



UDKAST

Forslag

til

Lov om supplerende bestemmelser til forordningen om cyberrobusthed¹⁾

Kapitel 1

Formål og anvendelsesområde

§ 1. Loven supplerer Europa-Parlamentets og Rådets forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordningen om cyberrobusthed).

§ 2. Loven gælder for produkter med digitale elementer, der gøres tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk med digitale elementer i overensstemmelse med artikel 2, stk. 1, i forordningen om cyberrobusthed. Loven gælder dog ikke i de tilfælde, der er nævnt i artikel 2, stk. 2-8, i forordningen om cyberrobusthed.

Kapitel 2

Bemyndigelse af overensstemmelsesvurderingsorganer

§ 3. Styrelsen for Samfundssikkerhed udpeges som bemyndigende myndighed vedrørende overensstemmelsesvurderingsorganer i henhold til artikel 36, stk. 1, i forordningen om cyberrobusthed.

Stk. 2. Styrelsen for Samfundssikkerhed bemyndiger efter ansøgning overensstemmelsesvurderingsorganer, der lever op til kravene i artikel 39, stk. 2-12, i forordningen

1) I loven er der medtaget visse bestemmelser fra Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed), EU-Tidende, L af 20. november 2024. Ifølge artikel 288 i EUF-Traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af disse bestemmelser i loven er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

om cyberrobusthed, til at gennemføre opgaver i henhold til forordningens artikel 32 og bilag VIII.

Stk. 3. Konstaterer Styrelsen for Samfundssikkerhed, at et overensstemmelsesvurderingsorgan, der er bemyndiget efter stk. 2, overtræder kravene hertil, kan Styrelsen for Samfundssikkerhed fastsætte en rimelig tidsfrist for afhjælpning af de konstaterede overtrædelser. Styrelsen for Samfundssikkerhed kan endvidere begrænse eller suspendere bemyndigelsen i overensstemmelse med artikel 45 i forordningen om cyberrobusthed. Foretages der ikke tilstrækkelig afhjælpning inden for fristen, eller er der tale om gentagen eller særligt grov forsømmelse af forordningens krav, inddrager Styrelsen for Samfundssikkerhed bemyndigelsen.

Stk. 4. Styrelsen for Samfundssikkerhed kan i forbindelse med bemyndigelse efter stk. 2 fastsætte nærmere vilkår om, at et overensstemmelsesvurderingsorgan søger akkreditering på et senere tidspunkt med henblik på opretholdelse af bemyndigelsen, hvis der ikke på tidspunktet for bemyndigelse forelå en relevant akkrediteringsordning.

§ 4. Den Danske Akkrediteringsfond (DANAK) foretager efter artikel 36, stk. 2, i forordningen om cyberrobusthed den vurdering og overvågning af overensstemmelsesvurderingsorganer, der er omhandlet i artikel 36, stk. 1, i forordningen om cyberrobusthed i forbindelse med bemyndigelse, jf. § 3, stk. 2.

Stk. 2. DANAK kan inden for en ramme aftalt med Styrelsen for Samfundssikkerhed beregne sig betaling for sine ydelser i forbindelse med akkreditering af virksomheder. De aktuelle satser for DANAK's ydelser offentliggøres på DANAK's hjemmeside og kan erhverves hos DANAK.

Kapitel 3

Markedsovervågning

§ 5. Styrelsen for Samfundssikkerhed udpeges som markedsovervågningsmyndighed i overensstemmelse med artikel 52, stk. 2, i forordningen om cyberrobusthed, jf. dog stk. 2.

Stk. 2. Markedsovervågningsmyndigheder udpeget efter forordningen om kunstig intelligens for så vidt angår systemer, der er klassificeret som højrisiko-AI-systemer i medfør af forordningens artikel 6, varetager i overensstemmelse med artikel 52, stk. 14, i forordningen om cyberrobusthed markedsovervågning med produkter med digitale elementer, hvori sådanne systemer indgår.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med vedkommende minister fastsætte nærmere regler om tilrettelæggelse og koordinering af de markedsovervågningsopgaver, der er omfattet af stk. 2.

§ 6. Styrelsen for Samfundssikkerhed udpeges som national koordinerende myndighed for markedsovervågning efter forordningen om cyberrobusthed.

Stk. 2. Styrelsen for Samfundssikkerhed fastsætter som national koordinerende myndighed en national strategisk ramme for markedsovervågningen efter forordningen om cyberrobusthed samt koordinerer samarbejdet mellem markedsovervågningsmyndighederne, herunder i forbindelse med fælles aktiviteter efter forordningens artikel 59 og koordinerede kontrolaktioner efter forordningens artikel 60.

Stk. 3. De markedsovervågningsmyndigheder, der er nævnt i § 5, stk. 2, skal tilrettelægge deres markedsovervågning efter den nationale strategiske ramme, der er nævnt i stk. 2, og underretter straks Styrelsen for Samfundssikkerhed om afgørelser, foranstaltninger og konstateringer vedrørende produkters cybersikkerhed, der er truffet i medfør af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Stk. 4. Ministeren for samfundssikkerhed og beredskab kan efter forhandling med vedkommende minister fastsætte nærmere regler om samarbejde, koordinering og informationsudveksling mellem markedsovervågningsmyndighederne og markedsovervågningsmyndighederne og CSIRT'en.

§ 7. Markedsovervågningsmyndighederne kan afkræve alle oplysninger, som er nødvendige for myndighedernes virksomhed, fra fysiske og juridiske personer omfattet af forordningen om cyberrobusthed, herunder til fastlæggelse af om et forhold er omfattet af bestemmelserne i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

§ 8. Markedsovervågningsmyndighederne kan som led i markedsovervågning efter forordningen om cyberrobusthed, herunder evalueringer efter forordningens artikel 54, udtage ethvert produkt med digitale elementer, der er omfattet af forordningen om cyberrobusthed, herunder ved brug af skjult identitet, for at kontrollere, om produkter og de processer, som fabrikanten har indført, opfylder kravene i forordningen om cyberrobusthed.

Stk. 2. Markedsovervågningsmyndighederne kan efter anmodning herom kræve, at erhvervsdrivende stiller et produkt med digitale elementer til rådighed for kontrol og, hvis det er relevant for kontrollen, giver adgang til relevante produktrelaterede udviklings-, test-, produktions- eller driftsmiljøer, som fabrikanten råder over.

Stk. 3. Markedsovervågningsmyndighederne kan som led i den kontrol, der er nævnt i stk.1, foretage eller få foretaget tekniske undersøgelser af produktet og i den forbindelse indhente teknisk eller anden faglig bistand i relevant omfang.

Stk. 4. Markedsovervågningsmyndighederne kan kræve omkostninger forbundet med kontrol refunderet af den erhvervsdrivende, hvis der træffes afgørelse om

manglende overensstemmelse med krav i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

§ 9. Markedsovervågningsmyndighederne har, i det omfang det er nødvendigt for kontrol eller evaluering vedrørende et produkt med digitale elementer omfattet af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf, mod behørig legitimation og uden retskendelse adgang til erhvervsmæssige lokaliteter, hvor produktet findes eller kan antages at findes, herunder hvor produktet er installeret eller taget i brug, eller hvor der findes eller kan antages at findes oplysninger, dokumentation, systemer, data eller andet materiale, som er nødvendigt for kontrollen med produktet.

Stk. 2. Markedsovervågningsmyndighederne kan som led i den kontrol, der er omtalt i stk. 1, fotografere og optage video, herunder skærbilleder og skærmoptagelser, når det er nødvendigt for at dokumentere kontrollen eller evalueringen.

Kapitel 4

Støtteforanstaltninger for små- og mellemstore virksomheder

§ 10. Styrelsen for Samfundssikkerhed iværksætter, hvor det er relevant, følgende tiltag skræddersyet til mikrovirksomheders og små virksomheders behov:

1) Tilrettelæggelse af specifikke oplysnings- og uddannelsesaktiviteter om anvendelsen af forordningen om cyberrobusthed.

2) Oprettelse af en særlig kommunikationskanal for mikrovirksomheder og små virksomheder og, i det omfang det er relevant, lokale offentlige myndigheder med henblik på at yde rådgivning og besvare spørgsmål om gennemførelsen af forordningen om cyberrobusthed.

3) Støtte af afprøvnings- og overensstemmelsesvurderingsaktiviteter, herunder, hvor det er relevant, med støtte fra Det Europæiske Kompetencecenter for Cybersikkerhed.

Stk. 2. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oprettelse af reguleringsmæssige sandkasser for cyberrobusthed i overensstemmelse med artikel 33, stk. 2, i forordningen om cyberrobusthed.

Stk. 3. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om tiltag, jf. stk. 1, og regulatoriske sandkasser, jf. stk. 2.

Kapitel 5

Videregivelse af oplysninger, digital kommunikation, undtagelse fra aktindsigt og gennemførelsesretsakter

§ 11. Styrelsen for Samfundssikkerhed, de myndigheder, der er omhandlet i § 5, stk. 2, og CSIRT'en kan videregive oplysninger til andre myndigheder eller virksomheder, herunder i andre medlemsstater, og til institutioner i Den Europæiske Union for at varetage myndighedsopgaver i medfør af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

§ 12. Skriftlig kommunikation til og fra Styrelsen for Samfundssikkerhed, de myndigheder, der er nævnt i § 5, stk. 2, og CSIRT'en om forhold, som er omfattet af forordningen om cyberrobusthed, denne lov eller regler fastsat i medfør heraf, skal foregå digitalt, jf. dog stk. 2.

Stk. 2. De myndigheder, der er nævnt i stk. 1, kan undtage en virksomhed fra digital kommunikation, når særlige omstændigheder taler for det. En sådan undtagelse kan dog ikke ske for så vidt angår indberetninger efter artikel 14 i forordningen om cyberrobusthed.

Stk. 3. Vedkommende minister kan efter forhandling med ministeren for samfundssikkerhed og beredskab fastsætte nærmere regler om digital kommunikation og anvendelse af bestemte it-systemer og særlige digitale formater og lignende, herunder digital signatur.

Stk. 4. Ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om et adgangspunkt for fabrikanters elektroniske underretninger til CSIRT'en.

§ 13. Fabrikanters underretninger til CSIRT'en i medfør af artikel 14 i forordningen om cyberrobusthed og frivillige indberetninger, som omhandlet i forordningens artikel 15, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

§ 14. Ministeren for samfundssikkerhed og beredskab kan fastsætte regler, som er nødvendige for at gennemføre de af Den Europæiske Union udstedte beslutninger, som træffes med henblik på gennemførelse af forordningen om cyberrobusthed, eller regler, som er nødvendige for at anvende de af Den Europæiske Union udstedte retsakter på forordningens område.

Kapitel 6

Klageadgang

§ 15. Styrelsen for Samfundssikkerhed behandler klager over afgørelser truffet af bemyndigede overensstemmelsesvurderingsorganer og DANAK i henhold til forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Stk. 2. Klager efter stk. 1 skal indgives skriftligt til Styrelsen for Samfundssikkerhed. Klagen skal være modtaget senest 4 uger fra tidspunktet, hvor afgørelsen er meddelt. Udløber klagefristen på en lørdag, søndag eller helligdag, udskydes udløbet af fristen til den følgende hverdag. Klagen afvises, hvis den ikke indgives i overensstemmelse hermed, jf. dog stk. 3.

Stk. 3. De relevante myndigheder kan se bort fra en fristoverskridelse, eller at klagen i øvrigt ikke er indgivet i overensstemmelse med stk. 2, hvis særlige omstændigheder taler herfor.

Stk. 4. De relevante myndigheder kan i forbindelse med behandling af en klage indhente alle oplysninger, der er nødvendige for behandling af klagen, fra erhvervsdrivende omfattet af loven, det nationale akkrediteringsorgan, bemyndigede overensstemmelsesvurderingsorganer og andre myndigheder, der træffer afgørelse efter forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

§ 16. Afgørelser truffet af Styrelsen for Samfundssikkerhed eller de myndigheder, der er omtalt i § 5, stk. 2, efter forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf kan ikke indbringes for anden administrativ myndighed.

Kapitel 8

Straffebestemmelser

§ 17. Medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der

- 1) undlader at overholde de væsentlige cybersikkerhedskrav, der følger af bilag I i forordningen om cyberrobusthed, eller fabrikanternes forpligtelser i henhold til forordningens artikel 13 eller underretningsforpligtelser i henhold til artikel 14,
- 2) undlader at overholde forpligtelserne i forordningens artikel 18-23, artikel 28, artikel 30, stk. 1-4, artikel 31, stk. 1-4, artikel 32, stk. 1, 2 og 3, artikel 33, stk. 5, og artikel 39, 41, 47, 49 og 53 eller
- 3) afgiver ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning.

Stk. 2. Stk. 1 finder dog ikke anvendelse i følgende tilfælde:

- 1) Fabrikanters manglende overholdelse af den frist, som er omhandlet i forordningen om cyberrobustheds artikel 14, stk. 2, litra a, og stk. 4, litra a, når disse betragtes som mikrovirksomheder eller små virksomheder.
- 2) Enhver overtrædelse af forordningen om cyberrobusthed begået af open source software-forvaltere.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Stk. 4. I forskrifter, der udstedes i medfør af loven, kan der fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

Stk. 5. Forældelsesfristen for overtrædelse af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf er 5 år.

Kapitel 9

Ikrafttræden

§ 18. Loven træder i kraft den 1. marts 2027, jf. dog stk. 2.

Stk. 2. §§ 5-11 og 17 træder i kraft den 11. december 2027.

Kapitel 10

Territorialbestemmelse

§ 19. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget

Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning	10
2. Baggrund	11
2.1. Forordningen om cyberrobusthed	11
2.2. Sammenhæng med visse EU-retsakter	15
2.2.1. Markedsovervågningsforordningen	15
2.2.2. Forordningen om cybersikkerhed	17
2.2.3. Forordningen om kunstig intelligens	18
2.2.4. NIS 2-direktivet	19
3. Lovforslagets hovedpunkter	21
3.1. Anvendelsesområde	21
3.1.1. Gældende ret	21
3.1.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning	23
3.2. Udpegning af Styrelsen for Samfundssikkerhed som bemyndigende myndighed	24
3.2.1. Gældende ret	24
3.2.1.1. Bemyndigelse af overensstemmelsesvurderingsorganer	24
3.2.1.2. Ændring af bemyndigelser	26
3.2.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning	27
3.3. Udpegning af markedsovervågningsmyndigheder	30
3.3.1. Gældende ret	30
3.3.1.1. Markedsovervågning	30
3.3.1.2. Håndhævelsesbeføjelser	32
3.3.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning	37
3.4. Klageadgang	40

3.4.1. Gældende ret	40
3.4.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning	40
3.5. Sanktioner	41
3.5.1. Gældende ret	41
3.5.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning	42
4. Forholdet til databeskyttelsesloven og databeskyttelsesforordningen	44
5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige	47
6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.	48
7. Administrative konsekvenser for borgerne	49
8. Klimamæssige konsekvenser	49
9. Miljø- og naturmæssige konsekvenser	49
10. Forholdet til EU-retten	49
11. Hørte myndigheder og organisationer m.v.	49
12. Sammenfattende skema	50

1. Indledning

Der indgår i dag digitale elementer i en lang række produkter. Det gælder både i forbrugerprodukter som f.eks. smartwatches og babyalarmer og produkter af betydning for samfundets kritiske infrastruktur som f.eks. adgangssystemer i bygninger eller produkter til opretholdelse af et sikkert internet. Cyberangreb rettet mod sådanne produkter kan derfor have en kritisk indvirkning på ikke blot samfundsøkonomien, men også på forbrugernes sikkerhed og sundhed. Samtidig er det Europa-Kommissionens forventning, at antallet og mangfoldigheden af forbundne enheder vil stige eksponentielt i de kommende år.

På den baggrund fastsætter Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordningen om cyberrobusthed) rammebetingelserne for udvikling af sikre produkter med digitale elementer ved at sikre, at hardware- og softwareprodukter bringes i omsætning med færre sårbarheder, og at fabrikanterne tager sikkerhed alvorligt i hele produktets livscyklus.

Forordningen om cyberrobusthed fastsætter en række krav til produkter med et digitalt element, der er forbundet med andre enheder eller et netværk, og har dermed et bredt anvendelsesområde. Forordningen omfatter både fysiske produkter, såsom routere og babyalarmer med app-adgang, og softwareprodukter som f.eks. programmet til at styre routeren eller appen til at kunne tilgå babyalarmen.

Forordningens systematik er, at produkter med digitale elementer skal opfylde de væsentlige cybersikkerhedskrav i forordningens bilag 1, før de må bringes i omsætning eller gøres tilgængelige i EU.

For at sikre den nationale gennemførelse af disse krav pålægger forordningen medlemsstaterne at fastsætte nationale bestemmelser om bl.a. udpegning af en bemyndigende myndighed, markedsovervågningsmyndigheder, tilsyns- og håndhævelsesmekanismer, sanktioner og klageadgang. Danmark er således forpligtet til at indføre supplerende regler i dansk lovgivning med henblik på at understøtte arbejdet med de nye krav til produkter med digitale elementer.

Dette lovforslag har til formål at fastsætte de nødvendige supplerende bestemmelser for at sikre anvendelsen af forordningen om cyberrobusthed.

Det forslås, at Styrelsen for Samfundssikkerhed og visse myndigheder udpeget i henhold til forordningen om kunstig intelligens udpeges som kompetente myndigheder, der skal varetage de påkrævede og indbyrdes forbundne funktioner relateret til bemyndigelse af overensstemmelsesvurderingsorganer og tilsyn.

