarsler om teleudbyderens overtrædelse af denne lov.

Det følger af den foreslåede *nr. 2,* at Center for Cybersikkerhed kan udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.

Det følger af den foreslåede *nr. 3,* at Center for Cybersikkerhed påbyde udbyderen at træffe foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse.

Det følger af det foreslåede *nr. 4,* at Center for Cybersikkerhed kan meddele udbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.

I tilfælde af, at en udbyder eksempelvis ikke lever op til de krav, der er fastsat i loven, vil Center for Cybersikkerhed kunne angive, hvilke nærmere foranstaltninger udbyderen skal træffe. Det kan eksempelvis være organisatoriske foranstaltninger vedrørende passende rolle- og ansvarsfordeling, herunder forbud mod ansvarssammenfald, samt procedurer i relation til erhvervelse og udvikling af net- og informationssystemer, tekniske foranstaltninger vedrørende sikkerhedskopiering af data eller om udbyderens anvendelse af bestemte logningsmetoder.

Det følger af det foreslåede *nr. 5,* at Center for Cybersikkerhed kan påbyde udbyderen at underrette de fysiske eller juridiske personer, til hvilke udbyderen leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig hændelse, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.

Bestemmelsen skal ses i sammenhæng med den foreslåede bestemmelse i § 12, stk. 2, som indeholder en forpligtelse for væsentlige teleudbydere og vigtige teleudbydere til i relevant omfang at underrette modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal udbyderene også informere de pågældende modtagere om den væsentlige cybertrussel.

Med den foreslåede bestemmelse vil Center for Cybersikkerhed kunne påbyde, at der skal foretages underretning af modtagerne af udbyderens tjenester, uanset om udbyderen selv vurderer, at det er relevant.

Det følger af det foreslåede *nr. 6,* at Center for Cybersikkerhed kan påbyde udbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 21, stk. 1, nr. 2, hvorefter Center for Cybersikkerhed kan foretage regelmæssige og målrettede sikkerhedsaudits eller stille krav om, at den væsentlige teleudbyder får et kvalificeret uafhængigt organ til at foretage disse audits, samt den foreslåede § 21, stk. 1, nr. 3, hvorefter Center for Cybersikkerhed kan foretage sikkerhedsaudits ad hoc.

Det følger af det foreslåede *nr. 7,* at Center for Cybersikkerhed kan påbyde udbyderen at udpege en person med ansvar for i en nærmere fastsat periode at føre tilsyn med udbyderens overholdelse af lovens kapitel 2 og 3 samt regler udstedt i medfør heraf.

Center for Cybersikkerhed vil enten kunne udpege en ansat eller en ekstern person. Det forudsættes, at den pågældende person har de nødvendige kvalifikationer til at udføre opgaven. Den pågældende person vil skulle monitorere udbyderens overholdelse af krav til foranstaltninger til styring af cybersikkerhedsrisici i medfør af den foreslåede § 5 og udbyderens overholdelse af oplysnings- og underretningspligterne i de foreslåede § 9, § 10, § 12 og § 13, samt regler udstedt i medfør af de nævnte bestemmelser.

Det følger af det foreslåede *nr. 8,* at Center for Cybersikkerhed kan påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-5 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at Center for Cybersikkerhed ved beslutningen om, hvilke oplysninger en udbyder pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentlig ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Til § 23

Det foreslås i *stk. 1*, at hvis de håndhævelsesforanstaltninger, der er pålagt i medfør af § 26 nr. 1-4, har vist sig at være utilstrækkelige, kan Center for Cybersikkerhed fastsætte en frist, inden for hvilken den væsentlige teleudbyder skal foretage de nødvendige tiltag for at afhjælpe manglerne eller opfylde Center for Cybersikkerheds krav. Er tiltagene ikke foretaget inden for

den fastsatte frist, kan Center for Cybersikkerhed træffe afgørelse om 1) midlertidigt at suspendere en certificering eller godkendelse vedrørende dele af eller alle de relevante tjenester, udbyderen leverer, eller aktiviteter, der udføres af udbyderen og 2) midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner ved den pågældende udbyder.

Bestemmelsen vil gennemføre artikel 32, stk. 5, 1. led, i NIS 2-direktivet, for så vidt angår telesektoren. Det følger af bestemmelsen, 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 gennemførelse af bestemmelsen i direktivet. Det skyldes navnlig, at rettighedsfrakendelse i medfør af straffelovens § 79 alene kan ske i forbindelse med dom for strafbart forhold, og hvis det udviste forhold begrunder en nærliggende fare for misbrug af stillingen.

Det bemærkes i den forbindelse, at det af den danske oversættelse af NIS 2-direktivets artikel 32, stk. 5, 1. led, fremgår, at bestemmelsen kan anvendes, hvor de relevante håndhævelsesforanstaltninger er »virkningsløse«. Denne oversættelse er efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse imidlertid ikke forenelig med den engelske udgave af direktivet, hvori »ineffective« er anvendt. Det er således Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at formuleringen »virkningsløse« ville udgøre en indholdsmæssig forskydning i forhold til den engelske sprogversion.

Det er desuden Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at et kriterium om, at foranstaltningerne er »virkningsløse«, ville indebære, at enhver virkning af de anvendte foranstaltninger – uanset om virkningen måtte være utilstrækkelig eller endda negativ – ville betyde, at bestemmelsen ikke vil kunne anvendes. Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at dette reelt ville gøre bestemmelsen uanvendelig i praksis i strid med direktivets forudsætninger. Der er på den baggrund anvendt et kriterie om, at foranstaltningerne er »utilstrækkelige«, da dette i en dansk juridisk sammenhæng vurderes at svare til »ineffektive« og afspejler et indbygget proportionalitetsprincip.

Det følger på den baggrund af den foreslåede bestemmelse, at det vil være en forudsætning for at anvende bestemmelsen, at håndhævelsesforanstaltninger pålagt i medfør af den foreslåede § 22, nr. 1-6, har vist sig at være utilstrækkelige. Det er dermed en forudsætning, at mindre indgribende midler har været forsøgt og vist sig utilstrækkelige til at sikre, at udbyderen foretager de nødvendige tiltag for at afhjælpe mangler, som Center for Cybersikkerhed har konstateret, eller opfylder centrets 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 fysisk eller ikke fysisk skade.

Center for Cybersikkerhed vil efter omstændighederne og i relevant omfang kunne træffe afgørelse om anvendelse af flere håndhævelsesforanstaltninger på én gang. Der er således ikke i medfør af den foreslåede § 22 et krav om, at relevante håndhævelsesforanstaltninger anvendes tidsmæssigt forskudt af hinanden, såfremt det vurderes, at flere foranstaltninger i kombination er nødvendige for at sikre, at reglerne efterleves.

Der vil efter bestemmelsen skulle fastsættes en nærmere angivet frist, inden for hvilken den væsentlige teleudbyder skal have truffet de nødvendige tiltag for at afhjælpe manglerne eller opfylde Center for Cybersikkerheds krav.

Varigheden af fristen vil afhænge af en konkret vurdering, som foretages af Center for Cybersikkerhed.

Det foreslås, at afgørelse om suspension eller forbud træffes af Center for Cybersikkerhed i første instans. Det skal ses i lyset af, at muligheden for suspension og forbud ligger i forlængelse af Center for Cybersikkerheds øvrige håndhævelsesmuligheder, og at der i en afgørelse om suspension eller forbud forudsættes at skulle indgå en begrundelse for, hvorfor allerede pålagte håndhævelsesforanstaltninger er utilstrækkelige.

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.

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 kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i § 4 og §§ 11-14, 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 der ved overtrædelsen er handlet 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 for overtrædelsen, samarbejder med de kompetente myndigheder.

Den foreslåede bestemmelse i stk. 1*, nr. 1,* indebærer, at såfremt den væsentlige teleudbyder ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme Center for Cybersikkerheds krav inden for den fastsatte frist, kan centret træffe afgørelse om midlertidigt at suspendere en certificering

eller godkendelse vedrørende dele af eller alle de relevante tjenester, udbyderen leverer, eller aktiviteter, der udføres af udbyderen.

Den foreslåede bestemmelse skal læses i sammenhæng med den foreslåede bestemmelse i stk. 4, hvorefter Center for Cybersikkerhed vil kunne fastsætte nærmere regler for, hvilke certificeringer og godkendelser, som bestemmelsen i stk. 1, nr. 1, finder anvendelse på. Det forudsættes, at den foreslåede bestemmelse i stk. 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 4, er anvendt.