På den måde tilstræbes det også, at de nye regler om cyberrobusthed sammentænkes med de gældende regler på cyberområdet, herunder lov om cybersikkerhedscertificering og NIS 2-loven, da det foreslås, at de samme myndigheder udpeges i forhold til forordningen om cyberrobusthed. Formålet er at understøtte en mere sammenhængende cybersikkerhedsindsats i forhold til produkters sikkerhed, kritiske enheders risikostyring og dokumentation af cybersikkerhedsniveauer.

Det bemærkes, at forordningen om cyberrobusthed trådte i kraft den 10. december 2024 og finder anvendelse fra den 11. december 2027. Forordningens kapitel IV om bemyndigelse af overensstemmelsesvurderingsorganer, herunder kravet om at der udpeges en bemyndigende myndighed, finder dog anvendelse fra den 11. juni 2026, mens artikel 14 om fabrikanters rapporteringsforpligtelser gælder umiddelbart fra den 11. september 2026. Der vil således være tale om forsinket fastsættelse af de supplerende bestemmelser vedrørende udpegningen af den bemyndigende myndighed.

2. Baggrund

2.1. Forordningen om cyberrobusthed

Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordningen om cyberrobusthed) fastsætter harmoniserede regler om cybersikkerhed for produkter med digitale elementer med henblik på at styrke produkternes cyberrobusthed gennem deres forventede levetid gennem bl.a. væsentlige cybersikkerhedskrav til design, udvikling og produktion, overensstemmelsesvurdering, sårbarhedshåndtering, sikkerhedsopdateringer og markedsovervågning.

Forordningen om cyberrobusthed er direkte gældende i Danmark, jf. TEUF artikel 288, hvilket betyder, at reglerne ikke skal gennemføres i national ret. Derudover må der som udgangspunkt ikke være anden dansk lovgivning, der regulerer cybersikkerhedskrav i produkter med digitale elementer, i det omfang dette er reguleret i forordningen.

Der kan i den forbindelse henvises til præambelbetragtning nr. 13, hvoraf følger at i overensstemmelse med forordningens mål om at fjerne hindringerne for den frie bevægelighed for produkter med digitale elementer, må medlemsstaterne ikke hindre tilgængeliggørelse på markedet af produkter med digitale elementer, der opfylder

kravene i denne forordning, for så vidt angår spørgsmål, der er omfattet af forordningen om cyberrobusthed. For så vidt angår spørgsmål, der harmoniseres ved forordningen, kan medlemsstaterne derfor ikke pålægge yderligere cybersikkerhedskrav for tilgængeliggørelse på markedet af produkter med digitale elementer.

Baggrunden for forordningen er, at produkter med digitale elementer i stigende grad forbindes med og integreres i andre produkter, systemer og netværk. Cyberangreb og manglende cybersikkerhed i sådanne produkter kan have vidtrækkende konsekvenser for bl.a. demokratiet og EU's økonomi samt forbrugernes mulighed for at vælge og anvende produkter sikkert.

Derudover har produkter med digitale elementer ofte et lavt cybersikkerhedsniveau præget af udbredte sårbarheder og utilstrækkelige sikkerhedsopdateringer samtidig med, at brugerne også ofte mangler den nødvendige information til at kunne træffe sikre valg for så vidt angår deres produkter. Cyberangreb kan dermed forplante sig via tilsyneladende uskyldige enheder – f.eks. routere, smartwatches eller legetøj med interaktive funktioner – og få alvorlige konsekvenser for både forbrugere og virksomheder.

Den stigende udbredelse af produkter med digitale elementer – fra legetøj og husholdningsudstyr til industrielle systemer og kritisk infrastruktur – øger risikoen for, at sårbarheder kan udnyttes. Forordningen om cyberrobusthed skal styrke EU's tilgang til cyberrobusthed og fastsætter rammebetingelserne for udvikling af sikre produkter med digitale elementer ved at sikre, at hardware- og softwareprodukter bringes i omsætning med færre sårbarheder, og at fabrikanterne tager sikkerheden alvorligt i hele et produkts livscyklus.

Forordningen om cyberrobusthed er udformet efter den produktretlige model i EU's lovgivningsmæssige rammer for produktregler. Forordningen anvender dermed en række kendte elementer fra EU's harmoniserede produktregulering, herunder væsentlige krav, fabrikantforpligtelser, teknisk dokumentation, EU-overensstemmelseserklæring, CE-mærkning, overensstemmelsesvurdering, bemyndigede organer og markedsovervågning.

Forordningen indebærer samtidig, at en række forpligtelser rækker ud over tidspunktet, hvor produktet bringes i omsætning eller gøres tilgængeligt på markedet. Cybersikkerhedskravene retter sig således ikke alene mod produktets egenskaber på det tidspunkt, hvor produktet bringes i omsætning, men også mod fabrikantens efterfølgende

håndtering af sårbarheder og opretholdelse af cybersikkerhed i vedligeholdelsesperioden.

Det omfatter bl.a. sårbarhedshåndtering, sikkerhedsopdateringer, rapportering af aktivt udnyttede sårbarheder og alvorlige hændelser, der har indvirkning på produktets sikkerhed, samt håndtering af cybersikkerhedsrisici ved væsentlige ændringer.

Visse produkter klassificeres som vigtige eller kritiske produkter, hvilket ikke indebærer særskilte materielle cybersikkerhedskrav, men har betydning for, hvordan fabrikanten skal dokumentere produktets overensstemmelse med kravene i bilag 1, herunder hvilken overensstemmelsesvurderingsprocedure, der skal anvendes.

Forordningens kapitel I indeholder forordningens almindelige ramme, herunder bestemmelser om genstand, anvendelsesområde og definitioner (artikel 1-3).

Artikel 4 fastsætter princippet om fri bevægelighed for produkter, der opfylder forordningens krav, mens artikel 5 regulerer medlemsstaternes adgang til at stille yderligere cybersikkerhedskrav ved offentlige indkøb og forpligter medlemsstaterne til at sikre, at der i udbudsprocesser tages hensyn til forordningens væsentlige cybersikkerhedskrav, uden at dette dog berører Europa Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og Europa Parlamentets og Rådets direktiv 2014/25/EU af 26. februar 2014 om fremgangsmåderne ved indgåelse af kontrakter inden for vand- og energiforsyning, transport samt posttjenester (forsyningsvirksomhedsdirektivet).

Artikel 6 fastsætter det grundlæggende krav om, at produkter med digitale elementer kun må gøres tilgængelige på markedet, hvis de opfylder kravene i bilag I. Artikel 7 og 8 fastlægger reglerne om henholdsvis vigtige og kritiske produkter, som er knyttet til produktkategorierne i bilag III og IV. Produktkategorierne har navnlig betydning for, hvilken overensstemmelsesvurderingsprocedure fabrikanten skal anvende for at dokumentere produktets overensstemmelse med forordningens krav, hvor kritiske produkter kan underlægges krav om europæisk cybersikkerhedscertificering.

Artikel 9 og 10 vedrører henholdsvis Kommissionens løbende inddragelse af interesserede parter ved udarbejdelsen af foranstaltninger til gennemførelse af denne forordning samt medlemsstaternes forbedring af færdigheder i et cybermodstandsdygtigt digitalt miljø.

Artikel 11 fastlægger forordningens sammenhæng med Europa-Parlamentets og Rådets (EU) forordning nr. 2023/988 af 10. maj 2023 om produktsikkerhed i almindelighed (produktsikkerhedsforordningen), mens artikel 12 fastsætter særlige regler for højrisiko AI-systemer, herunder samspillet med en dokumenteret opnåelse af det påkrævede niveau af cybersikkerhedsbeskyttelse i henhold til artikel 15 i Europa-Parlamentets og Rådets forordning (EU) nr. 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens (forordningen om kunstig intelligens).

Forordningens kapitel II vedrører fabrikanter af de omfattede produkters forpligtelser, herunder bl.a. indberetning af aktivt udnyttede sårbarheder (artikel 13-17), importørers forpligtelser (artikel 19) og distributørers forpligtelser (artikel 20). Artikel 21 og 22 vedrører samspillet mellem disse, mens artikel 23 vedrører erhvervsdrivendes identifikation over for markedsovervågningsmyndighederne. Artikel 24 og 25 vedrører forpligtelserne for open source software-forvaltere og Kommissionens mulighed for at vedtage delegerede retsakter specifikt for sikkerhedsattestering af fri og open source-software. Artikel 26 forpligter Kommissionen til at offentliggøre vejledninger til de økonomiske aktører om anvendelsen af forordningen.

Kapitel III vedrører selve vurderingen af overensstemmelsen af produkter med digitale elementer (artikel 27-34), herunder regler om formodning for overensstemmelse i visse tilfælde, CE-mærkning og kravene til teknisk dokumentation.

Kapitel IV vedrører bemyndigelsesorganer, herunder medlemsstaternes udpegning af en bemyndigende myndighed (artikel 35-38), kravene for de overensstemmelsesvurderingsorganer, der herefter kan bemyndiges af myndigheden, myndighedernes reaktionsmuligheder og pligten for medlemsstaterne til at fastsætte en klageprocedure (artikel 39-51).

Kapitel V vedrører kravet om, at der udpeges en markedsovervågningsmyndighed samt denne myndigheds håndhævelsesbeføjelser og opgaver (artikel 52-60), herunder koordination på tværs af EU-medlemsstaterne. Der henvises til pkt. 3.3.1.2 for en nærmere gennemgang heraf.

Kapitel IV og V indeholder således en række pligter for medlemsstaterne i forhold til at fastsætte nationale supplerende bestemmelser, herunder udpegning af kompetente myndigheder. Det er dermed primært forpligtelserne i disse kapitler, der udmøntes med dette lovforslag.

Kapitel VI vedrører Kommissionens delegerede beføjelser og udvalgsproceduren (artikel 61 og 62), mens kapitel VII vedrører tavshedspligt for alle parter, der er involveret i anvendelsen af forordningen (artikel 63), medlemsstaternes pligt til at fastsætte sanktionsregler (artikel 64) og anvendelsen af Europa-Parlamentets og Rådets direktiv (EU) 2020/1828 af 25. november 2020 om adgang til anlæggelse af gruppesøgsmål til beskyttelse af forbrugernes kollektive interesser, hvis der anlægges gruppesøgsmål vedrørende overtrædelser af forordningen (artikel 65).

Kapitel VIII vedrører overgangsbestemmelser og afsluttende bestemmelser (artikel 66-71), herunder om tidspunktet for forordningens ikrafttræden og anvendelse.

2.2. Sammenhæng med visse EU-retsakter

De gældende EU-retsakter på cybersikkerhedsområdet regulerer visse cybersikkerhedsaspekter fra forskellige vinkler og omfatter bl.a. Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (forordningen om cybersikkerhed), forordningen om kunstig intelligens, Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor (DORA-forordningen) og Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet). Derudover finder Europa-Parlamentets og Rådets forordning (EU) 2019/1020 af 20. juni 2019 om markedsovervågning og produkt-overensstemmelse (markedsovervågningsforordningen) også anvendelse for produkter omfattet af forordningen om cyberrobusthed.

De nævnte retsakter fastsætter imidlertid ikke et generelt regelsæt med obligatoriske cybersikkerhedskrav til produkter med digitale elementer, men har dog alligevel en nær tilknytning til forordningen om cyberrobusthed.

2.2.1. Markedsovervågningsforordningen

Det følger af artikel 1, stk. 1, i markedsovervågningsforordningen, at forordningen har til formål at forbedre det indre markeds funktion ved at styrke markedsovervågningen af produkter, der er omfattet af EU-harmoniseringslovgivningen som omhandlet i artikel 2, for at sikre, at kun produkter, der overholder de gældende regler og opfylder krav om et højt beskyttelsesniveau for offentlige interesser såsom sundhed og sikkerhed i almindelighed, sundhed og sikkerhed på arbejdspladsen, forbrugerbeskyttelse,

miljøbeskyttelse og den offentlige sikkerhed og alle andre offentlige interesser, der er beskyttet af nævnte lovgivning, gøres tilgængelige på EU-markedet.

Af artikel 2 i markedsovervågningsforordningen fremgår det, at forordningen finder anvendelse på produkter, der er omfattet af den EU-harmoniseringslovgivning, der er anført i forordningens bilag I (»EU-harmoniseringslovgivningen«), medmindre der findes særlige bestemmelser med samme formål i EU-harmoniseringslovgivningen, der på en mere specifik måde regulerer særlige markedsovervågnings- og håndhævelsesaspekter.

Dette skal ses i sammenhæng med artikel 66 i forordningen om cyberrobusthed, der indebærer, at markedsovervågningsforordningens ændres således, at der i bilag 1 indsættes et nyt nr. 72, hvori der henvises til forordningen om cyberrobusthed.

På tilsvarende vis følger det af artikel 52, stk. 1, i forordningen om cyberrobusthed, at markedsovervågningsforordningen finder anvendelse på produkter med digitale elementer, der er omfattet af anvendelsesområdet for forordningen om cyberrobusthed.

Det fremgår derudover af præambelbetragtning nr. 106 i forordningen om cyberrobusthed, at markedsovervågning er et væsentligt instrument til at sikre en korrekt og ensartet anvendelse af EU-retten. Det er derfor hensigtsmæssigt at skabe juridiske rammer, inden for hvilke markedsovervågningen kan foretages på en passende måde. Reglerne om EU-markedsovervågning og kontrol af produkter, der indføres på EU-markedet, i markedsovervågningsforordningen finder anvendelse på produkter med digitale elementer, der er omfattet af nærværende forordnings anvendelsesområde.

Den markedsovervågning, der er beskrevet i forordningen om cyberrobusthed, vil således skulle foretages inden for den generelle ramme, som markedsovervågningsforordningen udgør, men i sammenhæng med de bestemmelser i forordningen om cyberrobusthed, hvori der er fastsat regler om markedsovervågning målrettet produkter med digitale elementer.

Begge regelsæt er som udgangspunkt umiddelbart anvendelige for markedsovervågningsmyndighederne, mens visse beføjelser kræver national gennemførelse, herunder dem der er opført i markedsovervågningsforordningens artikel 14, stk. 4. Det følger således heraf, at de beføjelser, som markedsovervågningsmyndighederne tillægges af medlemsstaterne, mindst skal omfatte de i bestemmelsen opførte beføjelser. Disse vedrører bl.a. at pålægge erhvervsdrivende at udlevere dokumenter, data og oplysninger om produkter og forsyningskæder samt beføjelsen til uden forudgående varsel at

få adgang til relevante lokaler, arealer eller transportmidler og at kunne erhverve produktprøver under skjult identitet.

Derudover følger det af markedsovervågningsforordningens artikel 15, stk. 1, at medlemsstaterne kan tillade deres markedsovervågningsmyndigheder at opkræve alle omkostninger ved deres aktiviteter fra den relevante erhvervsdrivende for så vidt angår tilfælde af manglende overensstemmelse.

For en nærmere gennemgang heraf, kan der henvises til det foreslåede §§ 8 og 9 samt bemærkningerne hertil.

2.2.2. Forordningen om cybersikkerhed

Forordningen om cybersikkerhed handler overordnet om certificering og fastlægger ENISA's (European Network and Information Security Agency) mandat samt en fælles europæisk ramme for cybersikkerhedscertificeringer for IKT-produkter, -tjenester og -processer (informations- og kommunikationsteknologi) og administrerede sikkerhedstjenester. EU's cybersikkerhedscertificeringsordninger kan bruges af fabrikanter til at dokumentere, at deres IKT-produkter, -tjenester og -processer og administrerede sikkerhedstjenester opfylder kravene i den pågældende certificeringsordning. Certificeringsordningen er som udgangspunkt frivillig, medmindre andet er fastsat i EU-retten eller medlemsstaters ret, og kan efter forordningen om cyberrobusthed under visse betingelser anvendes til at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i forordningen, herunder for vigtige produkter i klasse II og kritiske produkter.

I forhold til sammenhængen med forordningen om cyberrobusthed kan særligt artikel 8, stk. 1, heri nævnes, hvor Europa-Kommissionen i overensstemmelse med artikel 61 tillægges beføjelse til at vedtage delegerede retsakter med henblik på at fastlægge, hvilke kritiske produkter, der skal indhentes en europæisk cybersikkerhedsattest på et tillidsniveau, der som minimum er »betydeligt« i henhold til en europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til forordningen om cybersikkerhed, for at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i bilag 1 eller dele heraf, forudsat at der er vedtaget en europæisk cybersikkerhedscertificeringsordning, der dækker disse kategorier af produkter med digitale elementer, og at den er tilgængelig for fabrikanterne.

Derudover kan også nævnes artikel 27 i forordningen om cyberrobusthed vedrørende overensstemmelsesformodning, herunder bestemmelsens stk. 8, hvorefter produkter med digitale elementer og processer indført af fabrikanten, for hvilke der er udstedt en EU-overensstemmelseserklæring eller en europæisk cybersikkerhedsattest i henhold

til en europæisk cybersikkerhedscertificeringsordning vedtaget i medfør af forordningen om cybersikkerhed, formodes at være i overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I i forordningen om cyberrobusthed i det omfang, at erklæringen eller attesten eller dele heraf dækker disse krav.

Yderligere kan nævnes artikel 32, stk. 3, litra c, i forordningen om cyberrobusthed, hvorefter fabrikanter af vigtige produkter i klasse II har mulighed for at kunne påvise overensstemmelse ved anvendelse af en europæisk cybersikkerhedscertificeringsordning. Det forudsætter dog, at ordningen er omfattet af artikel 27, stk. 9, og er tilgængelig og finder anvendelse på det pågældende produkt samt har et tillidsniveau, der som minimum er »betydeligt«. Artikel 27, stk. 9, giver EU-Kommissionens beføjelse til ved delegerede retsakter i overensstemmelse med artikel 61 at præcisere, hvilke europæiske cybersikkerhedscertificeringsordninger der kan anvendes til at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i bilag I eller dele heraf.

2.2.3. Forordningen om kunstig intelligens

Forordningen om kunstig intelligens har til formål at forbedre det indre markeds funktion og fremme udbredelsen af menneskecentreret og troværdig kunstig intelligens (AI) og samtidig sikre et højt niveau af beskyttelse af sundhed, sikkerhed og grundlæggende rettigheder.

I forhold til sammenhængen med forordningen om cyberrobusthed kan det nævnes, at et AI-system, der samtidig udgør et produkt med digitale elementer omfattet af forordningen om cyberrobusthed, som udgangspunkt skal opfylde kravene i begge forordninger.

For produkter med digitale elementer, der er klassificeret som højrisiko-AI-systemer i medfør af artikel 6 i forordningen om kunstig intelligens, følger der særlige regler af artikel 12 og artikel 52, stk. 14, i forordningen om cyberrobusthed vedrørende sammenhængen mellem de to forordningers cybersikkerhedskrav og overensstemmelsesvurderinger.

Det følger af artikel 12, stk. 1, i forordningen om cyberrobusthed, at sådanne produkter anses for at opfylde cybersikkerhedskravene i artikel 15 i forordningen om kunstig intelligens, hvis de væsentlige cybersikkerhedskrav i forordningen om cyberrobusthed er opfyldt, og det er dokumenteret i EU-overensstemmelseserklæringen, at det cybersikkerhedsniveau, der kræves efter artikel 15 i forordningen om kunstig intelligens, er opnået. Artikel 12, stk. 2 og 3, indeholder endvidere særlige regler om

overensstemmelsesvurderingen, herunder for visse vigtige og kritiske produkter med digitale elementer.

For så vidt angår markedsovervågningsmyndighederne er det bl.a. fastsat i artikel 52, stk. 14, i forordningen om cyberrobusthed, at for produkter med digitale elementer, der er omfattet af denne forordnings anvendelsesområde, og som er klassificeret som høj-risiko-AI-systemer i henhold til artikel 6 i forordningen om kunstig intelligens, skal de markedsovervågningsmyndigheder, der udpeges med henblik på nævnte forordning, være de myndigheder, der er ansvarlige for de markedsovervågningsaktiviteter, der kræves i henhold til nærværende forordning.

Der henvises i den forbindelse til det foreslåede § 5, stk. 2, og bemærkningerne hertil.

Disse myndigheder skal, hvor det er relevant, samarbejde med de markedsovervågningsmyndigheder, der er udpeget i henhold til forordningen om cyberrobusthed, og, for så vidt angår tilsynet med gennemførelsen af indrapporteringsforpligtelser efter artikel 14, med de CSIRT'er, der er udpeget som koordinatore, og med ENISA.

2.2.4. NIS 2-direktivet

NIS 2-direktivet har til formål at sikre et højt fælles cybersikkerhedsniveau ved at stille krav til enheders styring af cybersikkerhedsrisici og rapportering af væsentlige hændelser i 18 sektorer med henblik på at forebygge, opdage og håndtere hændelser. NIS 2-direktivet definerer, hvilke enheder, der som udgangspunkt er omfattet af kravene i direktivet. Enheder skal rapportere cyberhændelser, der har væsentlige konsekvenser for enhedernes samfundsvigtige tjenester inden for 24 timer til den nationale CSIRT.

NIS 2-direktivet er bl.a. implementeret i dansk ret ved lov nr. 434 af 6. maj 2025 om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven).

Det følger af præambelbetragtning nr. 24 i forordningen om cyberrobusthed, at forordningen, som finder anvendelse på alle hardware- og softwareprodukter, der kan forbindes, også har til formål at gøre det lettere for udbydere af digital infrastruktur at overholde kravene i forsyningskæden i henhold til NIS 2-direktivet ved at sikre, at de produkter med digitale elementer, som de anvender i forbindelse med leveringen af deres tjenester, udvikles på en sikker måde, og at de har adgang til rettidige sikkerhedsopdateringer for sådanne produkter.

For så vidt angår samspillet mellem forordningen om cyberrobusthed og både NIS 2-direktivet og forordningen om cybersikkerhed, kan det udledes af

præambelbetragtning nr. 107 i forordningen om cyberrobusthed, at markedsovervågningsmyndigheden efter forordningen om cyberrobusthed kan være en eksisterende eller ny myndighed, herunder en kompetent myndighed i overensstemmelse med artikel 8 i NIS 2-direktivet, en national cybersikkerhedscertificeringsmyndighed i overensstemmelse med artikel 58 i forordningen om cybersikkerhed, eller en markedsovervågningsmyndighed efter radioudstyrsdirektivet.

Der henvises pkt. 3.3 og det foreslåede § 5, og bemærkningerne hertil, for en nærmere beskrivelse af den foreslåede udpegning af markedsovervågningsmyndigheder.

NIS 2-direktivets artikel 12, stk. 1, omhandler koordineret offentliggørelse af sårbarheder og en europæisk sårbarhedsdatabase og er gennemført ved NIS 2-lovens § 18, hvoraf følger, at CSIRT'en sikrer, at fysiske og juridiske personer i anonymiseret form kan rapportere om sårbarheder.

Efter artikel 14, stk. 1, i forordningen om cyberrobusthed skal en fabrikant på tilsvarende vis underrette CSIRT'en og ENISA (European Network and Information Security Agency) om enhver aktivt udnyttet sårbarhed i et produkt med digitale elementer, som fabrikanten får kendskab til. Der skal tilsvarende indberettes om enhver alvorlig hændelse, der har indvirkning på sikkerheden af et sådant produkt, jf. stk. 3.

Dette skal ses i sammenhæng med forordningen artikel 3, nr. 51, hvoraf følger, at der ved »CSIRT, der er udpeget som koordinator« skal forstås en CSIRT, der er udpeget som koordinator i henhold til artikel 12, stk. 1, i NIS 2-direktivet.

Det fremgår af bemærkningerne til NIS 2-loven, jf. Folketingstidende 2024-25, tillæg A, L 141 som fremsat, side 21, at i Danmark blev Center for Cybersikkerhed ved implementeringen af NIS 1-direktivet udpeget som CSIRT i Danmark. Det fremgår endvidere af bemærkningerne, at opgaven hidtil har været varetaget af netsikkerhedstjenesten under Center for Cybersikkerhed, og den opgave vil netsikkerhedstjenesten for nuværende fortsat skulle varetage. Med den kongelige resolution af 29. august 2024 er Center for Cybersikkerhed, bortset fra netsikkerhedstjenesten, blevet ressortoverdraget til Ministeriet for Samfundssikkerhed og Beredskab fra Forsvarsministeriet.

Endelig følger også af artikel 15 i forordningen om cyberrobusthed, at fabrikanter såvel som andre fysiske eller juridiske personer på frivillig basis kan underrette en CSIRT, der er udpeget som koordinator, eller ENISA, om sårbarheder i et produkt med digitale elementer, cybertrusler, hændelser, og nærværd-hændelser, der har indvirkning på sikkerheden.

3. Lovforslagets hovedpunkter

3.1. Anvendelsesområde

3.1.1. Gældende ret

Det følger af artikel 2, stk. 1, i forordningen om cyberrobusthed, at forordningen finder anvendelse på produkter med digitale elementer, der gøres tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.

Ved »produkt med digitale elementer« vil skulle forstås et software- eller hardware-produkt og dets fjerndatabehandlingsløsninger, herunder software- eller hardware-komponenter, der bringes i omsætning separat, jf. forordningens artikel 3, nr. 1.

Ved »gøre tilgængelig på markedet« vil skulle forstås levering af et produkt med digitale elementer med henblik på distribution eller anvendelse på EU-markedet som led i erhvervsvirksomhed mod eller uden vederlag, jf. forordningens artikel 3, nr. 22.

Det kan derudover udledes af præambelbetragtning nr. 9, at produkter med digitale elementer, der er integreret i eller forbundet med et større elektronisk net- og informationssystem, kan fungere som angrebsvektor for ondsindede aktører. Selv mindre kritisk hardware og software kan muliggøre kompromittering af en enhed eller et netværk. Fabrikanterne bør derfor sikre, at produkter med digitale elementer, der kan forbindes fysisk eller logisk, designes og udvikles i overensstemmelse med de væsentlige cybersikkerhedskrav, der er fastsat i forordningen om cyberrobusthed. Dette gælder også for produkter, der kun er indirekte forbundet med andre enheder eller netværk.

I forlængelse heraf følger det af præambelbetragtning nr. 10, at forordningens cybersikkerhedskrav skal forbedre cybersikkerheden i produkter med digitale elementer for både forbrugere og virksomheder og sikre, at der tages hensyn til cybersikkerheden igennem forsyningskæden. Dette omfatter bl.a. produkter med digitale elementer beregnet til sårbare forbrugere, f.eks. legetøj og systemer til overvågning af spædbørn. Forordningen kategoriserer hertil visse produkter med digitale elementer som vigtige eller kritiske og underlægger dem strengere overensstemmelsesvurderingsprocedurer. Det følger endvidere af præambelbetragtning nr. 11, at forordningen skal sikre et højt cybersikkerhedsniveau for produkter med digitale elementer og deres integrerede fjerndatabehandlingsløsninger. En fjerndatabehandlingsløsning omfatter databehandling, der foretages eksternt, til hvilken softwaren er designet og udviklet af eller på vegne af fabrikanten eller under fabrikantens ansvar, og hvis fravær ville forhindre

produktet med digitale elementer i at udføre en af sine funktioner. Fjernbehandling eller -lagring er således kun omfattet i det omfang det er nødvendigt, for at et produkt med digitale elementer kan udføre sine funktioner. Kravene vedrørende fjerndatabasehåndlingsløsninger omfatter ikke tekniske, operationelle eller organisatoriske foranstaltninger til styring af risici for en fabrikants net- og informationssystemer som helhed.

Det kan derudover udledes af præambelbetragtning nr. 12, at cloudløsninger kun udgør fjerndatabasehåndlingsløsninger i forordningens forstand, hvis de opfylder definitionen heraf. Cloudbaserede funktioner, som stilles til rådighed af fabrikanten og understøtter funktionaliteten af et produkt med digitale elementer, kan således være omfattet af forordningen. Derimod er bl.a. cloudtjenester, der er designet og udviklet uden for fabrikantens ansvar for produktet med digitale elementer, ikke omfattet. Sådanne cloud computing-tjenester kan i stedet være omfattet af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2-direktivet).

Endelig skal det fremhæves, at det følger af præambelbetragtning nr. 14, at forordningen ikke bør berøre medlemsstaternes ansvar for beskyttelse af den nationale sikkerhed i overensstemmelse med EU-retten. Det fremgår også heraf, at medlemsstaterne bør kunne underlægge produkter med digitale elementer, der indkøbes eller anvendes til nationale sikkerheds- eller forsvarsformål, yderligere foranstaltninger, forudsat at sådanne foranstaltninger er i overensstemmelse med medlemsstaternes forpligtelser, der er fastsat i EU-retten.

Derudover følger en række undtagelser og modifikationer af artikel 2, stk. 2-8, vedrørende forordningens anvendelsesområde i forhold til andre EU-retsakter.

Det følger således af artikel 2, stk. 2, at produkter med digitale elementer ikke er omfattet af forordningen om cyberrobusthed, når de omfattet af Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og Europa-Parlamentets og Rådets forordning (EU) 2019/2144 af 27. november 2019 om krav til typegodkendelse af motorkøretøjer og påhængskøretøjer dertil samt systemer, komponenter og separate tekniske enheder til sådanne køretøjer for så vidt angår deres generelle sikkerhed og beskyttelsen af køretøjspassagerer og bløde trafikanter.

Forordningen finder heller ikke anvendelse for produkter med digitale elementer, der er certificeret i overensstemmelse med 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, jf. stk. 3, eller udstyr, der er omfattet af Europa-Parlamentets og Rådets direktiv 2014/90/EU af 23. juli 2014 om skibsudstyr, jf. stk. 4.

Anvendelsen af forordningen om cyberrobusthed for produkter med digitale elementer, som er omfattet af andre EU-forskrifter, der fastlægger krav vedrørende alle eller nogle af de risici, som er omfattet af de væsentlige cybersikkerhedskrav i bilag I, kan begrænses eller udelukkes, hvis en sådan begrænsning eller udelukkelse er i overensstemmelse med den overordnede lovgivningsmæssige ramme for de pågældende produkter, og de sektorspecifikke regler sikrer samme eller højere beskyttelsesniveau som det, der er fastsat i denne forordning, jf. stk. 5. Kommissionen kan ved delegerede retsakter præcisere, om en sådan begrænsning eller udelukkelse er nødvendig, hvilke produkter og regler der er berørt, og i givet fald begrænsningens omfang.

Yderligere finder forordningen om cyberrobusthed heller ikke anvendelse for reservedele, der gøres tilgængelige på markedet for at udskifte identiske komponenter i produkter med digitale elementer, og som er fremstillet efter de samme specifikationer som de komponenter, de skal udskifte, jf. stk. 6.

Endelig finder forordningen om cyberrobusthed ikke anvendelse på produkter med digitale elementer, der udelukkende udvikles eller ændres til nationale sikkerheds- eller forsvarsformål, eller på produkter, der er specifikt designet til at behandle klassificerede oplysninger, jf. stk. 7, ligesom de forpligtelser, der er fastsat i forordningen, heller ikke omfatter meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar, jf. stk. 8.

3.1.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning

Den gældende danske produktregulering bygger i vidt omfang på EU's harmoniserede produktregulering, og der findes derfor ikke i dansk ret en horisontal lovramme, der fastsætter generelle cybersikkerhedskrav til produkter med digitale elementer, da de eksisterende regler i stedet er knyttet til bestemte sektor- og produktområder.

Det er derfor Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at forordningen om cyberrobusthed har medført et behov for, at der i dansk ret fastsættes et supplerende nationalt regelsæt hertil. Lovens anvendelsesområde vil derfor skulle ses i sammenhæng med forordningens til enhver tid gældende anvendelsesområde, hvorfor den foreslåede bestemmelse herom i § 2 også alene vil have ordensmæssig karakter.

Dette gælder også, hvis Kommissionen vælger at vedtage delegerede retsakter i medfør af de i forordningen tillagte beføjelser og i overensstemmelse med proceduren i artikel 61, der supplerer forordningens anvendelsesområde ved f.eks. at foretage ændringer af produktkategorierne i bilag III om vigtige produkter eller produktkategorierne i bilag IV om kritiske produkter.

3.2. Udpegning af Styrelsen for Samfundssikkerhed som bemyndigende myndighed

3.2.1. Gældende ret

3.2.1.1. Bemyndigelse af overensstemmelsesvurderingsorganer

Det følger af artikel 36, stk. 1, i forordningen om cyberrobusthed, at enhver medlemsstat skal udpege en bemyndigende myndighed, som er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegning og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf, herunder overholdelsen af forordningens artikel 41.

Det følger af artikel 36, stk. 2, at en medlemsstat kan beslutte at lade et nationalt akkrediteringsorgan udpeget i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter (akkrediteringsforordningen) foretage den vurdering og overvågning, der er omhandlet i artikel 36, stk. 1.

Det følger af artikel 36, stk. 3, at hvis den bemyndigende myndighed uddelegerer eller på anden måde betror den vurdering, bemyndigelse eller overvågning, der er omhandlet i artikel 36, stk. 1, til et organ, der ikke er en statslig enhed, skal dette organ være en juridisk enhed og på tilsvarende vis overholde artikel 37. Derudover skal det have truffet foranstaltninger til dækning af erstatningsansvar i forbindelse med sine aktiviteter. Den bemyndigende myndighed påtager sig det fulde ansvar for de opgaver, der udføres af organet, jf. artikel 36, stk. 4.

Forordningens artikel 37 indeholder en række krav til de bemyndigende myndigheder. De bemyndigende myndigheder skal bl.a. oprettes og organiseres på en sådan måde, at der ikke opstår interessekonflikter med overensstemmelsesvurderingsorganer, og at

alle beslutninger om bemyndigelse af overensstemmelsesvurderingsorganet træffes af kompetente personer, der ikke er identiske med dem, der har foretaget vurderingen. De bemyndigende myndigheder skal desuden organiseres og arbejde på en sådan måde, at det sikres, at deres aktiviteter udøves objektivt og uvildigt.

Det følger endvidere af artikel 38, stk. 1, at hver medlemsstat skal underrette Kommissionen om sine procedurer for vurdering og bemyndigelse af overensstemmelsesvurderingsorganer og overvågning af bemyndigede organer og om eventuelle ændringer heraf. Bemyndigelsesproceduren for overensstemmelsesvurderingsorganer er fastsat i artikel 43 i forordningen om cyberrobusthed.

Da forordningen om cyberrobusthed indfører et nyt horisontalt regelsæt for cybersikkerhed i produkter med digitale elementer, findes der hverken regler om bemyndigelsesprocessen eller en udpeget kompetent bemyndigende myndighed på området.

Akkrediteringsområdet er dog reguleret inden for den gældende produktlovgivning.

Lov om produkter og markedsovervågning, jf. lovbekendtgørelse nr. 22 af 8. januar 2026, indeholder hjemmel til at fastsætte regler om akkreditering, herunder om udpegning af et nationalt akkrediteringsorgan. Den Danske Akkrediteringsfond (DANAK) fungerer som nationalt akkrediteringsorgan efter akkrediteringsforordningen.