En afgørelse efter nr. 1 vil være af midlertidig karakter, jf. også det foreslåede stk. 2, hvorefter afgørelsen kun kan anvendes, så længe den væsentlige teleudbyder ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller efterleve de krav fra Center for Cybersikkerhed, som gav anledning til, at foranstaltningerne blev anvendt.

Den foreslåede bestemmelse i stk. 1*, nr. 2,* indebærer, at såfremt den væsentlige teleudbyder ikke har iværksat tiltag for at afhjælpe manglerne eller efterkomme Center for Cybersikkerheds krav inden for den fastsatte frist, kan centret træffe afgørelse om midlertidigt at forbyde enhver fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant hos udbyderen at udøve ledelsesfunktioner ved den pågældende udbyder.

Det bemærkes hertil, at det af den danske oversættelse af NIS 2-direktivets artikel 32, stk. 5, litra b, bl.a. fremgår, at de personer med ledelsesansvar, der midlertidigt kan suspenderes, omfatter »enhver fysisk person med ledelsesansvar på direktionsniveau«. Denne oversættelse er efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse imidlertid ikke forenelig med den engelske udgave af direktivet, hvori »any natural person who is responsible for discharging managerial responsibilities at chief executive officer […] level« er anvendt. Den franske sprogversion anvender en tilsvarende formulering som den engelske. I den foreslåede bestemmelse anvendes på den baggrund betegnelsen »enhver fysisk person med ledelsesansvar på niveau med administrerende direktør«.

I det omfang en virksomhed eller organisation ikke har en administrerende direktør, vil bestemmelsen omfatte den øverste leder af den pågældende væsentlige teleudbyder, f.eks. en generalsekretær, direktør, koncernchef eller managing partner.

En afgørelse efter nr. 2 vil være af midlertidig karakter, jf. også det foreslåede stk. 2, hvorefter afgørelsen kun kan anvendes, så længe den væsentlige teleudbyder ikke har truffet de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav fra Center for Cybersikkerhed, som gav anledning til, at foranstaltningerne blev anvendt.

Det følger af det foreslåede *stk. 2,* at midlertidige suspensioner eller forbud, som er pålagt i medfør af stk. 1, kun kan anvendes, indtil den væsentlige teleudbyder træffer de nødvendige tiltag for 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 gennemføre NIS 2-direktivets artikel 32, stk. 5, 1. led, for så vidt angår telesektoren. Det følger af 32, stk. 5, 1. led, at midlertidige suspensioner eller forbud, som er pålagt i henhold til dette stykke, kun anvendes, indtil den pågældende enhed 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 med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 32, stk. 5, 1. led, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Bestemmelsen indebærer, at når Center for Cybersikkerhed har truffet afgørelse om midlertidigt at suspendere en certificering eller midlertidigt har forbudt en fysisk person med ledelsesansvar på niveau med administrerende direktør eller den juridiske repræsentant ved udbyderen at udøve ledelsesfunktioner ved den pågældende udbyder, skal centret træffe afgørelse om at ophæve foranstaltningen, når udbyderen har truffet de nødvendige tiltag for at afhjælpe de mangler eller opfylde de krav, som gav anledning til, at foranstaltningen blev anvendt.

Det følger af det foreslåede *stk. 3,* at en afgørelse efter stk. 1 kan forlanges indbragt for domstolene af den væsentlige teleudbyder eller den fysiske person, afgørelsen vedrører. Center for Cybersikkerhed anlægger i givet fald sag inden for rammerne af den civile retspleje mod den udbyder eller person, som har forlangt sagen indbragt.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 32, stk. 5, 2. led, 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 den væsentlige teleudbyder 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.

Det følger af det foreslåede *stk. 4,* at Center for Cybersikkerhed kan fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af stk. 1, nr. 1.

Den foreslåede bestemmelse i stk. 4 indebærer, at Center for Cybersikkerhed kan fastsætte nærmere regler om, hvilke certificeringer og godkendelser der er omfattet af den midlertidige suspensionsordning i § 23, stk. 1, nr. 1.

Ved at fastsætte nærmere regler i bekendtgørelsesform sikres det, at det vil være klart og forudsigeligt for de væsentlige teleudbydere, hvilke certificerings- og godkendelsesordninger, der vil kunne medføre suspension. Det sikres endvidere, at reglerne løbende kan tilpasses den udvikling, der er på området, f.eks. i tilfælde af, at der indføres en ny cybersikkerhedscertificering i EU-regi.

De nærmere regler vil skulle udarbejdes inden for den ramme, som det foreslåede stk. 1 udgør. Det indebærer bl.a., at reglerne vil skulle være i overensstemmelse med regeringens principper om minimumsimplementering. Det forudsættes, at den foreslåede bestemmelse i stk. 1, nr. 1, ikke anvendes, før bemyndigelsen i den foreslåede stk. 4, er anvendt.

Til § 24

Det foreslås i *stk. 1,* at Center for Cybersikkerhed kan som led i sit tilsyn ud fra en konkret vurdering af omstændighederne i hver enkelt sag anvende følgende tilsynsforanstaltninger over for en vigtig teleudbyder: 1) foretage kontrol på stedet, 2) foretage målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits, og at resultaterne heraf stilles til rådighed for Center for Cybersikkerhed, 3) foretage sikkerhedsscanninger, 4) kræve at få udleveret oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af sikkerhedsrisici, som den berørte udbyder har indført, 5) kræve at

få adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af tilsynsopgaven, herunder til afgørelse af, om et forhold er omfattet af denne lov eller regler udstedt i medfør af loven, 6) kræve at få udleveret dokumentation for gennemførelsen af sikkerhedspolitikker, og 7) kræve at få skriftlige udtalelser og redegørelser om faktisk forhold af betydning for Center for Cybersikkerheds tilsynsvirksomhed.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet.

Det følger af artikel 33, stk. 1, at når medlemsstaterne kommer i besiddelse af dokumentation for, tegn på eller oplysninger om, at en vigtig enhed angiveligt ikke overholder direktivet, navnlig artikel 21 og 23, sikrer de, at de kompetente myndigheder træffer foranstaltninger, hvor det er nødvendigt, gennem efterfølgende tilsynsforanstaltninger. Medlemsstaterne sikrer, at disse foranstaltninger er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Efter bestemmelsen i artikel 33, stk. 2, skal medlemsstaterne sikre, at de kompetente myndigheder, når de udfører deres tilsynsopgaver vedrørende vigtige enheder, som minimum har beføjelse til at pålægge vigtige enheder: a) Kontrol på stedet og eksternt efterfølgende tilsyn udført af uddannede fagfolk, b) målrettede sikkerhedsaudits udført af et kvalificeret uafhængigt organ eller en kompetent myndighed, c) sikkerhedsscanninger baseret på objektive, ikke-diskriminerende, fair og gennemsigtige risikovurderingskriterier, hvor det er nødvendigt i samarbejde med den berørte enhed, d) anmodninger om oplysninger, der er nødvendige for efterfølgende at vurdere de foranstaltninger til styring af cybersikkerhedsrisici, som den berørte enhed har indført, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at indgive oplysninger til de kompetente myndigheder i henhold til artikel 27 (om registreringspligt for bestemte typer af digitale tjenester), e) anmodninger om adgang til data, dokumenter og oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver og f) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsaudits udført af en kvalificeret revisor og den respektive underliggende dokumentation.

Efter direktivets artikel 33, stk. 2, 2. led, baseres de målrettede sikkerhedsaudits, der er omhandlet i første led, litra b, på risikovurderinger foretaget

af den kompetente myndighed eller den reviderede enhed eller på andre tilgængelige risikorelaterede oplysninger. Resultaterne af enhver målrettet sikkerhedsaudit stilles til rådighed for den kompetente myndighed. Omkostningerne ved en sådan målrettet sikkerhedsaudit, der udføres af et uafhængigt organ, afholdes af den reviderede enhed, undtagen i behørigt begrundede tilfælde, når den kompetente myndighed bestemmer andet.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 1 og 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse fastslår, at Center for Cybersikkerhed fører reaktivt tilsyn med vigtige enheders overholdelse af denne lov og regler udstedt i medfør af loven.