Derudover kan nævnes, at der i lov nr. 780 af 4. maj 2021 om cybersikkerhedscertificering er fastsat de nødvendige supplerende bestemmelser til forordningen om cybersikkerhed, der regulerer forskellige forhold for ENISA samt etablerer en fælleseuropæisk ramme for cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester og -processer samt administrerede sikkerhedstjenester. Forordningen er relevant i forhold til forordningen om cyberrobusthed, fordi europæiske cybersikkerhedscertificeringsordninger efter forordningen om cybersikkerhed under de betingelser, der følger af forordningen om cyberrobusthed, kan anvendes til at påvise overensstemmelse med de væsentlige cybersikkerhedskrav i forordningen om cyberrobusthed eller dele heraf. Forordningen om cyberrobusthed indeholder dog et særskilt regime for bemyndigelse og underretning af overensstemmelsesvurderingsorganer, der skal udføre overensstemmelsesvurderingsopgaver efter forordningen om cyberrobusthed.

Det følger i den forbindelse af § 3 i lov om cybersikkerhedscertificering, at Styrelsen for Samfundssikkerhed udpeges som national cybersikkerhedscertificeringsmyndighed, jf. artikel 58, stk. 1, i forordningen om cybersikkerhed. Derudover følger det af § 4 heri, at DANAK akkrediterer overensstemmelsesvurderingsorganer efter artikel 60,

stk. 1, i forordningen om cybersikkerhed, mens § 5 vedrører, at Styrelsen for Samfundssikkerhed kan bemyndige overensstemmelsesvurderingsorganer efter artikel 60, stk. 3, i forordningen om cybersikkerhed til at udføre opgaver i henhold til en europæisk cybersikkerhedscertificeringsordning.

Det bemærkes, at området i forbindelse med kgl. resolution af 29. august 2024 som led i overdragelsen af sager vedrørende cybersikkerhedscertificering blev overdraget fra Erhvervsministeriet til Ministeriet for Samfundssikkerhed og Beredskab. I forlængelse heraf er kompetencen blevet overdraget fra Sikkerhedsstyrelsen til Styrelsen for Samfundssikkerhed.

3.2.1.2. Ændring af bemyndigelser

I forhold til kravene til bemyndigede organer følger det af artikel 39 i forordningen om cyberrobusthed, at et overensstemmelsesvurderingsorgan skal opfylde kravene i artikel 39, stk. 2-12. Disse vedrører at være oprettet i henhold til national ret og være en juridisk person, jf. stk. 2, samt at være et tredjepartsorgan, der er uafhængigt af den organisation eller det produkt med digitale elementer, som det vurderer, jf. stk. 3. Derudover må overensstemmelsesvurderingsorganet, dets øverste ledelse og det personale, der er ansvarligt for at foretage overensstemmelsesvurdering, ikke være designeren, udvikleren, fabrikanten, leverandøren, importøren, distributøren, montøren, køberen, ejeren, brugeren eller reparatøren af de produkter med digitale elementer, som de vurderer, eller den bemyndigede repræsentant for nogen af disse parter, jf. stk. 4.

Der er også krav om, at aktiviteterne udføres med den størst mulige faglige integritet og den nødvendige tekniske kompetence samt ikke at være påvirket af nogen form for pression eller incitament, navnlig af økonomisk art, som kan have indflydelse på deres afgørelser eller resultaterne af deres overensstemmelsesvurderingsaktiviteter, særlig fra personer eller grupper af personer, som har en interesse i resultaterne af disse aktiviteter, jf. stk. 5.

Der stilles i stk. 6 en række krav til, hvilke overensstemmelsesvurderingsopgaver organet skal være i stand til at udføre samt hvilke kapaciteter, det skal have til rådighed, men der i stk. 7 fremgår en række krav til personalet. I stk. 8 stilles der krav om, at arbejdet udføres uvildigt, mens der i stk. 9 er krav om som udgangspunkt at tegne ansvarsforsikring.

I stk. 10 er der fastsat regler om tavshedspligt, mens der i stk. 11 stilles krav om, at overensstemmelsesvurderingsorganet skal deltage i, eller sikre at dets vurderingspersonale er orienteret om de relevante standardiseringsaktiviteter og aktiviteterne i den

koordineringsgruppe af bemyndigede organer, der er nedsat i henhold til artikel 51, og skal som generel retningslinje anvende de administrative afgørelser og dokumenter, som arbejdet i denne gruppe udmøntes i.

Endelig er der i stk. 12 fastsat nærmere regler om, at overensstemmelsesvurderingsorganer skal fungere i henhold til et sæt konsekvente, retfærdige, forholdsmæssige og rimelige vilkår og betingelser, samtidig med at unødvendige byrder undgås for erhvervsdrivende, idet der særlig tages hensyn til mikrovirksomheders og små og mellemstore virksomheders interesser for så vidt angår gebyrer.

I forhold til ændringer af bemyndigelser følger det af artikel 45, stk. 1, i forordningen om cyberrobusthed, at hvis en bemyndigende myndighed har konstateret eller er blevet underrettet om, at et bemyndiget organ ikke længere opfylder kravene i artikel 39, eller at det ikke opfylder sine forpligtelser, begrænser, suspenderer eller inddrager den bemyndigende myndighed bemyndigelsen, alt efter hvad der er relevant, og afhængigt af i hvor høj grad disse krav eller forpligtelser ikke er blevet opfyldt. Den underretter omgående EU-Kommissionen og de øvrige medlemsstater herom.

Det følger derudover af artikel 45, stk. 2, at hvis en bemyndigelse begrænses, suspenderes eller inddrages, eller hvis det bemyndigede organ har indstillet sin virksomhed, træffer den bemyndigende medlemsstat de nødvendige foranstaltninger for at sikre, at dette organs sager enten behandles af et andet bemyndiget organ eller gøres tilgængelige for de ansvarlige bemyndigende myndigheder og markedsovervågningsmyndigheder efter disses anmodning.

For så vidt angår bødestraf for manglende overholdelse af artikel 39, kan der henvises til artikel 64, stk. 3, i forordningen om cyberrobusthed og det foreslåede § 17, stk. 1, nr. 2, og bemærkningerne hertil.

3.2.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at Styrelsen for Samfundssikkerhed bør udpeges som bemyndigende myndighed, da styrelsen besidder den nødvendige faglige ekspertise og erfaring på cyberområdet, herunder som ansvarlig myndighed for så vidt angår lov om cybersikkerhedscertificering og NIS 2-loven.

Den foreslåede ordning vil medføre, at Styrelsen for Samfundssikkerhed med rollen som bemyndigende myndighed vil blive pålagt en række opgaver og forpligtelser.

Som bemyndigende myndighed er Styrelsen for Samfundssikkerhed ansvarlig for at indføre og gennemføre procedurer for vurdering, udpegning og bemyndigelse af overensstemmelsesvurderingsorganer samt overvågning heraf, jf. artikel 36, stk. 1, i forordningen om cyberrobusthed. Reglerne om bemyndigelse og bemyndigelsesproceduren er fastsat i artikel 42 og 43.

Styrelsen for Samfundssikkerhed vil endvidere være ansvarlig for overvågning af de bemyndigede organer, herunder deres overholdelse af kravene i artikel 39 og artikel 41. Efter artikel 41 skal et bemyndiget organ, der anvender en underleverandør eller et datterselskab til bestemte opgaver i forbindelse med overensstemmelsesvurdering, sikre, at underleverandøren eller datterselskabet opfylder kravene i artikel 39, og underretter den bemyndigende myndighed herom.

Styrelsen for Samfundssikkerhed vil som bemyndigende myndighed have det overordnede ansvar for vurdering, udpegning, bemyndigelse og overvågning af overensstemmelsesvurderingsorganer. Det følger imidlertid af artikel 37, stk. 3, at enhver beslutning om bemyndigelse af et overensstemmelsesvurderingsorgan skal træffes af kompetente personer, der ikke er identiske med dem, der har foretaget vurderingen. Ministeriet for Samfundssikkerhed og Beredskab vurderer derfor, at denne risiko bør afhjælpes ved at udnytte adgangen i artikel 36, stk. 2, til at bestemme, at den i stk. 1 omhandlede vurdering og overvågning foretages af et nationalt akkrediteringsorgan i den i akkrediteringsforordningen anvendte betydning og i overensstemmelse med nævnte forordning.

Det foreslås derfor, at den i stk. 1 omhandlede vurdering som udgangspunkt sker på grundlag af akkreditering, og at akkrediteringen som udgangspunkt foretages af Den Danske Akkrediteringsfond (DANAK). DANAK vil i disse tilfælde foretage den i artikel 36, stk. 1, omhandlede vurdering og den efterfølgende overvågning, jf. artikel 36, stk. 2, i forordningen om cyberrobusthed.

Et bevis på akkreditering kan efter artikel 42, stk. 2, anvendes som dokumentation for, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 39. Styrelsen for Samfundssikkerhed vil i forbindelse med bemyndigelsen kontrollere, at akkrediteringen dækker de overensstemmelsesvurderingsaktiviteter og -procedurer, som ansøgningen vedrører, og svarer til det vurderingsgrundlag, som styrelsen har fastlagt for den pågældende bemyndigelse inden for rammerne af artikel 39.

DANAK vil dermed foretage vurdering og overvågning af de overensstemmelsesvurderingsorganer, der akkrediteres af DANAK med henblik på bemyndigelse til at udføre tredjepartsoverensstemmelsesvurderinger efter forordningen om cyberrobusthed.

Hvis DANAK ikke kan foretage den relevante akkreditering, kan et overensstemmelsesvurderingsorgan i de tilfælde, der er fastsat i artikel 7, stk. 1, i akkrediteringsforordningen, søge akkreditering hos et nationalt akkrediteringsorgan i en anden medlemsstat. Et sådant bevis på akkreditering kan anvendes i forbindelse med en ansøgning om bemyndigelse efter artikel 42 i forordningen om cyberrobusthed, når akkrediteringen dækker de relevante overensstemmelsesvurderingsaktiviteter og -procedurer og svarer til det vurderingsgrundlag, som Styrelsen for Samfundssikkerhed har fastlagt for den pågældende bemyndigelse inden for rammerne af artikel 39.

Hvis overensstemmelsesvurderingsorganet efterfølgende søger om fornyelse eller udvidelse af akkrediteringen, og betingelserne i artikel 7, stk. 1, i akkrediteringsforordningen for at søge akkreditering hos et nationalt akkrediteringsorgan i en anden medlemsstat ikke længere er opfyldt, skal ansøgningen indgives til DANAK.

Det nationale akkrediteringsorgan, der har udstedt et bevis på akkreditering, vil herefter skulle foretage den løbende overvågning af, om overensstemmelsesvurderingsorganet fortsat opfylder de krav, som akkrediteringen omfatter, herunder kravene i artikel 39 i forordningen om cyberrobusthed. Styrelsen for Samfundssikkerhed vil som bemyndigende myndighed fortsat have det overordnede ansvar for overvågningen af det bemyndigede organ efter forordningen om cyberrobusthed, uanset om bemyndigelsen er baseret på akkreditering foretaget i Danmark eller i en anden medlemsstat.

Forordningen om cyberrobusthed giver desuden mulighed for bemyndigelse, hvor et overensstemmelsesvurderingsorgan ikke kan fremlægge et bevis på akkreditering. I sådanne tilfælde skal organet efter artikel 42, stk. 3, fremlægge den dokumentation, der er nødvendig for at kontrollere, anerkende og regelmæssigt overvåge, at kravene i artikel 39 er opfyldt. Artikel 43, stk. 4 og 5, regulerer bemyndigelse, der ikke er baseret på et akkrediteringscertifikat.

Hvis et overensstemmelsesvurderingsorgan bemyndiges uden et akkrediteringscertifikat, vil Styrelsen for Samfundssikkerhed skulle fortage overvågning af, at organet fortsat opfylder kravene til bemyndigelse. Det foreslås, at denne mulighed alene anvendes, hvor akkreditering ikke er mulig, og at der som betingelse for bemyndigelsen fastsættes krav om, at det pågældende overensstemmelsesvurderingsorgan skal søge akkreditering, når dette bliver muligt.

Der henvises til lovforslagets § 3 om udpegning af den bemyndigende myndighed og § 4 om DANAKS vurdering og overvågning i forbindelse hermed samt bemærkningerne til disse bestemmelser.

3.3. Udpegning af markedsovervågningsmyndigheder

3.3.1. Gældende ret

3.3.1.1. Markedsovervågning

Markedsovervågningsforordningen fastlægger den generelle EU-retlige ramme for markedsovervågning af produkter omfattet af EU-harmoniseringslovgivning og fastsætter bl.a. regler om markedsovervågningsmyndigheders opgaver og beføjelser, samarbejde mellem myndigheder og udveksling af oplysninger mellem medlemsstaterne og Europa-Kommissionen.

I lov om produkter og markedsovervågning, jf. lovbekendtgørelse nr. 22 af 8. januar 2026, som bl.a. supplerer markedsovervågningsforordningen på en række produktområder omfattet af EU-harmoniseringslovgivning, følger det af § 9, stk. 1, at Erhvervsstyrelsen varetager opgaven som kontrolmyndighed inden for lovens anvendelsesområde, medmindre andet følger af anden lovgivning for så vidt angår forebyggelse af specifikke risici ved særlige produkter, jf. stk. 2.

Det følger af artikel 52, stk. 1, i forordningen om cyberrobusthed, at markedsovervågningsforordningen finder anvendelse på produkter med digitale elementer, der er omfattet af anvendelsesområdet for forordningen om cyberrobusthed. Dette medfører, at forordningen om cyberrobusthed således indgår i det generelle EU-retlige system for markedsovervågning af produkter omfattet af EU-harmoniseringslovgivning.

Markedsovervågningsforordningen finder anvendelse, medmindre forordningen om cyberrobusthed indeholder bestemmelser med samme formål, der på en mere specifik måde regulerer særlige aspekter af markedsovervågningen og håndhævelsen, jf. markedsovervågningsforordningens artikel 2, stk. 1.

Forordningen om cyberrobusthed indeholder hertil særlige regler om markedsovervågning og håndhævelse for produkter med digitale elementer, herunder om udpegning af markedsovervågningsmyndigheder, samarbejde med CSIRT'er og ENISA, evaluering af produkter, som der er tilstrækkelig grund til at antage udgør en væsentlig cybersikkerhedsrisiko, og håndhævelse over for produkter, der ikke opfylder kravene i forordningen.

Det følger af artikel 52, stk. 2, i forordningen om cyberrobusthed, at hver medlemsstat skal udpege en eller flere markedsovervågningsmyndigheder med henblik på en virksomhedsfuld gennemførelse af forordningen om cyberrobusthed. Medlemsstaterne kan i den forbindelse udpege en eksisterende eller ny myndighed til at virke som markedsovervågningsmyndighed.

Det fremgår endvidere af forordningens præambelbetragtning nr. 107, at medlemsstaterne kan vælge at udpege enhver eksisterende eller ny myndighed som markedsovervågningsmyndighed (for så vidt angår forordningen om cyberrobusthed). Sådanne myndigheder vil f.eks. kunne være kompetente myndigheder udpeget eller etableret i henhold til artikel 8 i NIS 2-direktivet, nationale cybersikkerhedscertificeringsmyndigheder udpeget i henhold til artikel 58 i forordningen om cybersikkerhed eller markedsovervågningsmyndigheder udpeget med henblik på radioudstyrsdirektivet.

Forordningen om cyberrobusthed giver dermed medlemsstaterne en bred adgang til at placere markedsovervågningsopgaven hos en myndighed, der har de nødvendige kompetencer til at føre tilsyn med cybersikkerhedskrav til produkter med digitale elementer.

Forordningen indeholder dog i artikel 52, stk. 14, 1. pkt., en modifikation til dette udgangspunkt, da det følger heraf, at for produkter med digitale elementer, der er omfattet af denne forordnings anvendelsesområde, og som er klassificeret som højrisiko-AI-systemer i henhold til artikel 6 i forordningen om kunstig intelligens, skal de markedsovervågningsmyndigheder, der udpeges med henblik på nævnte forordning, være de myndigheder, der er ansvarlige for de markedsovervågningsaktiviteter, der kræves i henhold til nærværende forordning.

Om samarbejdet mellem disse markedsovervågningsmyndigheder følger det af artikel 52, stk. 14, 2. pkt., at de markedsovervågningsmyndigheder, der er udpeget i henhold til forordningen om kunstig intelligens, vil skulle samarbejde, hvor det er relevant, med de markedsovervågningsmyndigheder, der er udpeget efter forordningen om cyberrobusthed, og med de CSIRT'er, der er udpeget som koordinatore, og med ENISA om tilsynet med gennemførelsen af rapporteringsforpligtelserne i henhold til nærværendes forordnings artikel 14.

Det følger også af artikel 52, stk. 14, 3. pkt. i forordningen om cyberrobusthed, at markedsovervågningsmyndigheder udpeget i henhold til forordningen om kunstig intelligens navnlig underretter markedsovervågningsmyndigheder udpeget i henhold til

nærværende forordning om ethvert resultat, der er relevant for udførelsen af deres opgaver i forbindelse med gennemførelsen af nærværende forordning.

Udpegningen af markedsovervågningsmyndigheder for så vidt angår systemer, der er klassificeret som højrisiko AI-systemer i henhold til forordningen om kunstig intelligens foretages i medfør af regler på Forsknings-, Uddannelses- og Digitaliseringsministeriets område.

I forhold til sammenhængen mellem forordningen om cyberrobusthed og forordningen om cybersikkerhed bemærkes det, at det følger af artikel 54, stk. 1, litra j, i forordningen om cybersikkerhed, at europæiske cybersikkerhedscertificeringsordninger skal indeholde regler om løbende kontrol med, om certificerede IKT-produkter, -tjenester og -processer fortsat opfylder de relevante krav. Den nationale cybersikkerhedscertificeringsmyndighed skal efter artikel 58, stk. 7, føre tilsyn med og håndhæve disse regler i samarbejde med relevante markedsovervågningsmyndigheder. Myndigheden kan efter artikel 58, stk. 8, bl.a. kræve oplysninger, foretage undersøgelser og audit, påbyde overtrædelser bragt til ophør og efter national ret tilbagekalde europæiske cybersikkerhedsattester. Tilsynet er afgrænset til den europæiske ramme for cybersikkerhedscertificering, men omfatter løbende kontrol med certificerede produkter og mulighed for markedsrettet håndhævelse.

Afslutningsvis skal det bemærkes, at markedsovervågning efter forordningen om cyberrobusthed indgår i det generelle markedsovervågningssystem, hvor Erhvervsstyrelsen (tidligere Sikkerhedsstyrelsen) er udpeget som centralt forbindelseskantor, jf. § 27 i lov om produkter og markedsovervågning i overensstemmelse med markedsovervågningsforordningens artikel 10, stk. 3.

3.3.1.2. Håndhævelsesbeføjelser

Forordningen om cyberrobusthed indeholder i artikel 53-60 en række håndhævelsesbeføjelser, der finder direkte anvendelse. Disse supplerer således de generelle håndhævelsesbeføjelser i medfør af markedsovervågningsforordningen, jf. artikel 52 i forordningen om cyberrobusthed, som er nærmere beskrevet ovenfor i pkt. 3.3.1.1.

Det følger af artikel 53 i forordningen om cyberrobusthed, at hvis det er nødvendigt for at vurdere, om produkter med digitale elementer og de processer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I, tildeles markedsovervågningsmyndighederne efter begrundet anmodning adgang til de data på et for dem let forståeligt sprog, som er nødvendige for at vurdere designet, udviklingen,

produktionen og sårbarhedshåndteringen af sådanne produkter, herunder den relevante interne dokumentation fra den relevante erhvervsdrivende.

Hvis oplysningerne foreligger i et maskinlæsbart format, vil myndighederne kunne kræve, at det udleveres i dette format, så oplysningerne forsat kan behandles elektronisk i forbindelse med kontrollen. Det kan eksempelvis være relevant for software-komponentlister, konfigurationsoplysninger, logfiler og andre strukturerede data.

Det følger derudover af artikel 54, stk. 1, første afsnit, om den nationale procedure vedrørende produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, at hvis en medlemsstats markedsovervågningsmyndighed har tilstrækkelig grund til at antage, at et produkt med digitale elementer, herunder dets sårbarhedshåndtering, udgør en væsentlig cybersikkerhedsrisiko, foretager den uden unødigt ophold og, hvor det er hensigtsmæssigt, i samarbejde med den relevante CSIRT en evaluering af det pågældende produkt med digitale elementer for så vidt angår dets opfyldelse af alle de krav, der er fastsat i denne forordning. De relevante erhvervsdrivende samarbejder i nødvendigt omfang med markedsovervågningsmyndigheden.

Det fremgår derudover af bestemmelsens andet afsnit, at hvis markedsovervågningsmyndigheden i forbindelse med denne evaluering konstaterer, at produkter med digitale elementer ikke opfylder kravene i denne forordning, pålægger den straks den pågældende erhvervsdrivende at træffe alle fornødne afhjælpende tiltag for at bringe produktet med digitale elementer i overensstemmelse med disse krav, trække produktet med digitale elementer tilbage fra markedet eller tilbagekalde det inden for en rimelig tidsfrist, alt efter hvad markedsovervågningsmyndigheden måtte fastsætte i forhold til cybersikkerhedsrisikoens art.

Det vil således bero på en konkret vurdering under hensyntagen til cybersikkerhedsrisikoens art, hvilke af de omtalte pålæg, der bør udstedes, samt fristens længde.

Endelig følger det af bestemmelsens tredje afsnit, at markedsovervågningsmyndigheden underretter det relevante bemyndigede organ herom, og at artikel 18 i markedsovervågningsforordningen finder anvendelse på de afhjælpende tiltag.

Disse evalueringer kan omfatte en vurdering af, om produktet opfylder alle relevante krav efter forordningen og er således ikke begrænset til de forhold, der gav anledning til antagelsen om, at produktet udgør en væsentlig cybersikkerhedsrisiko.

Evalueringen kan også omfatte tekniske undersøgelses- og analysemetoder af produktets hardware, software og digitale funktioner, herunder reverse engineering, når den pågældende metode er nødvendig for at vurdere produktets overensstemmelse med forordningen.

Ved ”væsentlig cybersikkerhedsrisiko” forstås en cybersikkerhedsrisiko, hvor der som følge af dens tekniske karakteristika kan antages at være en stor sandsynlighed for en hændelse, som kan have en alvorlig negativ indvirkning, herunder ved at forårsage betydelige materielle eller immaterielle tab eller forstyrrelser, jf. artikel 3, nr. 38, i forordningen om cyberrobusthed.

Ved vurdering af risikoens væsentlighed skal markedsovervågningsmyndigheden efter artikel 54, stk. 2, i forordningen om cyberrobusthed også tage hensyn til ikke-tekniske risikofaktorer og navnlig dem, der er fastlagt som følge af de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder på EU-plan, jf. artikel 22 i NIS 2-direktivet. Hvor en markedsovervågningsmyndighed har tilstrækkelig grund til at antage, at et produkt med digitale elementer udgør en væsentlig cybersikkerhedsrisiko i lyset af sådanne ikke-tekniske faktorer, skal markedsovervågningsmyndigheden underrette og, i nødvendigt omfang, samarbejde med de relevante kompetente myndigheder, der er udpeget i henhold til artikel 8 i NIS 2-direktivet.

Derudover kan også artikel 54, stk. 5, fremhæves, hvoraf følger, at hvis den erhvervsdrivende ikke træffer tilstrækkelige afhjælpende tiltag inden for den frist, der er omhandlet i stk. 1, andet afsnit, træffer markedsovervågningsmyndigheden de nødvendige foreløbige foranstaltninger for at forbyde eller begrænse tilgængeliggørelsen af produktet med digitale elementer på det nationale marked eller for at trække produktet tilbage fra markedet eller kalde det tilbage. Myndigheden underretter straks Kommissionen og de øvrige medlemsstater om disse foranstaltninger.

Artikel 55 vedrører EU-beskyttelsesproceduren, der supplerer den nationale procedure i artikel 54 vedrørende produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko. Det følger således af artikel 55, stk. 1, at hvor en medlemsstat inden for tre måneder efter modtagelsen af den i artikel 54, stk. 5, omhandlede underretning gør indsigelse mod en anden medlemsstats foranstaltning, eller hvor Kommissionen finder, at foranstaltningen er i strid med EU-retten, drøfter Kommissionen straks spørgsmålet med den relevante medlemsstat og den eller de relevante erhvervsdrivende og evaluerer den nationale foranstaltning. På grundlag af resultaterne af denne evaluering træffer Kommissionen senest ni måneder efter den i artikel 54, stk. 5,

omhandlede underretning afgørelse om, hvorvidt den nationale foranstaltning er berettiget eller ej, og meddeler den pågældende medlemsstat denne afgørelse.

Artikel 55 stk. 2-5, indeholder nærmere regler om, hvordan EU-Kommissionen og de øvrige medlemsstater i forskellige tilfælde forholder sig til den nationale foranstaltning.

Artikel 56 vedrører proceduren på EU-plan vedrørende produkter med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, som indeholder nærmere regler om, hvordan EU-Kommissionen i forskellige tilfælde forholder sig, hvor der er tilstrækkelig grund til at antage, at et produkt med digitale elementer, der udgør en væsentlig cybersikkerhedsrisiko, ikke overholder kravene i forordningen om cyberrobusthed, herunder ved at underrette de nationale markedsovervågningsmyndigheder, foretage evalueringer eller iværksætte korrigerende eller restriktive foranstaltninger på EU-plan. Det følger dog af stk. 7, at EU-Kommissionens tiltag, jf. stk. 3-6, alene finder anvendelse, så længe den ekstraordinære situation, der begrundede EU-Kommissionens indgreb, gør sig gældende, forudsat at produktet med digitale elementer ikke er bragt til at overholde denne forordning.

Det følger af artikel 57, stk. 1, første afsnit, at en medlemsstats markedsovervågningsmyndighed pålægger en erhvervsdrivende at træffe alle passende foranstaltninger, hvor den efter at have foretaget en evaluering i henhold til artikel 54 finder, at et produkt med digitale elementer og de processer, som fabrikanten har indført, overholder denne forordning, men at de udgør en væsentlig cybersikkerhedsrisiko og en risiko for: a) menneskers sundhed eller sikkerhed, b) overholdelsen af forpligtelser i henhold til EU-ret eller national ret, der har til formål at beskytte de grundlæggende rettigheder, c) tilgængeligheden, autenticiteten, integriteten eller fortroligheden af tjenester, der leveres ved brug af et elektronisk informationssystem af væsentlige enheder som omhandlet i artikel 3, stk. 1, i NIS 2-direktivet, eller d) andre aspekter af beskyttelsen af den offentlige interesse.

Bestemmelsen finder således alene anvendelse, når der 1) har været foretaget en evaluering, jf. artikel 54, 2) evalueringen finder, et produkt med digitale elementer og de processer, som fabrikanten har indført, overholder forordningen om cyberrobusthed, 3) produktet og de nævnte processer udgør en væsentlig cybersikkerhedsrisiko, og 4) der foreligger en risiko på baggrund af de i litra a-d oplistede aspekter.

Det følger derudover af artikel 57, stk. 1, andet afsnit, at disse foranstaltninger kan omfatte foranstaltninger til at sikre, at det pågældende produkt med digitale elementer

og de processer, som fabrikanten har indført, ikke længere udgør de relevante risici, når det gøres tilgængeligt på markedet, tilbagetrækning fra markedet af det pågældende produkt med digitale elementer eller tilbagekaldelse af det, og de skal stå i et rimeligt forhold til arten af disse risici.

Det følger af artikel 58, stk. 1, i forordningen om cyberrobusthed, at en medlemsstats markedsovervågningsmyndighed pålægger den pågældende fabrikant at bringe manglende overholdelse af følgende forhold til ophør: a) CE-mærkningen er anbragt i strid med artikel 29 og 30, b) CE-mærkningen er ikke anbragt, c) EU-overensstemmelseserklæringen er ikke udarbejdet, d) EU-overensstemmelseserklæringen er ikke udarbejdet korrekt, e) identifikationsnummeret på det bemyndigede organ, der er involveret i overensstemmelsesvurderingsproceduren, hvor dette er relevant, er ikke anbragt, eller f) den tekniske dokumentation mangler eller er ufuldstændig.

De oplyste forhold vedrører på forskellig vis forhold, der knytter sig til oplysninger om de omfattede produkter, herunder anbringelse af CE-mærkning, jf. forordningens artikel 29 og 30, udarbejdelse af EU-overensstemmelseserklæring, anbringelse af identifikationsnummer på det relevante overensstemmelsesvurderingsorgan og manglende eller ufuldstændig teknisk dokumentation.

Det følger derudover af artikel 58, stk. 2, at hvis den i stk. 1 omhandlede manglende overholdelse varer ved, træffer den pågældende medlemsstat alle nødvendige foranstaltninger til at begrænse eller forbyde tilgængeliggørelsen af produktet med digitale elementer på markedet eller sikre, at det tilbagekaldes eller trækkes tilbage fra markedet.

Sådanne foranstaltninger kan f.eks. være at standse salg, levering eller nye downloads af produktet eller at trække det tilbage fra distributionskæden, indtil en fabrikant har iværksat de nødvendige foranstaltninger for, at produktet opfylder de væsentlige cybersikkerhedskrav, eller, hvis mindre indgribende foranstaltninger ikke er tilstrækkelige, tilbagekalde det fra slutbrugerne. Den konkrete foranstaltning skal i hvert tilfælde vurderes at være nødvendig og proportional samt tilpasset produktets karakter.

Artikel 59 vedrører markedsovervågningsmyndighedernes fælles aktiviteter, og det følger i den forbindelse af stk. 1, at markedsovervågningsmyndighederne kan aftale med andre relevante myndigheder at gennemføre fælles aktiviteter, der har til formål at sikre cybersikkerhed og forbrugerbeskyttelse for så vidt angår specifikke produkter med digitale elementer, der bringes i omsætning eller gøres tilgængelige på markedet, navnlig produkter med digitale elementer, der ofte viser sig at udgøre en

cybersikkerhedsrisiko. I stk. 2-5 er det nærmere fastsat, at EU-Kommissionen eller ENISA foreslår de fælles kontrolaktiviteter, samt hvordan den skal udføres, og hvordan oplysninger i den forbindelse håndteres.

Artikel 60 vedrører kontrolaktioner, og det følger her af stk. 1, at markedsovervågningsmyndighederne gennemfører samtidige, koordinerede kontrolaktioner af bestemte produkter med digitale elementer eller kategorier heraf for at kontrollere overholdelse eller afsløre overtrædelser af denne forordning. Disse kontrolaktioner kan omfatte inspektioner af produkter med digitale elementer, der er erhvervet under en dækidentitet. Det følger endvidere af stk. 2, at medmindre andet aftales af de involverede markedsovervågningsmyndigheder, koordinerer Kommissionen kontrolaktionerne, og at kontrolaktionens koordinator gør, hvor det er hensigtsmæssigt, de samlede resultater offentligt tilgængelige, mens stk. 3 vedrører ENISA's rolle i denne sammenhæng. Det følger af stk. 4, at ved gennemførelsen af kontrolaktioner kan de involverede kontrolovervågningsmyndigheder gøre brug af undersøgelsesbeføjelserne i artikel 52-58 og eventuelle andre beføjelser, som de er tillagt i henhold til national ret. Endelig følger det af stk. 5, at markedsovervågningsmyndighederne kan opfordre tjenestemænd i Kommissionen og andre ledsagende personer, der er bemyndiget af Kommissionen, til at deltage i kontrolaktioner.

3.3.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning

Forordningen om cyberrobusthed giver medlemsstaterne en bred adgang til at vælge, hvilke kompetente myndigheder der skal varetage markedsovervågningsopgaverne, herunder myndigheder, der i forvejen varetager en tilsvarende funktion i henhold til bl.a. NIS 2-reglerne og som national cybersikkerhedscertificeringsmyndighed, hvilket i begge tilfælde er Styrelsen for Samfundssikkerhed. Forordningen om cyberrobusthed forudsætter dog en markedsovervågning, der kan håndtere tekniske og cybersikkerhedsfaglige vurderinger af produkter med digitale elementer. Det omfatter bl.a. vurderinger af produktets tekniske dokumentation, sårbarhedshåndtering, sikkerhedsopdateringer, rapporteringsforpligtelser, produktarkitektur og eventuelle cybersikkerhedsrisici.

Det er derfor Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at funktionen som markedsovervågningsmyndighed primært bør placeres hos en myndighed med cybersikkerhedsfaglig kompetence og forudsætninger for at samarbejde med relevante nationale og europæiske myndigheder.

Det foreslås på den baggrund, at Styrelsen for Samfundssikkerhed udpeges som markedsovervågningsmyndighed samtidig med, at styrelsen også i medfør af denne lov udpeges som bemyndigende myndighed. Herved samles de to centrale nationale funktioner hos én myndighed, hvilket skal understøtte en sammenhængende anvendelse af reglerne og et klart nationalt myndighedsansvar.

Der henvises til det foreslåede § 5, stk. 1, og bemærkningerne hertil.

Dette vil svare til den gældende ordning i medfør af § 5 i lov om cybersikkerhedscertificering om bemyndigelse af overensstemmelsesorganer i henhold til forordningen om cybersikkerhed, og §§ 9-14 heri om tilsyn, idet begge funktioner også her varetages af Styrelsen for Samfundssikkerhed.

Den foreslåede ordning, hvorefter markedsovervågningen efter forordningen om cyberrobusthed som udgangspunkt varetages af én national markedsovervågningsmyndighed, gælder dog med forbehold for de modifikationer, der følger af artikel 52, stk. 14, om systemer, der er klassificeret som højrisiko-AI-systemer i henhold til forordningen om kunstig intelligens.

Der henvises i den forbindelse til det foreslåede § 5, stk. 2, og bemærkningerne hertil.

Forordningen om cyberrobusthed fastsætter horisontale cybersikkerhedskrav til produkter med digitale elementer. Kravene gælder på tværs af produktkategorier og anvendelsesområder og omfatter både hardware og software. Produkterne kan indgå i meget forskellige sammenhænge, men cybersikkerhedskravene knytter sig til produktet og de erhvervsdrivendes forpligtelser efter forordningen og ikke alene til produktets anvendelse, herunder sektorspecifikke anvendelse.

Det er derfor også Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at de samme produktretlige cybersikkerhedskrav bør fortolkes og håndhæves ensartet uanset produktets forskellige anvendelser, og uanset hvilken myndighed der varetager markedsovervågningen. Der bør derfor fastsættes en fælles strategisk ramme for markedsovervågningen efter forordningen om cyberrobusthed, så reglerne anvendes ensartet og sammenhængende på tværs af produktkategorier, herunder med henblik på at bidrage til klare konkurrencevilkår på det danske marked. Disse rammer vil samtidig skulle understøtte, at danske kontrolindsatser prioriteres risikobaseret under hensyn til bl.a. produktkategorier og forbundne cybersikkerhedsrisici, og at danske prioriteringer koordineres med det europæiske samarbejde, herunder eventuelt også relevante nationale cybersikkerhedsindsatser, uden at ændre markedsovervågningens produktretlige

karakter. Den fælles strategiske ramme vil dog ikke være til hinder for, at kontrolindsatsen prioriteres risikobaseret under hensyn til bl.a. produktkategorier, produkternes tilsigtede formål og de forbundne cybersikkerhedsrisici.