Det fremgår desuden af NIS 2-direktivets artikel 33, stk. 2, litra a, at der kan foretages »eksternt efterfølgende tilsyn«, hvilket er en formulering, der efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse kan give anledning til fortolkningstvivl i dansk sammenhæng. I den engelske sprogversion af NIS 2-direktivet anvendes formuleringen »off-site *ex post* supervision«. Efter Ministeriet for Samfundssikkerhed og Beredskabs opfattelse udgør eksternt efterfølgende tilsyn forstået som off-site ex post supervision et reaktivt tilsyn fra en kompetent myndighed uden fysisk tilstedeværelse *på stedet*, men eksempelvis udført på skriftligt grundlag. Det bemærkes, at de kompetente myndigheder i medfør af den foreslåede bestemmelse kan kræve relevante oplysninger fra enhederne. Det indebærer også, at de kompetente myndigheder kan kræve at få udleveret nødvendige oplysninger til afgørelse af, om et forhold er omfattet af loven eller regler udstedt i medfør af loven.

Center for Cybersikkerheds tilsyn vil efter de foreslåede bestemmelser kunne gennemføres ved fysiske tilsynsbesøg eller på administrativt grundlag.

Bestemmelsens svarer til § 24, stk. 1 i forslag til lov om sikring af et højt cybersikkerhedsniveau, som fremsættes samtidig med nærværende lovforslag. Bestemmelsen skal således fortolkes i overensstemmelse med forslag til lov om sikring af højt cybersikkerhedsniveau.

Det følger af det foreslåede *stk. 2,* at de Center for Cybersikkerhed ved anvendelse af tiltagene i stk. 1, nr. 4-6, skal angive formålet med kravet og præcisere, hvilke oplysninger, der kræves udleveret.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 33, stk. 3, hvorefter de kompetente myndigheder ved udøvelsen af deres beføjelser i henhold til artikel 33, stk. 2, litra d, e, og f, skal angive formålet med anmodningen og præcisere, hvilke oplysninger der anmodes om.

Bestemmelsens svarer til § 24, stk. 2 i forslag til lov om sikring af et højt cybersikkerhedsniveau, som fremsættes samtidig med nærværende lovforslag. Bestemmelsen skal således fortolkes i overensstemmelse med forslag til lov om sikring af højt cybersikkerhedsniveau.

Det foreslås i *stk. 3,* at Center for Cybersikkerhed kan stille nærmere krav om, hvordan og i hvilken form oplysningerne eller materialet nævnt i stk. 1, nr. 4-6, skal afgives.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerhed i forbindelse med, at der stilles krav om udlevering af oplysninger eller materiale efter de foreslåede bestemmelser i stk. 1, nr. 4-6, samtidig kan kræve, at oplysningerne eller materialet udleveres på en bestemt måde, på et bestemt sprog og i en bestemt form.

Der vil eksempelvis kunne stilles krav om anvendelse af bestemte skemaer, eller at der skal foretages indtastninger på en hjemmeside.

Bestemmelsens svarer til § 24, stk. 3 i forslag til lov om sikring af et højt cybersikkerhedsniveau, som fremsættes samtidig med nærværende lovforslag. Bestemmelsen skal således fortolkes i overensstemmelse med forslag til lov om sikring af højt cybersikkerhedsniveau.

Til § 25

Det foreslås i stk. 1, at Center for Cybersikkerhed ud fra en konkret vurdering af omstændighederne i hver enkelt sag kan anvende følgende håndhævelsesforanstaltninger over for en vigtig teleudbyder: 1) udstede advarsler om teleudbyderens overtrædelse af denne lov, 2) udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de på-

gældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov, 3) meddele udbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven, 4) påbyde udbyderen at underrette de fysiske eller juridiske personer, til hvilke udbyderen leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel, 5) påbyde udbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit, og 6) påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 1 og 2, i NIS 2-direktivet.

Den foreslåede bestemmelse vil gennemføre artikel 33, stk. 4, litra a-g, i NIS 2-direktivet for så vidt angår telesektoren.

Den foreslåede bestemmelse svarer med sproglige tilpasninger uden indholdsmæssig betydning til NIS 2-direktivets artikel 33, stk. 4, litra a-g, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Det bemærkes i den forbindelse, at det følger af NIS 2-direktivets artikel 32, stk. 1, at de håndhævelsesforanstaltninger, der anvendes overfor væsentlige teleudbydere i medfør af den foreslåede bestemmelse, skal være effektive, stå i et rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det følger af den foreslåede bestemmelse, at Center for Cybersikkerhed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når centret anvender håndhævelsesforanstaltningerne over for væsentlige teleudbydere, således at proportionalitetsprincippet overholdes ved valg mellem de oplistede håndhævelsesmuligheder.

De foranstaltninger, der anvendes i forhold til vigtige teleudbydere skal i overensstemmelse med NIS 2-direktivets artikel 33, stk. 1, være effektive, stå i rimeligt forhold til overtrædelsen og have en afskrækkende virkning under hensyntagen til omstændighederne i hver enkelt sag.

Det følger af den foreslåede bestemmelse, at Center for Cybersikkerhed skal foretage en konkret vurdering af omstændighederne i hver enkelt sag, når centret anvender håndhævelsesforanstaltningerne over for vigtige udbydere. Center for Cybersikkerhed skal derfor i overensstemmelse med NIS 2-direktivets artikel 32, stk. 7, litra a, jf. artikel 33, stk. 5, tage hensyn til: 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 Center for Cybersikkerhed, d) hindringer for audits eller overvågningsaktiviteter beordret af Center for Cybersikkerhed efter konstatering af en overtrædelse, og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i § 4 og §§ 11-14, 2) overtrædelsens varighed, 3) den pågældende udbyders relevante tidligere overtrædelser, 4) enhver fysisk eller ikke fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af udbyderen for at forebygge eller afbøde den fysisk eller ikke fysisk skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med Center for Cybersikkerhed.

Det følger endvidere af NIS 2-direktivets artikel 32, stk. 7, at en kompetent myndighed ved anvendelsen af håndhævelsesforanstaltninger skal overholde retten til forsvar. Dette sikres ved, at et påbud eller forbud efter den foreslåede § 25, vil være omfattet af forvaltningslovens almindelige regler, herunder bestemmelserne i kapitel 3 (om vejledning og repræsentation mv.), kapitel 5 (om partshøring), kapitel 6 (om begrundelse mv.) og kapitel 7 (om klagevejledning). Derudover vil der være mulighed for at påklage afgørelsen i medfør af det ulovbestemte princip om administrativ rekurs, ligesom afgørelsen vil kunne indbringes for domstolene.

Der vil i forbindelse med en afgørelse om påbud eller forbud efter den foreslåede § 25 blive fastsat en frist, inden for hvilken udbyderen skal overholde indholdet i afgørelsen.

Det følger af det foreslåede *nr. 1,* at Center for Cybersikkerhed kan udstede advarsler om teleudbyderens overtrædelse af denne lov.

Det følger af den foreslåede *nr. 2,* at Center for Cybersikkerhed kan udstede bindende instrukser, herunder vedrørende foranstaltninger, der er nødvendige for at forhindre eller afhjælpe en hændelse, samt frister for gennemførelse af sådanne foranstaltninger og for rapportering om deres gennemførelse eller pålægge de pågældende enheder at afhjælpe de konstaterede mangler eller overtrædelserne af denne lov.

Det følger af det foreslåede *nr. 3,* at Center for Cybersikkerhed kan meddele udbyderen påbud og forbud for at sikre overholdelsen af de krav, der er fastsat i loven eller regler udstedt i medfør af loven.

I tilfælde af, at udbyderen ikke lever op til de krav, der er fastsat i loven, vil Center for Cybersikkerhed eksempelvis kunne angive, hvilke nærmere foranstaltninger udbyderen skal træffe. Det kan eksempelvis være organisatoriske foranstaltninger vedrørende passende rolle- og ansvarsfordeling, herunder forbud mod ansvarssammenfald eller procedurer i relation til erhvervelse og udvikling af net- og informationssystemer, tekniske foranstaltninger vedrørende sikkerhedskopiering af data, eller om udbyderens anvendelse af bestemte logningsmetoder.

Det følger af det foreslåede *nr. 4,* at Center for Cybersikkerhed kan påbyde udbyderen at underrette de fysiske eller juridiske personer, til hvilke udbyderen leverer tjenester eller udfører aktiviteter, som potentielt kan være berørt af en væsentlig cybertrussel, om denne trussels karakter samt om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som de fysiske eller juridiske personer kan træffe som reaktion på denne trussel.