Den strategiske ramme for markedsovervågning efter forordningen om cyberrobusthed erstatter ikke den nationale markedsovervågningsstrategi efter artikel 13 i markedsovervågningsforordningen, men indgår som en underliggende ramme for markedsovervågningen af de cybersikkerhedsrisici, der er reguleret af forordningen om cyberrobusthed. I overensstemmelse med artikel 11 i forordningen om cyberrobusthed finder også produktsikkerhedsforordningen fortsat anvendelse på aspekter og risici, der ikke er omfattet af forordningen om cyberrobusthed. Rammen ændrer heller ikke de opgaver, der efter artikel 10, stk. 3, i markedsovervågningsforordningen varetages af det centrale forbindelseskantor.

Det er Ministeriet for Samfundssikkerhed og Beredskabs opfattelse, at behovet for en nationalt koordineret markedsovervågningsindsats samtidig skal ses i lyset af, at produkter med digitale elementer markedsføres og anvendes på tværs af medlemsstater, og at cybersikkerhedsrisici ofte kan have grænseoverskridende karakter. Det europæiske samarbejde om markedsovervågning, herunder gruppen for administrativt samarbejde (ADCO), der oprettes efter forordningens artikel 52, stk. 15, kan understøtte videndeling, koordinering af kontrolindsatser, bedre udnyttelse af test- og analysekapacitet og en mere ensartet håndhævelse af reglerne i EU. Dette skal samtidig understøtte en risikobaseret prioritering af den danske kontrolindsats.

Det foreslås på den baggrund, at Styrelsen for Samfundssikkerhed udpeges som national koordinerende myndighed for markedsovervågning efter forordningen om cyberrobusthed. Dette vil indebære, at styrelsen skal fastsætte den nationale strategiske ramme for markedsovervågningen, koordinere samarbejdet mellem relevante markedsovervågningsmyndigheder og koordinere den danske deltagelse i ADCO. Funktionen berører dog ikke de opgaver, der varetages af det centrale forbindelseskantor, jf. artikel 10 i markedsovervågningsforordningen, eller øvrige EU-retlige forpligtelser og beføjelser, der påhviler andre udpegede markedsovervågningsmyndigheder.

Markedsovervågningsmyndighedernes håndhævelsesbeføjelser følger bl.a. af artikel 52-60 i forordningen om cyberrobusthed, der finder direkte anvendelse og derfor er gennemgået oven for i pkt. 3.3.1.2 under gældende ret. Det er dog Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der er behov for at fastsætte en række supplerende bestemmelser hertil for at sikre, at de beføjelser, der er omtalt i

markedsovervågningsforordningen, også vil kunne anvendes af markedsovervågningsmyndighederne i forhold til forordningen om cyberrobusthed.

Der kan i den forbindelse bl.a. henvises til lovforslagets §§ 8 og 9 om håndhævelsesbeføjelser og adgang til erhvervsmæssige lokaliteter og bemærkningerne hertil.

Markedsovervågningsmyndighederne bør derudover generelt samarbejde med andre myndigheder i relevant omfang, hvis forhold der henhører under forordningen om cyberrobustheds anvendelsesområde har betydning herfor. Det kunne f.eks. være cyberhændelser relateret til produkter med digitale elementer, hvor disse produkter har en sådan karakter, at fabrikanten samtidig udgør en enhed, der er omfattet NIS 2-loven. Der kan i sådanne tilfælde efter omstændighederne være behov for koordination med de kompetente NIS 2-myndigheder, herunder videregivelse af oplysninger i relevant omfang.

3.4. Klageadgang

3.4.1. Gældende ret

Det følger af artikel 48 i forordningen om cyberrobusthed, at medlemsstaterne skal sikre, at der findes en procedure for klager over de bemyndigede organers afgørelser.

Der stilles ikke i forordningen yderligere krav hertil, hvorfor det er op til den enkelte medlemsstat at fastsætte passende regler om klageprocedure.

Der er derudover i dansk ret som udgangspunkt adgang til administrativ rekurs efter de almindelige forvaltningsretlige principper herom, dvs. at en afgørelse kan påklages til højere administrativ myndighed.

Når der er tale om en afgørelse i forvaltningsretlig forstand, vil også 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), finde anvendelse.

3.4.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at forordningens krav bør iagttages ved, at der fastsætte regler om henholdsvis klageinstans, formkrav og klagefrist, herunder konsekvensen af manglende overholdelse heraf, for så vidt angår de bemyndigede organer og DANAK. Dette vil varetage et hensyn til en effektiv og transparent klageprocedure.

Der vil således kunne klages til Styrelsen for Samfundssikkerhed over vurderinger foretaget af de organer, der er bemyndiget hertil, samt deres øvrige virke, ligesom der også vil kunne klages til styrelsen over DANAK's vurdering og overvågning.

Det vurderes derudover, at der ikke bør være mulighed for at indbringe afgørelser i klagesager for anden administrativ myndighed. Dette skyldes, at den nærmere behandling og stillingtagen til indholdet af sådanne sager forudsætter en særlig faglig ekspertise, der som udgangspunkt foreligger hos henholdsvis Styrelsen for Samfundssikkerhed og de myndigheder, der er omhandlet i det foreslåede § 5, stk. 2.

Der henvises til lovforslagets §§ 15 og 16 og bemærkningerne hertil.

3.5. Sanktioner

3.5.1. Gældende ret

Det følger af artikel 64, stk. 1, i forordningen om cyberrobusthed, at medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af bestemmelserne i forordningen, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelserne og have afskrækkende virkning. Medlemsstaterne skal straks give Kommissionen meddelelse om disse regler og foranstaltninger samt om senere ændringer, der berører dem.

Der lægges med forordningens artikel 64, stk. 2-4, op til, at bøder pålægges administrativt. Forordningens artikel 64, stk. 2-4, fastsætter således, hvilke overtrædelser, der skal kunne straffes med administrative bøder, og de maksimale bødeniveauer herfor. Det fremgår af artikel 64, stk. 2, at manglende opfyldelse af de væsentlige cybersikkerhedskrav i bilag I og forpligtelserne i artikel 13 og 14 straffes med administrative bøder på op til 15 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2,5 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det fremgår af artikel 64, stk. 3, at manglende opfyldelse af forpligtelserne i artikel 18-23, artikel 28, artikel 30, stk. 1-4, artikel 31, stk. 1-4, artikel 32, stk. 1, 2 og 3, artikel 33, stk. 5, og artikel 39, 41, 47, 49 og 53, straffes med administrative bøder på op til 10 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det fremgår af artikel 64, stk. 4, at afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning straffes med administrative bøder på op til 5 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 1 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det følger endvidere af artikel 64, stk. 7, at medlemsstaterne kan fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og offentlige organer, der er etableret i den pågældende medlemsstat.

Det er i dansk ret et generelt princip, at staten, regioner og kommuner alene kan straffes for overtrædelser, der begås ved udøvelse af virksomhed, som svarer til eller kan side-stilles med virksomhed udøvet af private, jf. straffelovens § 27, stk. 2.

En anvendelse af dette princip vil betyde, at offentlige myndigheder kun vil kunne straffes for tilsidesættelse af deres forpligtelser omfattet af forordningen om cyberrobusthed, når deres aktiviteter ikke har karakter af myndighedsudøvelse, dvs. i forbindelse med f.eks. at levere tjenester eller udøve virksomhed.

Det fremgår af artikel 64, stk. 8, at afhængigt af den enkelte medlemsstats retssystem kan reglerne om administrative bøder anvendes på en sådan måde, at bøderne pålægges af kompetente nationale domstole eller andre organer i overensstemmelse med den nationalt fastlagte kompetencefordeling. En sådan national ordning skal have en virkning, der svarer til anvendelsen af administrative bøder efter forordningen.

Det følger endelig af artikel 64, stk. 10, i forordningen om cyberrobusthed, at administrative bøder ikke finder anvendelse på fabrikanten, der betragtes som mikrovirksomhed eller små virksomheder, for så vidt angår manglende overholdelse af 24-timersfristerne for tidlig varsling om aktivt udnyttede sårbarheder eller alvorlige hændelser, der har indvirkning på sikkerheden af et produkt med digitale elementer, jf. artikel 14, stk. 2, litra a, og stk. 4, litra a. Administrative bøder finder heller ikke anvendelse på overtrædelser af forordningen begået af open source software-forvaltere.

3.5.2. Ministeriet for Samfundssikkerhed og Beredskabs overvejelser og den foreslåede ordning

Det foreslås, at der indsættes sanktionsbestemmelser i loven med det formål, at der kan idømmes bødestraf for overtrædelse af forordningens bestemmelser om overholdelse af de væsentlige cybersikkerhedskrav i bilag I og fabrikanternes øvrige forpligtelser efter artikel 13 samt underretningspligten efter artikel 14. Bødeniveauet herfor

vil være op til 15 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2,5 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Derudover strafbelægges manglende opfyldelse af forpligtelserne for bemyndigede repræsentanter, importører, distributører, personer der foretager væsentlige ændringer (artikel 18-22), manglende identifikation (artikel 23), samt kravet om at udfærdige overensstemmelseserklæringer (artikel 28), anbringelse af CE-mærkning (artikel 30, stk. 1-4), kravene til teknisk dokumentation (artikel 31, stk. 1-4), foretagelse af overensstemmelsesvurderinger (artikel 31, stk. 1-3), de særlige krav til mikrovirksomheders dokumentation (artikel 33, stk. 5), kravene til de bemyndigede organer (artikel 39), herunder dattervirksomheder og underleverandører (artikel 41), bemyndigede organers operationelle forpligtelser og oplysningspligt (artikel 47 og 49), og manglende tildeling af adgang til oplysninger og dokumentation over for markedsovervågningsmyndigheder (artikel 53). Bødeniveauet herfor vil være op til 10 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 2 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Endelig foreslås det også, at afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning vil kunne straffes med bøde. Bødeniveauet herfor vil være op til 5 000 000 EUR eller, hvis lovovertræderen er en virksomhed, op til 1 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at de i artikel 64, stk. 2-4, omtalte sanktioner for overtrædelse af forordningens bestemmelser i dansk ret bør fastsættes som strafferetlige sanktioner i henhold til muligheden herfor i artikel 64, stk. 8, i stedet for som administrative bøder.

Dette skyldes, at indførelse af administrative bøder i dansk ret kan give anledning til betænkeligheder i forhold til grundlovens § 3 om magtens tredeling. Bestemmelsen antages at indebære, at lovgivningsmagten ikke i almindelighed kan henlægge behandlingen af strafferetlige bødesager til administrative myndigheder. I dansk retspleje er det i øvrigt 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.

Forordningens bestemmelser om administrative bøder vil dermed i en dansk sammenhæng skulle anvendes således, at bøder ikke pålægges administrativt, men i det almindelige strafferetlige system. Det indebærer, at de kompetente myndigheder i givet fald vil skulle indgive politianmeldelse, såfremt de konstaterer strafbelagte overtrædelser af denne lov eller regler udstedt i medfør af denne lov.

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 hensyn, der er beskrevet i forordningens artikel 64, stk. 5.

Det er endvidere Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at der ikke bør være mulighed for at udstede administrative bødeforlæg. Dette skyldes bl.a., at det vurderes, at der ikke i alle tilfælde vil være tale om klare og umiddelbart konstaterbare overtrædelser, ligesom der heller ikke med lovforslaget lægges op til at fastsætte konkrete bødestørrelser uden skønsmæssige elementer af betydning.

Det er derudover Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at det er mest hensigtsmæssigt, at forældelsesfristen for overtrædelse af denne lov, regler udstedt i medfør af loven eller forordningen om cyberrobusthed fastsættes til 5 år, under hensyntagen til, at de omfattede straffesager kan antage en vis størrelse og kompleksitet.

Der kan i den forbindelse henvises til, at der bl.a. følger en tilsvarende forældelsesfrist af § 41, stk. 7, i databeskyttelsesloven, jf. lovbekendtgørelse nr. 289 af 8. marts 2024, og § 10, stk. 4, i lov nr. 467 af 14. maj 2025 om supplerende bestemmelser til forordningen om kunstig intelligens.

Endelig forslås det at udgangspunktet i straffelovens § 27, stk. 2, om at statslige myndigheder og kommuner alene kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private, finder anvendelse for de foreslåede bestemmelser i denne lov.

For en nærmere gennemgang af de foreslåede bestemmelser om straf henvises der til den foreslåede § 17 og bemærkningerne hertil.

4. Forholdet til databeskyttelsesloven og databeskyttelsesforordningen

De myndigheder, der foreslås udpeget i overensstemmelse med forordningen om cyberrobusthed, vil som udgangspunkt være omfattet af reglerne i

databeskyttelsesforordningen og databeskyttelsesloven. Der henvises i den forbindelse til præambelbetragtning nr. 32 i forordningen om cyberrobusthed.

De foreslåede bestemmelser om udpegning af kompetente myndigheder vil på forskellig vis kunne indebære behandling af personoplysninger i forbindelse med myndighedernes varetagelse af de opgaver, der følger af forordningen om cyberrobusthed. Dette vil f.eks. være tilfældet som led i bemyndigelse af overensstemmelsesvurderingsorganer, markedsovervågning og håndhævelse, herunder indsamling af oplysninger ved adgang, kommunikation om foranstaltninger og klageprocedurer, idet der her vil kunne indgå almindelige personoplysninger om f.eks. ansattes navn, uddannelsesniveau eller kontaktoplysninger, når dette fremgår af det relevante materiale, herunder hvis der måtte være tale om en enkeltmandsvirksomhed.

Behandling af personoplysninger er lovlig, hvis én af betingelserne i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, er opfyldt, herunder hvis behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som led i myndighedsudøvelse (litra e).

Behandling i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra e, skal have et såkaldt supplerende retsgrundlag, som forpligter eller berettiger myndigheden til at udføre en bestemt myndighedsopgave. Det følger af databeskyttelsesforordningens artikel 6, stk. 3.

Behandling af personoplysninger vedrørende straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger på grundlag af databeskyttelsesforordningens artikel 6, stk. 1, må kun foretages under kontrol af en offentlig myndighed, eller hvis behandling har hjemmel i EU-retten eller medlemsstaternes nationale ret, som giver passende garantier for registreredes rettigheder og frihedsrettigheder. Ethvert omfattende register over straffedomme må kun føres under kontrol af en offentlig myndighed.

Behandling af følsomme oplysninger er som udgangspunkt forbudt, jf. databeskyttelsesforordningens artikel 9, stk. 1. Dette forbud finder dog bl.a. ikke anvendelse, hvis behandlingen vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede, jf. stk. 2, litra e, eller hvis behandlingen er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares, jf. stk. 2, litra f. Derudover kan nævnes det tilfælde, at behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse

og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser, jf. stk. 2, litra g.

Det er Ministeriet for Samfundssikkerhed og Beredskabs vurdering, at behandling af de omhandlede personoplysninger i disse tilfælde er nødvendig, idet behandlingen sker af hensyn til myndighedernes opfyldelse af de opgaver, der følger af forordningen om cyberrobusthed.

Der vil også i medfør af de foreslåede bestemmelser kunne blive fastsat nærmere regler om de kompetente myndigheders samarbejde, koordinering og informationsudveksling, som vil kunne indebære udveksling af personoplysninger i forbindelse med de kompetente myndigheders koordinering af markedsovervågning og håndtering af hændelser mv. Dette vil som udgangspunkt alene vedrøre almindelige personoplysninger.

Det følger af den foreslåede § 11, at Styrelsen for Samfundssikkerhed, de myndigheder, der er nævnt i § 5, stk. 2, og CSIRT'en kan videregive oplysninger til andre myndigheder eller virksomheder, herunder i andre medlemsstater, og til institutioner i Den Europæiske Union for at varetage myndighedsopgaver i medfør af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf. Myndighederne vil i den forbindelse i relevant omfang kunne videregive personoplysninger, såsom navn på medarbejdere hos fabrikanter eller andre erhvervsdrivende, herunder hvis der er tale om en enkeltmandsvirksomhed, til bl.a. kompetente myndigheder i andre EU-medlemsstater eller EU's institutioner, herunder ENISA og EU-Kommissionen. Den foreslåede bestemmelse vil også kunne omfatte videregivelse som led i koordination mellem nationale myndigheder, hvor det er relevant, f.eks. mellem markedsovervågningsmyndighederne og kompetente myndigheder i forhold til NIS 2-loven.

Uanset ovenstående bestemmelser vil der alene kunne behandles nødvendige og relevante oplysninger til brug for de kompetente myndigheders behandling af en konkret sag. Det forudsættes derudover, at de øvrige bestemmelser i databeskyttelsesforordningen og databeskyttelsesloven iagttages, når der behandles personoplysninger i forbindelse med varetagelsen af de opgaver, der følger af forordningen om cyberrobusthed.

Afslutningsvis bemærkes det, at funktionen som CSIRT i Danmark for nuværende varetages af netsikkerhedstjenesten på Forsvarsministeriets område, der bl.a. reguleres af lov om Center for Cybersikkerhed, jf. lovbekendtgørelse nr. 836 af 7. august 2019. Det følger af lovens § 8, at centerets virksomhed er undtaget databeskyttelsesloven og databeskyttelsesforordningen.

Uanset at virksomheden er undtaget fra databeskyttelseslovgivningen, finder størstedelen af de centrale principper i databeskyttelseslovgivningen anvendelse for netsikkerhedstjenesten i medfør af kapitel 6 i lov om Center for Cybersikkerhed.

5. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Lovforslaget vurderes ikke i sig selv at medføre økonomiske- eller implementeringsmæssige konsekvenser for staten.

Forordningen om cyberrobusthed vurderes dog at medføre økonomiske- og implementeringsmæssige konsekvenser for staten, herunder negative økonomiske konsekvenser i form af udgifter relateret til Styrelsen for Samfundssikkerheds varetagelse af funktionen som bemyndigende myndighed, markedsovervågningsmyndighed og hertil relaterede myndighedsopgaver, herunder løbende bistand til de myndigheder, der er omhandlet i det foreslåede § 5, stk. 2, på ca. 5,7 mio. kr. i 2027 og ca. 11,8 mio. kr. i 2028 stigende til 14,3 mio. kr. i 2029. Udgiftsestimatet er baseret på, at der skal anvendes 12 årsværk til varetagelse af opgaven i Styrelsen for Samfundssikkerhed.