Bestemmelsen skal ses i sammenhæng med den foreslåede bestemmelse i § 12, stk. 2, som indeholder en forpligtelse for væsentlige teleudbydere og vigtige teleudbydere til i relevant omfang at underrette modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller modforholdsregler, som modtagerne kan træffe som reaktion på den pågældende trussel. Hvor det er relevant, skal udbyderne også informere de pågældende modtagere om den væsentlige cybertrussel.

Med det foreslåede nr. 4 vil Center for Cybersikkerhed kunne påbyde, at der skal foretages underretning af modtagerne af udbyderens tjenester, uanset om udbyderen selv vurderer, at det er relevant.

Det følger af det foreslåede *nr. 5,* at Center for Cybersikkerhed kan påbyde udbyderen at gennemføre de anbefalinger, der er fremsat i forbindelse med en gennemført sikkerhedsaudit.

Bestemmelsen skal ses i sammenhæng med den foreslåede § 24, stk. 1, nr. 2, hvorefter Center for Cybersikkerhed kan foretage målrettede sikkerhedsaudits eller stille krav om, at udbyderen får et kvalificeret uafhængigt organ til at foretage disse audits.

Det følger af det foreslåede *nr. 6,* at Center for Cybersikkerhed kan påbyde udbyderen i ikke-anonymiseret form og på en nærmere angiven måde at offentliggøre afgørelser om håndhævelsesforanstaltninger efter nr. 1-3 samt resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde.

I overensstemmelse med principperne i betænkning nr. 1516 om offentlige myndigheders offentliggørelse af kontrolresultater, afgørelser mv. forudsættes det, at den kompetente myndighed ved beslutningen om, hvilke oplysninger en enhed pålægges at offentliggøre, i fornødent omfang bl.a. iagttager de hensyn til fortrolighed, der fremgår af forvaltningslovens § 27 om offentligt ansattes tavshedspligt, herunder bl.a. hensynene til enkeltpersoners private forhold, forretningshemmeligheder samt forebyggelse, efterforskning og forfølgning af lovovertrædelser.

Til § 26

Det følger af den foreslåede *§ 26,* at inden Center for Cybersikkerhed træffer afgørelse om at anvende håndhævelsesforanstaltninger efter §§ 22, 23 og 25, underrettes den berørte væsentlige eller vigtige teleudbyder om de påtænkte håndhævelsesforanstaltninger og begrundelsen herfor. Center for Cybersikkerhed skal give udbyderen en rimelig frist til at fremsætte bemærkninger, undtagen i tilfælde hvor formålet med foranstaltningen ellers ville forspildes.

Den foreslåede bestemmelse vil gennemføre artikel 32, stk. 8, i 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) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), for så vidt angår telesektoren. Artikel 32, stk. 8, fastsætter, at de kompetente myndigheder giver en detaljeret begrundelse for deres håndhævelsesforanstaltninger. Inden de kompetente myndigheder

træffer sådanne foranstaltninger, underretter de kompetente myndigheder de berørte enheder om deres foreløbige resultater. De giver også disse enheder en rimelig frist til at fremsætte bemærkninger, undtagen i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret. Det bemærkes, at artikel 32, stk. 8, også finder anvendelse på vigtige enheder, jf. artikel 33, stk. 5.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 32, stk. 8, jf. artikel 33, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indeholder en forpligtelse for Center for Cybersikkerhed til at foretage en høring af den væsentlige teleudbyder eller vigtige teleudbyder, før der træffes beslutning om at anvende en påtænkt håndhævelsesforanstaltning efter §§ 22, 23 og 25.

Høringsskrivelsen skal være ledsaget af en nærmere begrundelse for den påtænkte håndhævelsesforanstaltning, ligesom det skal fremgå klart, at der er tale om en høring, at der ikke er truffet afgørelse i sagen endnu, at udbyderens bemærkninger til høringen kan få indflydelse på resultatet, og at Center for Cybersikkerhed lader agterskrivelsen få virkning som en afgørelse, hvis udbyderen ikke kommer med bemærkninger til høringen inden dennes udløb.

Høringsskrivelsen skal indeholde en rimelig frist for udbyderen til at afgive bemærkninger til høringsskrivelsens indhold. Kravet om at fastsætte en rimelig frist gælder dog ikke i behørigt begrundede tilfælde, hvor øjeblikkelige foranstaltninger til at forebygge eller reagere på hændelser ellers ville blive hindret.

Til § 27

Det foreslås i *stk. 1*, at Center for Cybersikkerhed i ikke-anonymiseret form kan offentliggøre 1) Påbud og forbud meddelt i medfør af § 28 og afgørelser truffet i medfør af regler, der er udstedt i medfør af 5, stk. 3, § 9, stk. 4, § 14, stk. 2, og § 14, stk. 4, 2) resultater af tilsyn efter 22. stk. 1, 3) resumeer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov, og 4) resumeer af domme i retssager, hvor Center for Cybersikkerhed er part.

Bestemmelsen viderefører indholdet af § 10, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Ministeriet for Samfundssikkerhed og Beredskab finder det således henset til vurderingen af det aktuelle trusselsniveau mod telesektoren væsentligt at opretholde det nuværende sikkerhedsniveau for sektoren. Der er med videreførelsen af bestemmelsen ikke tilsigtet materielle ændringer af bestemmelsens indhold.

Den foreslåede bestemmelse har til formål at give væsentlige og vigtige teleudbydere øget incitament til at overholde kravene til sikkerhed i net og informationssystemer og beredskab, ligesom bestemmelsen giver telekunder mulighed for at vurdere, i hvilket omfang de enkelte udbydere har levet op til lovgivningens krav.

Offentliggørelse af afgørelser efter *nr. 1*, indebærer, at der kan ske offentliggørelse i sager, hvor en væsentlig eller vigtig teleudbyder ikke lever op til kravene til sikkerhed i net og informationssystemer eller beredskab, såvel som i sager, hvor Center for Cybersikkerhed giver påbud til en udbyder om eksempelvis at foretage nærmere angivne foranstaltninger til sikring af sikkerheden i net og informationssystemer. Der vil også kunne ske offentliggørelse i sager, hvor Center for Cybersikkerhed på baggrund af eksempelvis en klage konstaterer, at en udbyder overholder kravene til sikkerhed i net og informationssystemer og beredskab. Center for Cybersikkerheds beslutning om at overgive sager til politimæssig efterforskning vil også kunne offentliggøres efter bestemmelsen.

Efter *nr. 2*, kan centeret endvidere offentliggøre resultater af tilsyn udført efter § 22, stk. 1. Sådanne tilsynsresultater kan omfatte centerets tilsynsrapporter, ligesom det vil kunne omfatte statistik, eksempelvis i form af en kvartalvis eller årlig opgørelse over antallet af påbud til de enkelte teleudbydere.

Det foreslås endvidere med *nr. 3*, at resuméer af domme eller bødevedtagelser, hvor der idømmes eller vedtages en bøde for overtrædelse af denne lov eller regler, der er udstedt i medfør af denne lov, skal kunne offentliggøres.

Herudover skal der efter *nr. 4*, kunne ske offentliggørelse af resuméer af domme i retssager vedrørende sikkerhed i net og informationssystemer og beredskab på teleområdet, og hvor Center for Cybersikkerhed er part. Der

sker ikke med bestemmelsen en fravigelse af retsplejelovens regler om aktindsigt i domme.

Offentliggørelse vil ske på Center for Cybersikkerheds hjemmeside i ikke-anonymiseret form. Det vil således fremgå af det offentliggjorte materiale, hvilken udbyder afgørelsen, tilsynsresultatet, dommen eller bødevedtagelsen er rettet imod.

Det foreslås i *stk. 2*, at offentliggørelse efter stk. 1 ikke må indeholde 1) oplysninger om tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold el. lign., for så vidt det er af væsentlig økonomisk betydning for den væsentlige teleudbydere eller vigtige teleudbyder, som oplysningerne angår, 2) oplysninger, der er af væsentlig betydning for statens sikkerhed eller rigets forsvar, 3) klassificerede informationer, 4) fortrolige oplysninger, der hidrører fra nationale tilsynsmyndigheder i andre EU-medlemsstater, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelse, eller 5) oplysninger om enkeltpersoners forhold.

Bestemmelsen viderefører indholdet af § 10, stk. 2, i lov om sikkerhed i net og tjenester.