Derudover vil forordningen også kunne medføre udgifter for staten til CSIRT'en i forbindelse med varetagelsen af rollen som koordinator for fabrikanternes underretninger af udnyttelse af sårbarheder. Disse udgifter kvantificeres ikke nærmere.

Lovforslaget vil ikke have økonomiske- eller implementeringsmæssige konsekvenser for regioner eller kommuner.

Principperne for digitaliseringsklar lovgivning

Det vurderes, at lovforslaget følger principperne for digitaliseringsklar lovgivning.

Det er hensigten med lovforslaget at udarbejde en enkel og klar lovgivning, som supplerer forordningen om cyberrobusthed, hvor dette er påkrævet. I enkelte tilfælde er det vurderet hensigtsmæssigt med gengivelse af bestemmelser fra forordningen eller henvisninger hertil med henblik på at lette forståelsen af lovforslaget. Lovforslaget lægger sig derudover op ad forordningens etablering af en ensartet ramme for cybersikkerhed i produkter med digitale elementer og følger dermed princip nr. 1 om enkle og klare regler, idet det har til formål at understøtte forordningens fremme af anerkendelse og anvendelse af cybersikkerhedskrav til produkter med digitale elementer på tværs af produktkategorier i alle EU-landene.

Derudover vil lovforslaget understøtte digital kommunikation, som ligger i naturlig forlængelse af, at der er tale om regulering af produkter med digitale elementer, idet

der i det foreslåede § 12, stk. 1, fremgår et udgangspunkt om digital kommunikation med de kompetente myndigheder. Fastsættes der i medfør af § 12, stk. 3, nærmere regler om digital kommunikation og anvendelse af bestemte it-systemer og særlige digitale formater, herunder digital signatur, vil eksisterende offentlig it-infrastruktur blive forsøgt udnyttet. Lovforslaget er dermed i overensstemmelse med princip nr. 2 og 6.

Det bemærkes, at lovforslaget i sammenhæng med selve forordningen om cyberrobusthed vurderes at understøtte princip nr. 7 om forebyggelse af snyd og fejl, da forordningen netop har til formål at imødekomme de tiltagende cybersikkerhedsudfordringer i EU, herunder gennem etableringen af en fælleseuropæisk ramme for cybersikkerhedskrav til produkter med digitale elementer, og derved øge forbrugere og virksomheders bevidsthed om cybersikkerhed og tillid til de omfattede produkter.

De øvrige principper for digitaliseringsklar lovgivning vurderes ikke at være relevante for lovforslaget.

6. Økonomiske og administrative konsekvenser for erhvervslivet m.v.

Det bemærkes overordnet, at lovforslaget supplerer forordningen om cyberrobusthed. Forordningen kan have økonomiske og administrative konsekvenser for erhvervslivet m.v. Dette vil navnlig vedrøre fabrikanternes udgifter til overholdelse af forordningens krav i forbindelse med at bringe produkter med digitale elementer i omsætning på det indre marked.

Lovforslaget forventes derudover at medføre begrænsede negative økonomiske konsekvenser for erhvervslivet m.v. for så vidt angår overensstemmelsesvurderingsorganers betaling af en engangsydelse i form af det gebyr, der er omhandlet i det foreslåede § 4, stk. 2, til DANAK i forbindelse med vurdering som led i at opnå bemyndigelse som overensstemmelsesvurderingsorgan, jf. det foreslåede § 3, stk. 2. Der vil endvidere også være negative økonomiske konsekvenser for de erhvervsdrivende, der skal refundere markedsovervågningsmyndighedernes omkostninger i forbindelse med kontrol, jf. det foreslåede § 8, stk. 4, hvis der træffes afgørelse om manglende overensstemmelse med krav i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Endelig vil der kunne være mindre negative administrative konsekvenser for erhvervslivet forbundet med administration som led i at ansøge på ny om bemyndigelse i det tilfælde, hvor akkreditering ikke har været muligt, og der er meddelt en foreløbig bemyndigelse med vilkår herom, jf. det foreslåede § 3, stk. 4.

7. Administrative konsekvenser for borgerne

Lovforslaget har ikke direkte administrative konsekvenser for borgerne, men vil dog medvirke til at sikre en effektiv og hensigtsmæssig myndighedsstruktur, der skal understøtte forordningen om cyberrobusthed, der bl.a. vil gøre det lettere for forbrugerne at finde den relevante information om produkter med digitale elementer, idet der med forordningen fastsættes en række oplysningspligter for fabrikanter og krav om CE-mærkning af produkter, der bringes i omsætning og derved gøres tilgængelige for forbrugerne.

8. Klimamæssige konsekvenser

Lovforslaget har ikke klimamæssige konsekvenser.

9. Miljø- og naturmæssige konsekvenser

Lovforslaget har ikke miljø- og naturmæssige konsekvenser.

10. Forholdet til EU-retten

Lovforslaget fastsætter supplerende bestemmelser til forordningen om cyberrobusthed. Hovedparten af forordningen finder anvendelse fra den 11. december 2027, mens kapitel IV om bemyndigelse af overensstemmelsesvurderingsorganer, herunder kravet om at der udpeges en bemyndigende myndighed, finder anvendelse fra den 11. juni 2026, mens artikel 14 om fabrikanterers rapporteringsforpligtelser gælder umiddelbart fra den 11. september 2026.

Lovforslaget foreslås at træde i kraft den 1. marts 2027, hvorfor der vil være tale om forsinket gennemførelse af kravet om, at der udpeges en bemyndigende myndighed. For så vidt angår de dele af forordningen, der først finder anvendelse fra den 11. december 2027, vil der være tale om udskudt ikrafttræden af de supplerende bestemmelser hertil, således at de ikke gennemføres før den EU-retlige forpligtelse hertil indtræder.

11. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 5. oktober 2026 til den 2. november 2026 (28 dage) været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatrådet, Amnesty International, ATP, Belysningsbranchen Danmark, Borch Teknik, Brancheforeningen Cirkulær, Certificerede Organers Forum, DANAK – Den Danske Akkrediteringsfond, Danish Care, Danish Cloud Community, Danish e-infrastructure consortium, Dansk El-tavle Forening, Danmarks Aktive Forbrugere, Danmarks

Apotekerforening, Dansk Arbejdsgiverforening, Dansk Beredskabskommunikation, Dansk Brand- og sikringsteknisk Institut, Dansk Erhverv, Dansk Industri, Dansk Internet Forum (DIFO), DANSK IT, Dansk Selskab for Patientsikkerhed, Dansk Standard, Danske Advokater, Danske Maritime, Danske Open Source Leverandører (DOSL), Danske Rederier, Danske Regioner, Danske Universiteter, Dataetisk Råd, Datatilsynet, De Samvirkende Købmænd, DJØF, DKCERT, D-mærket, Domstolsstyrelsen, DNV, Danmark Fagbevægelsens Hovedorganisation, Finans Danmark, Forbrugerklagenævnet, Forbrugerlaboratoriet, Forbrugerombudsmanden, Forbrugerrådet Tænk, Forenede Danske Antenneanlæg, Foreningen af Rådgivende Ingeniører, Force Technology, Green power Denmark, GTS-foreningen, Industriens Fond, Industriforeningen for Generiske og Biosimilære Lægemidler, Ingeniørforeningen i Danmark, Institut for Menneskerettigheder, IT-Branchen, IT-Politisk Forening, IT-Universitetet, Justitia, KL, KOMBIT, Landbrug og Fødevarer, Lederne, Legebranchen (LEG), Lægemiddelindustriforeningen, MEDCOM, Medicoindustrien, Odense Robotics, Open-Denmark, OS2 – Offentligt Digitaliseringsfællesskab, Pharmadanimark, Professionel Elektronik, Retspolitisk Forening, Rigsrevisionen, Røde Kors, Rådet for Digital Sikkerhed, SamAqua, samtlige byretter, Sikkerhedsbranchen, SMVdanmark, Sø- og Handelsretten, Tekniq Arbejdsgiverne, Teknologisk Institut, TeleDCIS, Teleindustrien (TI), TÜV Syd Danmark, UL International Demko A/S, VELTEK, Vestre Landsret og Østre Landsret.

12. Sammenfattende skema		
	Positive konsekvenser/mindre-udgifter (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.	Ingen.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen.	Ingen.
Økonomiske konsekvenser	Ingen.	Der vil være begrænsede omkostninger for

for erhvervsli- vet m.v.		overensstemmelsesvurderingsorganer relateret til betaling af gebyr til DANAK for akkreditering i forbindelse med be- myndigelse og derudover erhvervsdriv- endes eventuelle refundering af myn- dighedens kontrolomkostninger i til- fælde af manglende overensstemmelse med forordningens krav.
Administrative konsekvenser for erhvervsli- vet m.v.	Ingen.	Overensstemmelsesvurderingsorga- ner, der meddeles en foreløbig bemyn- digelse, vil have begrænsede omkost- ninger i forbindelse med ansøgning påny med henblik på endelig bemyndi- gelse, hvis der er fastsat vilkår herom.
Administrative konsekvenser for borgerne	Understøttelse af kravene i for- ordningen om cyberrobusthed ved- rørende bl.a. fabrikanters oplys- ningspligter og CE-mærkning vil gøre det lettere for forbrugerne at finde den relevante information i forbindelse med valg af produkt og anvendelsen heraf.	Ingen.
Klimamæssige konsekvenser	Ingen.	Ingen.
Miljø- og natur- mæssige konse- kvenser	Ingen.	Ingen.
Forholdet til EU-retten	Lovforslaget fastsætter supplerende bestemmelser til Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer (forordningen om cyberrobusthed). For så vidt angår de supplerende bestemmelser til artikel 35-51 vil der være tale om forsinket national gennemførelse, idet disse bestemmelser finder an- vendelse fra den 11. juni 2026.	
Er i strid med de fem princip- per for imple- mentering af er- hvervsrettet EU-regulering (der i relevant	Ja	Nej X

omfang også gælder ved implementering af ikke-erhvervsrettet EU-regulering) (sæt X)	
---	--

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Der er ikke fastsat generelle regler i dansk ret vedrørende produkter med digitale elementer, der er egnede til at supplere forordningen om cyberrobusthed.

Med forordningen om cyberrobusthed etableres blandt andet en fælles europæisk ramme for cybersikkerhedskrav til produkter med digitale elementer. Forordningen om cyberrobusthed gælder umiddelbart i Danmark, men forudsætter visse supplerende nationale gennemførelsesforanstaltninger.

Det foreslås i § 1, at loven supplerer Europa-Parlamentets og Rådets forordning (EU) 2024/2847 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed).

Den foreslåede bestemmelse vil indebære, at det tydeliggøres, at loven har til formål at fastsætte de nødvendige supplerende bestemmelser til forordningen om cyberrobusthed, der er nødvendige for forordningens anvendelse i Danmark.

Til § 2

Det følger af artikel 2, stk. 1, i forordningen om cyberrobusthed, at forordningen finder anvendelse på produkter med digitale elementer, der gøres tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk.

Ved »produkter med digitale elementer« forstås et software- eller hardwareprodukt og dets fjerndatabehandlingsløsninger, herunder software- eller hardwarekomponenter, der bringes i omsætning separat, jf. forordningens artikel 3, nr. 1. For en nærmere

gennemgang af forordningens anvendelsesområde henvises til pkt. 3.1.1 i lovforslagets almindelige bemærkninger.

Artikel 2, stk. 2-8, indeholder derudover en række undtagelser og modifikationer relateret til sammenhænge og overlap med anden relevant EU-regulering.

Der kan i den forbindelse henvises til artikel 2, stk. 2, hvoraf følger, at forordningen ikke finder anvendelse for produkter med digitale elementer, som er reguleret af Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, Europa-Parlamentets og Rådets forordning (EU) 2017/746 af 5. april 2017 om medicinsk udstyr til in vitro-diagnostik og Europa-Parlamentets og Rådets forordning (EU) 2019/2144 af 27. november 2019 om krav til typegodkendelse af motorkøretøjer og påhængskøretøjer dertil samt systemer, komponenter og separate tekniske enheder til sådanne køretøjer for så vidt angår deres generelle sikkerhed og beskyttelsen af køretøjspassagerer og bløde trafikanter.

Forordningen finder heller ikke anvendelse på produkter med digitale elementer, der er certificeret i overensstemmelse med 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, jf. artikel 2, stk. 3, eller som er omfattet af Europa-Parlamentets og Rådets direktiv 2014/90/EU af 23. juli 2014 om skibsudstyr, jf. artikel 2, stk. 4.

Kommissionen kan efter artikel 2, stk. 5, ved delegerede retsakter begrænse eller udelukke anvendelsen af forordningen om cyberrobusthed på produkter med digitale elementer, som er omfattet af andre EU-forskrifter, der fastlægger krav vedrørende alle eller nogle af de risici, som er omfattet af de væsentlige cybersikkerhedskrav i forordningens bilag I, hvis: a) en sådan begrænsning eller udelukkelse er i overensstemmelse med den overordnede lovgivningsmæssige ramme, der gælder for disse produkter, og b) de sektorspecifikke regler sikrer samme eller højere beskyttelsesniveau som det, der er fastsat i denne forordning.

Det følger af artikel 2, stk. 6, i forordningen om cyberrobusthed, at forordningen ikke finder anvendelse for reservedele, der gøres tilgængelige på markedet for at udskifte identiske komponenter i produkter med digitale elementer, og som er fremstillet efter de samme specifikationer som de komponenter, de skal udskifte.

Det fremgår af Kommissionens vejledning om anvendelsen af forordningen om cyberrobusthed (C(2026) 5252 final), afsnit 4.2, at reservedelen skal leveres med det formål at reparere eller forlænge levetiden for et produkt, der allerede er bragt i omsætning.

Det er derfor ikke nok, at reservedelen rent teknisk kan anvendes som erstatning. Undtagelsen kan omfatte både hardware og software. Ved vurderingen af, om reservedelen er identisk, lægges der navnlig vægt på, om den har samme funktion og de samme cybersikkerhedsrelevante egenskaber som den oprindelige komponent. Hvis reservedelen ikke er identisk, er den et selvstændigt produkt med digitale elementer, som er omfattet af forordningen. Det betyder dog ikke nødvendigvis, at det reparerede produkt er blevet væsentligt ændret. Dette skal vurderes særskilt efter artikel 3, nr. 30.

Endelig finder forordningen om cyberrobusthed ikke anvendelse på produkter med digitale elementer, der udelukkende udvikles eller ændres til nationale sikkerheds- eller forsvarsformål, eller på produkter, der er specifikt designet til at behandle klassificerede oplysninger, jf. artikel 2, stk. 7, ligesom de forpligtelser, der er fastsat i forordningen, heller ikke omfatter meddelelse af oplysninger, hvis videregivelse ville stride mod væsentlige interesser med hensyn til medlemsstaternes nationale sikkerhed, offentlige sikkerhed eller forsvar, jf. artikel 2, stk. 8.

Det foreslås i § 2, at loven gælder for produkter med digitale elementer, der gøres tilgængelige på markedet, hvis tilsigtede formål eller rimeligt forudsigelige anvendelse omfatter en direkte eller indirekte logisk eller fysisk dataforbindelse til en enhed eller et netværk med digitale elementer i overensstemmelse med artikel 2, stk. 1, i forordningen om cyberrobusthed. Loven gælder dog ikke i de tilfælde, der er nævnt i artikel 2, stk. 2-8, i forordningen om cyberrobusthed.

Det foreslåede vil medføre, at loven finder anvendelse i samme omfang som forordningen og vil tjene et ordensmæssigt hensyn med henblik på at tydeliggøre lovens anvendelsesområde. Der er således ikke tiltænkt materielle forskelle mellem lovens og forordningens anvendelsesområde.

Den foreslåede bestemmelse skal dermed også ses i sammenhæng med forordningens undtagelser og modifikationer til anvendelsesområdet i artikel 2, stk. 2-8.

For en nærmere gennemgang af forordningens anvendelsesområde henvises til pkt. 3.1 i lovforslagets almindelige bemærkninger.

Til § 3

Efter artikel 36, stk. 1, i forordning om cyberrobusthed, skal hver medlemsstat udpege en bemyndigende myndighed, som er ansvarlig for at indføre og gennemføre de nødvendige procedurer for vurdering, udpegning og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf, herunder overholdelsen af artikel 41 i forordningen.

Det følger af præambelbetragtning nr. 99, at for at sikre et ensartet kvalitetsniveau ved overensstemmelsesvurderingen af produkter med digitale elementer er det nødvendigt at fastsætte krav til bemyndigende myndigheder og andre organer, som er involveret i vurdering, bemyndigelse og overvågning af bemyndigede organer.

Det fremgår endvidere, at ordningen bør suppleres af akkrediteringsordningen efter Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter, og at akkreditering er et vigtigt middel til at efterprøve overensstemmelsesvurderingsorganernes kompetence i forbindelse med bemyndigelse, hvorfor det bør anvendes med henblik på bemyndigelse.