Det foreslås med *nr. 1*, at offentliggørelsen ikke må indeholde oplysninger vedrørende tekniske indretninger eller fremgangsmåder eller om drifts- eller forretningsforhold eller lignende, for så vidt det er af væsentlig økonomisk betydning for den væsentlige teleudbyder eller vigtige teleudbyder, oplysningerne angår. Definitionen af oplysninger vedrørende tekniske indretninger mv. skal forstås i overensstemmelse med § 30, nr. 2, i offentlighedsloven og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

Efter *nr. 2*, vil oplysninger undtages fra offentliggørelse i det omfang, det er af væsentlig betydning for statens sikkerhed eller rigets forsvar. Vurderingen af, hvornår offentliggørelse af oplysninger kan være af væsentlig betydning for statens sikkerhed eller rigets forsvar, skal foretages i overensstemmelse med principperne i § 31 i offentlighedsloven.

Desuden vil klassificerede informationer efter *nr. 3*, blive slettet i det materiale, der offentliggøres.

Efter *nr. 4*, vil der endvidere ikke ske offentliggørelse af fortrolige oplysninger, der hidrører fra myndigheder i andre EU-medlemsstater, jf. den fo-

reslåede § 31, stk. 2, medmindre de myndigheder, der har afgivet oplysningerne, har givet deres udtrykkelige tilladelse til offentliggørelsen.

Endelig vil enkeltpersoners forhold efter *nr. 5* blive slettet inden offentliggørelsen. Det kan eksempelvis være oplysninger om navne, adresser eller telefonnumre på klagere eller andre berørte parter, som vil skulle undtages fra offentliggørelsen.

Det bemærkes i øvrigt, at Center for Cybersikkerhed forudsættes ikke at offentliggøre afgørelser eller tilsynsresultater, såfremt efterforskningsmæssige hensyn taler derimod.

Det foreslås i *stk. 3*, at Center for Cybersikkerhed kan fastsætte nærmere regler om sagsbehandlingen i forbindelse med offentliggørelse efter stk. 1.

Bestemmelsen er en videreførelse af § 10, stk. 3, i lov om sikkerhed i net og tjenester.

Bestemmelsens stk. 3, bemyndiger Center for Cybersikkerhed til at fastsætte nærmere regler for centerets sagsbehandling i forbindelse med offentliggørelser efter stk. 1.

Center for Cybersikkerhed vil med hjemmel i bestemmelsen eksempelvis kunne fastsætte regler for, hvornår der kan ske offentliggørelse. Center for Cybersikkerhed vil endvidere kunne fastsætte regler om forudgående høring eller orientering af en udbyder vedrørende spørgsmålet om en forestående offentliggørelse af en afgørelse eller tilsynsresultat mv.

Center for Cybersikkerhed vil herudover kunne fastsætte regler om, at det skal fremgå af offentliggørelsen, såfremt en afgørelse er påklaget til Ministeriet for Samfundssikkerhed og Beredsab, eller såfremt der verserer en sag for domstolene.

Endelig vil Center for Cybersikkerhed kunne fastsætte regler om, hvor lang tid den pågældende afgørelse, tilsynsresultat mv. skal være offentligt tilgængelige på centerets hjemmeside.

Til § 28

Det foreslås i *stk. 1,* at de forpligtelser, der er fastsat i denne lov eller i regler udstedt i medfør af loven, ikke omfatter meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser af hensyn til den nationale sikkerhed, offentlige sikkerhed eller forsvar.

Bestemmelsen gennemfører artikel 2, stk. 11, i 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), for så vidt angår telesektoren. Artikel 2, stk. 11, fastsætter, at de forpligtelser, der er fastsat i direktivet, ikke omfatter meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar.

Baggrunden for artikel 2, stk. 11, er beskrevet i NIS 2-direktivets præambelbetragtning nr. 9, 4. pkt., hvor det fremgår, at ingen medlemsstat bør være forpligtet til at meddele oplysninger, hvis videregivelse efter dens opfattelse ville stride mod dens væsentlige interesser med hensyn til national sikkerhed, offentlig sikkerhed eller forsvar. Det følger samme sted, at nationale regler eller EU-regler om beskyttelse af fortrolige oplysninger, hemmeligholdelsesaftaler og uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol, bør tages i betragtning i denne sammenhæng. Traffic Light Protocol skal forstås som et middel til at informere om eventuelle begrænsninger, for så vidt angår den videre spredning af oplysninger. Den anvendes i næsten alle enheder, der håndterer it-sikkerhedshændelser (CSIRT'er), og i nogle informationsanalyse- og informationsdelingscentre.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 2, stk. 11, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Under hensyn til bestemmelsen i NIS 2-direktivets artikel 2, stk. 7 (om at direktivet ikke finder anvendelse på offentlige forvaltningsenheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse), og den foreslåede bestemmelse i § 1, stk. 4 (om undtagelse af specifikke enheder, der udfører aktiviteter inden for national sikkerhed, offentlig sikkerhed, forsvar eller retshåndhævelse mv.), er det Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at den foreslåede bestemmelse i § 2, stk. 1, vil have et begrænset anvendelsesområde.

Det følger af det foreslåede *stk. 2*, at oplysninger, der modtages eller hidrører fra myndigheder i andre EU-medlemsstater, behandles som fortrolige, såfremt den afgivende myndighed betragter oplysningerne som fortrolige i henhold til EU-regler eller nationale regler.

Den foreslåede bestemmelse vil bl.a. sikre, at oplysninger, som de danske myndigheder modtager fra andre medlemsstater eller EU-institutioner i medfør af NIS 2-direktivets artikel 23, stk. 6, vil blive behandlet med den fornødne fortrolighed.

Det følger således af NIS 2-direktivets artikel 23, stk. 6, at hvor det er relevant, og navnlig hvor en væsentlig hændelse berører to eller flere medlemsstater, informerer CSIRT'en, den kompetente myndighed eller det centrale kontaktpunkt uden unødigt ophold de øvrige berørte medlemsstater og ENISA om den væsentlige hændelse.

Den foreslåede bestemmelse vil finde anvendelse, uanset om oplysningerne modtages direkte fra den pågældende nationale myndighed eller via andre, herunder Europa-Kommissionen.

Til § 29

Det foreslås i *stk. 1*, at Center for Cybersikkerhed hos udbydere, der er omfattet af § 14, stk. 3, kan indsamle oplysninger med henblik på at videregive disse til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater, idet omfang det er nødvendigt for, at disse kan opfylde deres opgaver i forhold til traktatmæssige forpligtelser eller forpligtelser i henhold til den gældende EU-ret.

Bestemmelsen viderefører – for så vidt angår udbydere omfattet af den foreslåede § 14, stk. 3 – § 12, stk. 1, i lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021.

Bestemmelsen gennemfører delvist artikel 20, stk. 2, i EU's telekodeks samt artikel 40, stk. 2, i EU's telekodeks, som ophæves ved artikel 43 i NIS 2-direktivet.

Efter det foreslåede stk. 1, kan Center for Cybersikkerhed indsamle oplysninger om sikkerhed i net og informationssystemer og beredskab på teleområdet hos udbydere, der er omfattet af den foreslåede § 14, stk. 3, med henblik på at videregive oplysningerne til Kommissionen eller nationale tilsynsmyndigheder i andre EU-medlemsstater. Det foreslås, at bestemmelsen også skal omfatte indsamling af oplysninger om sikkerhed i net og informationssystemer med henblik på videregivelse af oplysningerne til ENISA, som har til opgave at sikre en høj grad af net- og informationssikkerhed i EU, og som

bl.a. fungerer som et forum for erfaringsudveksling for de nationale tilsynsmyndigheder.

Det foreslås i *stk. 2*, at Center for Cybersikkerhed orienterer de udbydere, der er omfattet af § 14, stk. 3, og som der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til Kommissionen, Den Europæiske Unions Agentur for Cybersikkerhed eller nationale tilsynsmyndigheder i andre EU-medlemsstater.

Bestemmelsen viderefører – for så vidt angår udbydere omfattet af den foreslåede § 14, stk. 3 – § 12, stk. 2, i lov om sikkerhed i net og tjenester.

Bestemmelsen gennemfører delvist artikel 20, stk. 2, i EU's telekodeks.

Efter det foreslåede stk. 2 skal udbydere, der er omfattet af den foreslåede § 14, stk. 3, hvis oplysninger videregives til Kommissionen eller til myndigheder i andre EU-medlemsstater, orienteres forud for videregivelsen. Center for Cybersikkerhed skal ikke afvente udbyderens eventuelle kommentarer eller accept af videregivelsen. Det vil således være tilstrækkeligt, at der i forbindelse med indsamlingen af oplysningerne orienteres om videregivelsen. På baggrund af det foreslåede stk. 1, vedrørende videregivelse af oplysninger til ENISA, foreslås det, at Center for Cybersikkerhed også orienterer de udbydere, der er indsamlet oplysninger fra, forud for videregivelse af oplysningerne til ENISA.

Til § 30

Det foreslås i *stk. 1,* at hvor en væsentlig teleudbyder eller en vigtig teleudbyder leverer tjenester i mere end én medlemsstat i Den Europæiske Union, eller hvor udbyderen leverer tjenester i en eller flere medlemsstater, og udbyderens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder Center for Cybersikkerhed med de andre medlemsstaters kompetente myndigheder i relevant omfang. Samarbejdet indebærer, at: 1) Center for Cybersikkerhed underretter de kompetente myndigheder i relevante medlemsstater om tilsyns- og håndhævelsesforanstaltninger, 2) Center for Cybersikkerhed kan anmode en anden medlemsstats kompetente myndigheder om at anvende tilsyns- og håndhævelsesforanstaltninger, og 3) Center for Cybersikkerhed yder i rimeligt omfang bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom.

Bestemmelsen vil gennemføre artikel 37, stk. 1, i NIS 2-direktivet, for så vidt angår telesektoren. Det følger af artikel 37, stk. 1, at hvor en enhed leverer tjenester i mere end én medlemsstat, eller hvor den leverer tjenester i en eller flere medlemsstater og dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder de kompetente myndigheder i de pågældende medlemsstater med og bistår hinanden efter behov. Dette samarbejde indebærer mindst: a) at de kompetente myndigheder, der anvender tilsyns- eller håndhævelsesforanstaltninger i en medlemsstat, via det fælles kontaktpunkt underretter og hører de kompetente myndigheder i de øvrige berørte medlemsstater om de tilsyns- og håndhævelsesforanstaltninger, der er truffet, b) at en kompetent myndighed kan anmode en anden kompetent myndighed om at træffe tilsyns- eller håndhævelsesforanstaltninger, og c) at en kompetent myndighed efter modtagelse af en begrundet anmodning fra en anden kompetent myndighed yder bistand til den anden kompetente myndighed, der står i et rimeligt forhold til dens egne ressourcer, således at tilsyns- eller håndhævelsesforanstaltningerne kan gennemføres på en effektiv, virkningsfuld og konsekvent måde.

Det følger af NIS 2-direktivets artikel 37, stk. 1, 2. led, at den gensidige bistand, der er omhandlet i litra c, kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller eksternt tilsyn eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, må ikke afvise anmodningen, medmindre det er fastslået, at den ikke er kompetent til at yde den ønskede bistand, at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds tilsynsopgaver, eller anmodningen vedrører oplysninger eller indebærer aktiviteter, som, hvis de blev videregivet eller udført, ville stride mod den medlemsstats væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før den kompetente myndighed afslår en sådan anmodning, hører den de øvrige berørte kompetente myndigheder samt, efter anmodning fra en af de berørte medlemsstater, Europa-Kommissionen og ENISA.

Den foreslåede bestemmelse svarerindholdsmæssigt til NIS 2-direktivets artikel 37, stk. 1, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse indebærer, at Center for Cybersikkerhed i relevant omfang skal samarbejde med de kompetente myndigheder i andre medlemsstater om deres opgaveudførelse vedrørende væsentlige og vigtige teleudbydere, der leverer tjenester i mere end én medlemsstat i Den Euro-

pæiske Union, og udbyderens net- og informationssystemer er beliggende i én eller flere andre medlemsstater.

Samarbejdet indebærer, at der skal ske underretning af de kompetente myndigheder i relevante medlemsstater om anvendte tilsyns- og håndhævelsesforanstaltninger. At der skal ske underretning til kompetente myndigheder i »relevante medlemsstater« betyder, at der skal ske underretning til de kompetente myndigheder i medlemsstater, hvor udbyderen leverer tjenester, eller hvor udbyderens net- og informationssystemer er beliggende.

Samarbejdet indebærer desuden, at Center for Cybersikkerhed kan anmode en anden medlemsstats kompetente myndigheder om at iværksætte tilsyns- og håndhævelsesforanstaltninger.

Samarbejdet indebærer endvidere, at Center for Cybersikkerhed i rimeligt omfang skal yde bistand til en anden medlemsstats kompetente myndighed efter modtagelse af en begrundet anmodning herom. Denne bistand kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder eksempelvis anmodninger om at foretage kontrol på stedet eller målrettede sikkerhedsaudits.

En anmodning om bistand kan afvises, hvis anmodningen ikke står i rimeligt forhold til Center for Cybersikkerheds tilsynsopgaver og ressourcer.

En anmodning om bistand kan desuden afvises, hvis anmodningen vedrører videregivelsen af oplysninger eller indebærer udførelsen af aktiviteter, som ville stride mod væsentlige interesser med hensyn til national sikkerhed, offentlige sikkerhed eller forsvar. Før der kan ske afvisning af en anmodning, skal Center for Cybersikkerhed høre de relevante kompetente myndigheder i andre medlemsstater samt, efter anmodning fra en af de relevante kompetente myndigheder i andre medlemsstater, Europa-Kommissionen og ENISA.

Efter NIS 2-direktivets præambelbetragtning nr. 134 er formålet med bestemmelsen i direktivets artikel 37 at sikre, at enhederne overholder de forpligtelser, der er fastsat i direktivet. En anmodning om gensidig bistand efter den foreslåede stk. 1 vil derfor ikke blive imødekommet, såfremt anmodningen entydigt vedrører en anden medlemsstats nationale overimplementering af NIS 2- direktivet.

Det følger af det foreslåede *stk. 2*, at Center for Cybersikkerhed efter nærmere aftale kan gennemføre fælles tilsynstiltag med kompetente myndigheder fra andre medlemsstater i Den Europæiske Union.

Bestemmelsen vil gennemføre NIS 2-direktivets artikel 37, stk. 2, for så vidt angår telesektoren. Det følger af artikel 37, stk. 2, at hvor det er hensigtsmæssigt og efter fælles overenskomst, kan de kompetente myndigheder fra forskellige medlemsstater gennemføre fælles tilsynstiltag.

Den foreslåede bestemmelse svarer således indholdsmæssigt til NIS 2-direktivets artikel 37, stk. 2, og skal forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Der stilles med den foreslåede bestemmelse ikke nærmere formkrav til den aftale, der indgås om udførelsen af fælles tilsynstiltag.

Den foreslåede bestemmelse indebærer ikke, at andre medlemsstaters myndigheder selvstændigt kan udøve tilsynsbeføjelser her i landet.

Til § 31

Det følger af den foreslåede *§ 31,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen i medfør af NIS 2-direktivet.

Europa-Kommissionen er flere steder NIS 2-direktivet tillagt kompetence til at vedtage retsakter, der nærmere udmønter bestemte dele af direktivet.

For så vidt angår væsentlige teleudbydere og vigtige teleudbydere, kan Europa-Kommissionen i medfør af artikel 21, stk. 5, 2. led, vedtage gennemførelsesretsakter, der fastsætter de tekniske og metodologiske samt om nødvendigt sektorspecifikke krav til de foranstaltninger, der er omhandlet i direktivets artikel 21, stk. 2 (foranstaltninger til styring af cybersikkerhedsrisici).

Ved udarbejdelsen af de nævnte gennemførelsesretsakter følger Europa-Kommissionen i videst muligt omfang europæiske og internationale standarder samt relevante tekniske specifikationer. Europa-Kommissionen samarbejder med samarbejdsgruppen og ENISA om udkastene til gennemførelsesretsakter.

Det følger desuden af NIS 2-direktivets artikel 23, stk. 11, at Europa-Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer

typen af oplysninger, formatet og proceduren for en underretning indgivet i henhold til artikel 23, stk. 1 (underretning af myndighederne om hændelser), og artikel 30 (frivillig meddelelse af relevante oplysninger) og for en meddelelse, der er indgivet i henhold til artikel 23, stk. 2 (oplysning til modtagerne af tjenester).

Det følger endvidere af NIS 2-direktivets artikel 24, stk. 2, at Europa-Kommissionen tillægges beføjelser til at vedtage delegerede retsakter for at supplere NIS 2-direktivet ved at præcisere, hvilke kategorier af væsentlige og vigtige enheder der skal anvende visse certificerede IKT-produkter, -tjenester og -processer eller indhente en attest i henhold til en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til artikel 49 i Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed). Disse delegerede retsakter vedtages, når der er identificeret utilstrækkelige cybersikkerhedsniveauer og skal indeholde en gennemførelsesperiode.

Ministeren for samfundssikkerhed og beredskab får efter bestemmelsen hjemmel til inden for telesektoren at fastsætte regler, som er nødvendige for at gennemføre retsakter udstedt af Europa-Kommissionen.

Til § 32

Det følger af den foreslåede *§ 32,* at ministeren for samfundssikkerhed og beredskab kan fastsætte regler om digital kommunikation, herunder om anvendelsen af bestemte it-systemer og særlige digitale formater samt digital signatur eller lignende.

Den foreslåede bestemmelse indebærer, at det kan gøres obligatorisk for væsentlige teleudbydere og vigtige teleudbydere at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Der kan endvidere med hjemmel i bestemmelsen fastsættes regler om, hvem der omfattes af pligten til at kommunikere digitalt, om hvilke forhold, og på hvilken måde.

Bestemmelsen forventes navnlig anvendt til at fastsætte regler om, hvordan væsentlige teleudbydere og vigtige teleudbydere skal foretage underretninger om hændelser i medfør af de foreslåede §§ 9 og 10. Der vil eksempelvis

kunne fastsættes regler om anvendelse af bestemte digitale internetløsninger såsom Virk.dk. Det kan eksempelvis også være relevant at fastsætte regler om, at bl.a. registreringspligterne i de foreslåede § 8 skal efterkommes ved anvendelse af bestemte internetløsninger såsom Virk.dk.

Der kan med hjemmel i bestemmelsen fastsættes regler om, at skriftlige henvendelser til Center for Cybersikkerhedom forhold, som er omfattet af et krav om digital kommunikation, ikke anses for behørigt modtaget af centret, hvis de indsendes på anden vis end den foreskrevne digitale måde.

Hvis en væsentlig eller vigtig teleudbyder retter henvendelse til Center for Cybersikkerhed på anden måde end den foreskrevne digitale måde, følger det af den almindelige vejledningspligt, jf. forvaltningslovens § 7, stk. 2, at centret skal vejlede om reglerne på området, herunder om pligten til at kommunikere digitalt.

Der kan desuden fastsættes regler om fritagelse for pligten til digital kommunikation. Fritagelsesmuligheden tænkes navnlig anvendt, hvor det er påkrævet at anvende en dansk digital signatur, men der er tale om en virksomhed med hjemsted i udlandet, og som dermed ikke kan få udstedt en dansk digital signatur. Det bemærkes i den forbindelse, at fritagelsesmuligheden er stærkt begrænset, idet der er tale om kommunikation om erhvervsforhold, og idet virksomheder med hjemsted i udlandet kun i begrænset omfang vil høre under dansk jurisdiktion.

Det forhold, at en væsentlig eller vigtig teleudbyders computere ikke fungerer, at udbyderen har mistet koden til sin digitale signatur, eller at der opstår lignende hindringer, som det er op til udbyderen at overvinde, vil ikke kunne føre til fritagelse for pligten til digital kommunikation. I så fald må den pågældende udbyder eksempelvis anmode en rådgiver om at varetage kommunikationen på virksomhedens vegne.

Der kan efter bestemmelsen også fastsættes regler om, at en digital meddelelse anses for at være kommet frem til adressaten for meddelelsen på det tidspunkt, hvor meddelelsen er tilgængelig digitalt for adressaten. Dermed er der tale om samme retsvirkning som ved fysisk post, der anses for at være kommet frem, når den pågældende meddelelse mv. er lagt i adressatens fysiske postkasse. En meddelelse vil normalt anses for at være kommet frem, når meddelelsen er tilgængelig digitalt for adressaten, således at vedkommende har mulighed for at behandle meddelelsen. Dette tidspunkt vil normalt blive registreret automatisk i adressatens it-system.

Det bemærkes, at Europa-Kommissionen på visse punkter er tillagt kompetence til at fastsætte nærmere regler om, hvordan oplysninger skal afgives fra de væsentlige teleudbydere og de vigtige teleudbydere. Europa-Kommissionen kan således bl.a. fastsætte nærmere regler om formatet og proceduren for en underretning indgivet i henhold til artikel 23, stk. 1 (underretning af myndighederne om hændelser), og artikel 30 (frivillig meddelelse af relevante oplysninger) og for en meddelelse, der er indgivet i henhold til artikel 23, stk. 2 (oplysning til modtagerne af tjenester). Såfremt Europa-Kommissionen måtte vælge at udnytte denne kompetence til at fastsætte nærmere regler, vil det skulle sikres, at regler om digital kommunikation, der måtte være udstedt eller siden udstedes i medfør af den foreslåede bestemmelse, er i overensstemmelse med Europa-Kommissionens retsakter.

Til § 33

Det foreslås i *stk. 1,* at den, der 1) overtræder § 5, stk. 1, eller 2, eller §§ 6, 8-10 eller 12, 2) undlader at efterkomme Center for Cybersikkerheds afgørelse efter 27, stk. 1, 3) undlader at efterkomme påbud eller forbud §§ 22 eller 25, 4) undlader at efterkomme krav efter § 13, stk. 2, § 21, stk. 1, nr. 2 eller nr. 5-7, § 24, stk. 1, nr. 2 eller nr. 4-6, eller 5) hindrer Center for Cybersikkerhed i at føre tilsyn efter bestemmelserne i § 21, stk. 1, nr. 1-4, eller § 24, stk. 1, nr. 1-3, eller i at få adgang efter bestemmelsen i § 22, straffes med bøde.

Den foreslåede bestemmelse vil gennemføre artikel 36, stk. 1, NIS 2-direktivet. Artikel 36, stk. 1, forpligter medlemsstaterne til at fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale foranstaltninger, der er vedtaget i medfør af NIS 2-direktivet og til at træffe alle nødvendige foranstaltninger for at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Den foreslåede bestemmelse svarer med sproglige tilpasninger indholdsmæssigt til NIS 2-direktivets artikel 36, stk. 1, og skal således forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Den foreslåede bestemmelse vil endvidere gennemføre NIS 2-direktivets artikel 34, hvoraf det følger, at medlemsstaterne sikrer, at de administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til artiklen, for så vidt angår overtrædelser af direktivet, er effektive, står i rimeligt forhold

til overtrædelsen og har afskrækkende virkning, under hensyntagen til omstændighederne i hver enkelt sag.

Efter artikel 34, stk. 2, kan administrative bøder pålægges i tillæg til en hvilken som helst af foranstaltningerne omhandlet i artikel 32, stk. 4, litra a-h, artikel 32, stk. 5, og artikel 33, stk. 4, litra a-g.

Efter artikel 34, stk. 4, skal medlemsstaterne sikre, at hvor væsentlige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med artiklernes stk. 2 og 3 med administrative bøder med et maksimum på mindst 10.000.000 euro eller et maksimum på mindst 2 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

Det følger af artikel 34, stk. 5, at medlemsstaterne sikrer, at hvor vigtige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med artiklernes stk. 2 og 3 med administrative bøder med et maksimum på mindst 7.000.000 euro eller et maksimum på mindst 1,4 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efsssster hvad der er højest.

Det følger endvidere af artikel 34, stk. 8, 1. og 2. pkt., at hvis en medlemsstats retssystem ikke giver mulighed for at pålægge administrative bøder, sørger den pågældende medlemsstat for, at artiklen anvendes på en sådan måde, at den kompetente myndighed tager skridt til bøder, og de kompetente nationale domstole pålægger dem, idet det sikres, at disse retsmidler er effektive, og at deres virkning svarer til virkningen af administrative bøder, som pålægges af de kompetente myndigheder. De bøder, der pålægges, skal under alle omstændigheder være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning.

Endelig vil den foreslåede bestemmelse – i kombination med den foreslåede bestemmelse i § 6, stk. 1 – gennemføre NIS 2-direktivets artikel 20, stk. 1, hvoraf det følger, at medlemsstaterne sikrer, at de væsentlige og vigtige teleudbyderes ledelsesorganer godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 21, fører tilsyn med dens gennemførelse og kan gøres ansvarlige for enhedernes overtrædelser af forpligtelserne i nævnte artikel.

Det forudsættes i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 4, at bødens størrelse for væsentlige teleudbydere maksimalt vil udgøre et beløb svarende til 10.000.000 euro eller 2 pct.af den væsentlige teleudbyders samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Det forudsættes endvidere i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 5, at bødens størrelse for vigtige teleudbyderes maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct.af den vigtige teleudbyders samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Der forudsættes ikke i tilknytning til øvrige bestemmelser end de specifikt angivne ovenfor anlagt særlige forudsætninger for så vidt angår udmålingen af bøders størrelse. Det samme gælder eventuel udmåling af bøder til fysiske personer, hvor det dog i overensstemmelse med direktivets præambelbetragtning nr. 130, 2. pkt., forudsættes, at der lægges vægt på det generelle indkomstniveau og personens økonomiske stilling.

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 3, jf. artikel 32, stk. 7, at der lægges vægt på følgende hensyn ved pålæg af en bøde og ved udmåling af bødens størrelse: 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 kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i §§ 6, 12, 13, 15 og 16, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver fysisk eller ikke-fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den fysiske eller ikke-fysiske skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

De almindelige regler i straffelovens kapitel 10 om henholdsvis strafskærpende og strafformildende omstændigheder skal ligeledes iagttages ved anvendelsen af nærværende strafbestemmelser.

Den fastsatte bøde skal i overensstemmelse med NIS 2-direktivets artikel 34, stk. 1, være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning under hensyntagen til omstændighederne i den konkrete sag.

Bøde vil i overensstemmelse med NIS 2-direktivets artikel 34, stk. 2, kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 22, 23 og 25.

Det følger af det foreslåede *stk. 2,* at der kan pålægges selskaber mv. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Den foreslåede bestemmelse indebærer, at selskaber mv. (juridiske personer) kan pålægges strafansvar for overtrædelse af denne lov eller regler udstedt i medfør af loven efter reglerne i straffelovens kapitel 5.

Det følger af det foreslåede *stk. 3,* at hvor der er pålagt en bøde for overtrædelse af databeskyttelsesforordningen eller databeskyttelsesloven, kan der ikke pålægges en bøde for overtrædelse af denne lov eller regler udstedt i medfør af loven, hvis overtrædelsen skyldes den samme adfærd som den, der var genstand for bøden i medfør af nævnte forordning eller databeskyttelsesloven.

Den foreslåede bestemmelse vil gennemføre NIS 2-direktivets artikel 35, stk. 2, hvoraf det følger, at tilsynsmyndighederne efter Europa-Parlamentets og Rådets forordning af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) har pålagt en bøde i henhold til forordningens artikel 58, stk. 2, litra i, må de kompetente myndigheder efter NIS 2-direktivet ikke pålægge en bøde i henhold til NIS 2-direktivets artikel 34, der skyldes den samme adfærd som den, der var genstand for bøden efter databeskyttelsesforordningen.

Den foreslåede bestemmelse svarer indholdsmæssigt til NIS 2-direktivets artikel 35, stk. 2, og skal således forstås og anvendes i overensstemmelse med direktivets forudsætninger.

Center for Cybersikkerhed vil fortsat kunne anvende øvrige håndhævelsesforanstaltninger i medfør af denne lov, uagtet at der måtte være pålagt en bøde for overtrædelse af databeskyttelseslovgivningen.

Det følger af det foreslåede *stk. 4,* at der i regler udstedt i medfør af loven kan fastsættes straf i form af bøde for overtrædelse af regler udstedt i medfør af loven.

Med bestemmelsen bemyndiges ministeren for samfundssikkerhed og beredskab til at fastsætte straf i form af bøde for overtrædelse af bestemmelser i regler, som udstedes i medfør af loven.

Det følger af artikel 34, stk. 4, i NIS 2-direktivet, at medlemsstaterne skal sikre, at hvor væsentlige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 10.000.000 euro eller et maksimum på mindst 2 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den væsentlige enhed tilhører, alt efter hvad der er højest.

Efter NIS 2-direktivets artikel 34, stk. 5, skal medlemsstaterne sikre, at hvor vigtige enheder overtræder artikel 21 (foranstaltninger til styring af cybersikkerhedsrisici) eller artikel 23 (rapporteringsforpligtelser), straffes de i overensstemmelse med nærværende artikels stk. 2 og 3 med administrative bøder med et maksimum på mindst 7.000.000 euro eller et maksimum på mindst 1,4 pct. af den samlede globale årsomsætning i det foregående regnskabsår i den virksomhed, som den vigtige enhed tilhører, alt efter hvad der er højest.

Det forudsættes i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 4, at bødens størrelse for væsentlige teleudbydere maksimalt vil udgøre et beløb svarende til 10.000.000 euro eller 2 pct. af den væsentlige teleudbyders samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Det forudsættes i overensstemmelse med en minimumsimplementering af NIS 2-direktivets artikel 34, stk. 5, at bødens størrelse for vigtige teleudbyderes overtrædelse maksimalt vil udgøre et beløb svarende til 7.000.000 euro eller 1,4 pct. af den vigtige enheds samlede globale årsomsætning i det foregående regnskabsår alt efter, hvad der er højest.

Det forudsættes i overensstemmelse med NIS 2-direktivets artikel 34, stk. 3, jf. artikel 32, stk. 7, at der lægges vægt på følgende hensyn ved pålæg af en bøde og ved udmåling af bødens størrelse: 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 kompetente myndigheder, d) hindringer for audits eller overvågningsaktiviteter beordret af den kompetente myndighed efter konstatering af en overtrædelse og e) afgivelse af urigtige eller klart unøjagtige oplysninger vedrørende cybersikkerhedsrisikostyringsforanstaltninger eller rapporteringsforpligtelser, der er fastsat i §§ 6, 12, 13, 15 og 16, 2) overtrædelsens varighed, 3) den pågældende enheds relevante tidligere overtrædelser, 4) enhver fysisk eller ikke-fysisk skade, der er forårsaget, herunder ethvert finansielt eller økonomisk tab, virkninger for andre tjenester og antallet af brugere, der er berørt, 5) hvorvidt der ved overtrædelsen er handlet forsætligt eller uagtsomt, 6) enhver foranstaltning truffet af enheden for at forebygge eller afbøde den fysiske eller ikke-fysiske skade, 7) hvorvidt godkendte adfærdskodekser eller godkendte certificeringsmekanismer er overholdt, og 8) i hvilken udstrækning de fysiske eller juridiske personer, der holdes ansvarlige for overtrædelsen, samarbejder med de kompetente myndigheder.

De almindelige regler i straffelovens kapitel 10 om henholdsvis strafskærpende og strafformildende omstændigheder skal ligeledes iagttages ved anvendelsen af nærværende strafbestemmelser.

Den fastsatte bøde skal i overensstemmelse med NIS 2-direktivets artikel 34, stk. 1, være effektiv, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning under hensyntagen til omstændighederne i den konkrete sag.

Bøde vil i overensstemmelse med NIS 2-direktivets artikel 34, stk. 2, kunne pålægges i tillæg til håndhævelsesforanstaltningerne i de foreslåede §§ 22, 23 og 25.

Til § 34

Det foreslås i *stk. 1*, at loven træder i kraft den 1. juli 2025.

Det følger af artikel 41, stk. 1, i NIS 2-direktivet, at direktivet skal være gennemført i dansk ret senest den 17. oktober 2024 og træde i kraft senest

den 18. oktober 2024. Med den foreslåede bestemmelse vil loven træde i kraft 9 måneder efter direktivets implementeringsfrist.

Det foreslås i *stk. 2,* at lov om sikkerhed i net og tjenester, jf. lovbekendtgørelse nr. 153 af 1. februar 2021, som ændret ved § 18 i lov nr. 1156 af 8. juni 2021, ophæves ved denne lovs ikrafttræden.

Til § 35

Det foreslås, at loven ikke skal gælde for Færøerne og Grønland.

Til § 36

I lov om leverandørsikkerhed i den kritiske teleinfrastruktur, jf. lov nr. 1156 af 8. juni 2021, foretages følgende ændringer.

1. § 1, nr. 3, affattes således:

»3) Vigtig teleudbyder: En teleudbyder, som er identificeret som en vigtig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«

2. I § 1 indsættes som *nr. 4:*

»4) Væsentlig teleudbyder: En teleudbyder, som er identificeret som en væsentlig teleudbyder i henhold til lov om sikkerhed og beredskab i telesektoren.«

3. I § 2, stk. 1, § 3, stk. 1-2, og § 15, ændres »væsentlig erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester« til: »væsentlig eller vigtig teleudbyder«.