De oven for omtalte krav i præambelbetragtning nr. 99, følger endvidere af artikel 37 og vedrører, at myndigheden er oprettet på en sådan måde, at der ikke opstår interessekonflikter med overensstemmelsesvurderingsorganer, jf. stk. 1, er organiseret og arbejder på en sådan måde, at det sikres, at dens aktiviteter udøves objektivt og uvildigt, jf. stk. 2, samt at alle beslutninger om bemyndigelse af overensstemmelsesvurderingsorganet træffes af kompetente personer, der ikke er identiske med dem, der foretog vurderingen, jf. stk. 3. Derudover må myndigheden ikke udføre aktiviteter, som udføres af overensstemmelsesvurderingsorganer, eller yde rådgivningsservice på kommercielt eller konkurrencemæssigt grundlag, jf. stk. 4, ligesom den bemyndigende myndighed skal sikre, at de oplysninger, som den indhenter, behandles fortroligt, jf. stk. 5. Afslutningsvis følger det af stk. 6, at myndigheden skal have et tilstrækkeligt antal kompetente medarbejdere til, at den kan udføre sine opgaver behørigt.

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed udpeges som bemyndigende myndighed vedrørende overensstemmelsesvurderingsorganer i henhold til artikel 36, stk. 1, i forordningen om cyberrobusthed.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed varetager funktionen som bemyndigende myndighed i overensstemmelse med artikel 36, stk. 1, i forordningen om cyberrobusthed og dermed vil skulle varetage opgaver relateret til at indføre og gennemføre nødvendige procedurer for vurdering, udpegning og bemyndigelse af overensstemmelsesvurderingsorganer og for overvågning heraf, herunder overholdelse af artikel 41.

Det forudsættes, at Styrelsen for Samfundssikkerhed opfylder og vil vedblive med at opfylde de omtalte krav til bemyndigende myndigheder i forordningens artikel 37 om bl.a. uafhængighed, fortrolighed, kompetencer og fravær af interessekonflikter.

Dette skal bl.a. ses i sammenhæng med det foreslåede i § 5 i denne lov, hvorefter DANAK som udgangspunkt vil foretage vurderinger og efterfølgende overvågning af overensstemmelsesvurderingsorganer i overensstemmelse med forordningens artikel 36, stk. 2.

Når vurderingen foretages af DANAK, vil beslutningen om bemyndigelse blive truffet af Styrelsen for Samfundssikkerhed. Dette understøtter overholdelsen af kravet i artikel 37, stk. 3, om, at alle beslutninger om bemyndigelse skal træffes af kompetente personer, der ikke er identiske med dem, der foretog vurderingen. Hvis Styrelsen for Samfundssikkerhed selv foretog vurderingen af et overensstemmelsesvurderingsorgan, ville styrelsen organisatorisk skulle sikre den tilsvarende adskillelse mellem vurdering og beslutning om bemyndigelse.

Bemyndigelse af et overensstemmelsesvurderingsorgan, som omtalt i artikel 36, forudsætter, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 39, stk. 2-12. Dette indebærer bl.a., at organet skal være oprettet i henhold til national ret og være en juridisk person, samt at det skal være uafhængigt af den organisation eller det produkt, der skal vurderes. Der stilles derudover en række krav til personale og ledelse, herunder sammensætning og faglig integritet, ligesom der som udgangspunkt stilles krav om ansvarsforsikring og tavshedspligt.

Det følger derudover af artikel 41, stk. 1, at et bemyndiget organ, der giver bestemte opgaver i forbindelse med overensstemmelsesvurdering til underleverandører eller anvender en dattervirksomhed, skal sikre, at underleverandøren eller dattervirksomheden opfylder kravene i artikel 39, samt skal underrette den bemyndigende myndighed herom.

Af artikel 41, stk. 2-4, følger yderligere krav til det bemyndigede organ, der har henlagt opgaver i henhold til forordningen til underleverandører eller en dattervirksomhed.

Det foreslås i *stk. 2*, at Styrelsen for Samfundssikkerhed efter ansøgning bemyndiger overensstemmelsesvurderingsorganer, der lever op til kravene i artikel 39, stk. 2-12, i forordningen om cyberrobusthed, til at gennemføre opgaver i henhold til artikel 32 og bilag VIII i nævnte forordning.

Det foreslåede skal ses i sammenhæng med den foreslåede udpegning af Styrelsen for Samfundssikkerhed som bemyndigende myndighed og vil indebære, at Styrelsen for Samfundssikkerhed kan bemyndige overensstemmelsesvurderingsorganer, der kan bevise, at de opfylder kravene i artikel 39, stk. 2-12, i forordningen om cyberrobusthed til at gennemføre opgaver i henhold til artikel 32 og bilag VIII i nævnte forordning.

I forbindelse med Styrelsen for Samfundssikkerheds vurdering af om et overensstemmelsesvurderingsorgan opfylder kravene i artikel 39, stk. 2-12, i forordningen om cyberrobusthed, vil organet skulle fremlægge dokumentation herfor.

Vurderingen vil som udgangspunkt ske på grundlag af akkreditering, og i disse tilfælde vil et bevis herpå efter artikel 42, stk. 2, kunne anvendes som dokumentation for, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 39.

Styrelsen for Samfundssikkerhed vil i forbindelse med bemyndigelsen kontrollere, at akkrediteringen dækker de overensstemmelsesvurderingsaktiviteter og -procedurer samt produkter med digitale elementer, som ansøgningen vedrører, og svarer til det vurderingsgrundlag, som styrelsen har fastlagt for den pågældende bemyndigelse inden for rammerne af artikel 39.

Kan DANAK ikke foretage den relevante akkreditering, vil et dansk overensstemmelsesvurderingsorgan i de tilfælde, der er fastsat i artikel 7, stk. 1, i forordning (EF) nr. 765/2008, kunne søge akkreditering hos et nationalt akkrediteringsorgan i en anden medlemsstat. Et bevis på akkreditering udstedt af et sådant organ vil kunne anvendes i forbindelse med ansøgningen om bemyndigelse, når akkrediteringen dækker de relevante overensstemmelsesvurderingsaktiviteter og -procedurer og svarer til det vurderingsgrundlag, som Styrelsen for Samfundssikkerhed har fastlagt for den pågældende bemyndigelse inden for rammerne af artikel 39.

Det nationale akkrediteringsorgan, der har udstedt et bevis på akkreditering, vil herefter skulle foretage den løbende overvågning som led i akkrediteringen. Styrelsen for Samfundssikkerhed vil dog som bemyndigende myndighed fortsat have det overordnede ansvar for overvågningen af det bemyndigede organ efter forordningen om cyberrobusthed. Hvis betingelserne i artikel 7, stk. 1, i forordning (EF) nr. 765/2008 for at anvende et nationalt akkrediteringsorgan i en anden medlemsstat ikke længere er opfyldt, vil et overensstemmelsesvurderingsorganet ved en efterfølgende fornyelse eller udvidelse af akkrediteringen skulle søge akkreditering hos DANAK.

Kan et overensstemmelsesvurderingsorgan ikke fremlægge et bevis på akkreditering, vil organet efter artikel 42, stk. 3, i forordningen om cyberrobusthed skulle fremlægge den dokumentation, der er nødvendig for at verificere, anerkende og løbende overvåge, at kravene i artikel 39 er opfyldt. Hvis et overensstemmelsesvurderingsorgan bemyndiges på dette grundlag, vil Styrelsen for Samfundssikkerhed skulle sikre den løbende overvågning af organets opfyldelse af artikel 39 og overholdelse af artikel 41.

Det forudsættes, at denne mulighed alene anvendes, hvor akkreditering ikke er mulig, og at det pågældende overensstemmelsesvurderingsorgan efterfølgende vil skulle søge akkreditering, når dette bliver muligt.

Det foreslås i *stk. 3, 1. pkt.*, at hvis Styrelsen for Samfundssikkerhed konstaterer, at et overensstemmelsesvurderingsorgan, der er bemyndiget efter stk. 2, overtræder de specifikke krav, som er nævnt heri, kan Styrelsen for Samfundssikkerhed fastsætte en rimelig tidsfrist for afhjælpning af de konstaterede overtrædelser.

Det følger af artikel 45, stk. 1, 1. pkt., i forordningen om cyberrobusthed, at hvis en bemyndigende myndighed har konstateret eller er blevet underrettet om, at et bemyndiget organ ikke længere opfylder kravene i artikel 39, eller at det ikke opfylder sine forpligtelser, begrænser, suspenderer eller inddrager den bemyndigende myndighed bemyndigelsen, alt efter hvad der er relevant, og afhængigt af i hvor høj grad disse krav eller forpligtelser ikke er blevet opfyldt.

Det foreslåede indebærer således, at Styrelsen for Samfundssikkerhed i disse tilfælde som udgangspunkt indledningsvist vil fastsætte en rimelig frist for afhjælpning. Et sådan påbud vil dog kunne kombineres med en foreløbig begrænsning af bemyndigelsen eller suspendering heraf, jf. det foreslåede 2. pkt., afhængigt af, hvad der er relevant i det konkrete tilfælde henset til overtrædelsens karakter.

Det foreslås i *stk. 3, 2. pkt.*, at Styrelsen for Samfundssikkerhed endvidere kan begrænse eller suspendere bemyndigelsen i overensstemmelse med artikel 45 i forordningen om cyberrobusthed.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed i overensstemmelse med artikel 45 i forordningen om cyberrobusthed vil kunne begrænse bemyndigelsen inden for et nærmere bestemt område eller suspendere den, hvorefter overensstemmelsesvurderingsorganet ikke vil kunne foretage vurderinger i henhold til den pågældende bemyndigelse. Dette vil bl.a. kunne ske som led i det foreslåede 1. pkt. om, at der ved konstatering af en overtrædelse indledningsvis fastsættes en frist for afhjælpning.

Styrelsen for Samfundssikkerhed vil i disse tilfælde omgående skulle underrette EU-Kommissionen og de øvrige medlemsstater herom, jf. artikel 45, stk. 1, 2. pkt.

Det fremgår derudover af artikel 45, stk. 2, at hvis en bemyndigelse begrænses, suspenderes eller inddrages, eller hvis det bemyndigede organ har indstillet sin virksomhed, træffer den bemyndigende medlemsstat de nødvendige foranstaltninger for at sikre, at dette organs sager enten behandles af et andet bemyndiget organ eller gøres tilgængelige for de ansvarlige bemyndigende myndigheder og markedsovervågningsmyndigheder efter disses anmodning.

Det foreslås i *stk. 3, 3. pkt.*, at foretages der ikke tilstrækkelig afhjælpning inden for fristen, eller er der tale om gentagen eller grov forsømmelse af forordningens krav, inddrager Styrelsen for Samfundssikkerhed bemyndigelsen.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed inddrager bemyndigelsen, hvis der ikke foretages tilstrækkelig afhjælpning inden for den frist, der er fastsat i medfør af det foreslåede 1. pkt., eller hvis der er tale om gentagen eller særligt grov forsømmelse af forordningens krav.

Foretages der ikke tilstrækkelig afhjælpning inden for fristen, som er fastsat i medfør af 1. pkt., vil inddragelsen således ske i forlængelse heraf.

Er der tale om gentagen eller særligt grov forsømmelse, vil bemyndigelsen kunne inddrages helt eller delvis, f.eks. i forhold til en specifik produktkategori eller branche, hvis det konkret vurderes at være nødvendigt og proportionalt, herunder i 1. gangstilfælde.

Den foreslåede mulighed bør derfor også alene finde anvendelse i tilfælde, hvor dette vurderes nødvendigt og proportionalt ud fra en samlet afvejning mellem hensynet til organets mulighed for fortsat at opretholde bemyndigelsen og karakteren af den eller de pågældende forsømmelser.

Vurderingen af, om en bemyndigelse skal begrænses, suspenderes eller inddrages, vil i overensstemmelse med artikel 45, stk. 1, generelt skulle ske under hensyn til, hvad der er relevant i lyset af karakteren og alvoren af den manglende opfyldelse af kravene.

Det foreslås i *stk. 4*, at Styrelsen for Samfundssikkerhed i forbindelse med bemyndigelse efter stk. 2 kan fastsætte nærmere vilkår om, at et

overensstemmelsesvurderingsorgan søger akkreditering på et senere tidspunkt, hvis der ikke på tidspunktet for bemyndigelse forelå en relevant akkrediteringsordning.

Det foreslåede vil have til formål at understøtte, at der kan ske bemyndigelse, selvom der ikke foreligger et akkrediteringscertifikat, hvor dette ikke er muligt, idet der ikke foreligger en tilgængelig akkrediteringsordning, der er relevant at anvende i den pågældende sammenhæng.

Det foreslåede vil således indebære, at Styrelsen for Samfundssikkerhed i forbindelse med bemyndigelse af et overensstemmelsesorgan vil kunne fastsætte vilkår om, at organet vil skulle søge akkreditering på et senere tidspunkt, når dette bliver muligt, med henblik på opretholdelse af bemyndigelsen.

Der vil således være tale om en foreløbig bemyndigelse, hvortil der er knyttet et nærmere bestemt vilkår om, at bemyndigelsen udløber f.eks. inden en forudbestemt dato, det tidspunkt, hvor akkreditering bliver mulig eller en nærmere fastsat periode herefter, eller når Styrelsen for Samfundssikkerhed henvender sig herom.

Det forudsættes, at vilkåret knyttes til det tidspunkt, hvor det bliver muligt at dokumentere overensstemmelse via en akkrediteringsordning, idet den bliver tilgængelig at anvende. I den mellemliggende periode vil Styrelsen for Samfundssikkerhed overvåge organet i forhold til, om kravene til bemyndigelsen overholdes.

Udgangspunktet om, at et overensstemmelsesvurderingsorgans ansøgning om bemyndigelse ledsages af et akkrediteringscertifikat udstedt af et nationalt akkrediteringsorgan, hvor det attesteres, at overensstemmelsesvurderingsorganet opfylder kravene i artikel 39, følger af forordningens artikel 42, stk. 2.

Det følger dog af artikel 42, stk. 3, at hvis det pågældende overensstemmelsesvurderingsorgan ikke kan forelægge et akkrediteringscertifikat, forelægger det den bemyndigende myndighed al den dokumentation, der er nødvendig for at kontrollere, anerkende og regelmæssigt overvåge, at det opfylder kravene i artikel 39.

Derudover følger det af artikel 43, stk. 3, at hvis en bemyndigelse ikke er baseret på et akkrediteringscertifikat som anført i artikel 42, stk. 2, forelægger den bemyndigende myndighed Kommissionen og de øvrige medlemsstater dokumentation, der attesterer overensstemmelsesvurderingsorganets kompetence og de ordninger, der er indført til sikring af, at der regelmæssigt føres tilsyn med organet, og at organet også fremover vil opfylde de i artikel 39 fastsatte krav.

Der henvises i øvrigt til pkt. 3.2 i lovforslagets almindelige bemærkninger.

Til § 4

Det følger af artikel 36, stk. 2, i forordningen om cyberrobusthed, at medlemsstater kan bestemme, at den i stk. 1 omhandlede vurdering og overvågning skal foretages af et nationalt akkrediteringsorgan i den i forordning nr. 765/2008 anvendte betydning og i overensstemmelse med nævnte forordning.

Det skal i den forbindelse bemærkes, at det følger af præambelbetragtning nr. 100 til forordningen om cyberrobusthed, at overensstemmelsesvurderingsorganer, der er akkrediteret og bemyndiget i henhold til EU-retten, der fastsætter krav svarende til dem, der er fastsat i forordningen om cyberrobusthed, såsom et overensstemmelsesvurderingsorgan, der er bemyndiget til en europæisk cybersikkerhedscertificeringsordning vedtaget i henhold til forordningen om cybersikkerhed eller bemyndiget i henhold til delegeret forordning (EU) 2022/30, skal vurderes og bemyndiges på ny i henhold til forordningen om cyberrobusthed.

Det følger endvidere af præambelbetragtning nr. 101, at gennemsigtig akkreditering efter forordning (EF) nr. 765/2008 bør betragtes som det foretrukne middel til dokumentation af overensstemmelsesvurderingsorganers tekniske kompetence. Nationale myndigheder kan dog vurdere, at de selv råder over passende midler til at foretage denne evaluering, men bør i så fald forelægge Kommissionen og de øvrige medlemsstater den nødvendige dokumentation for, at de evaluerede overensstemmelsesvurderingsorganer overholder de relevante forskriftsmæssige krav med henblik på at sikre et passende troværdighedsniveau for evalueringer, der foretages af andre nationale myndigheder.

Den Danske Akkrediteringsfond (DANAK) er udpeget som Danmarks nationale akkrediteringsorgan efter § 1 i bekendtgørelse nr. 1230 af 11. december 2009 om udpegning af det nationale akkrediteringsorgan i overensstemmelse med Europa-Parlamentets og Rådets forordning nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter.

Det kan i den forbindelse nævnes, at det følger af § 4 i lov om cybersikkerhedscertificering, at DANAK akkrediterer overensstemmelsesvurderingsorganer efter artikel 60, stk. 1, i forordningen om cybersikkerhed, hvis organet opfylder kravene i bilaget til forordningen.

Kravene til de nationale akkrediteringsorganer følger af artikel 8 i Europa-Parlamentets og Rådets forordning nr. 765/2008, hvori der – ligesom i forordningen om cyberrobusthed – bl.a. stilles krav om, at organet 1) er uafhængig af kommercielle interesser, og at der ikke opstår interessekonflikter, 2) kan udøve sin virksomhed objektivt og uvildigt, 3) er indrettet på en sådan måde, at afgørelser om attesting af kompetence træffes af kompetente personer, som ikke må være de samme som dem, der forestår evalueringen, 4) skal have passende procedurer til at garantere en fortrolig behandling af de modtagne oplysninger og 5) skal råde over det antal kompetente ansatte, der er nødvendigt til, at det kan varetage sine opgaver på behørig måde

Det foreslås i *stk. 1*, at Den Danske Akkrediteringsfond (DANAK) foretager efter artikel 36, stk. 2, i forordningen om cyberrobusthed den vurdering og overvågning af overensstemmelsesvurderingsorganer, der er omhandlet i artikel 36, stk. 1, i forordningen om cyberrobusthed, i forbindelse med bemyndigelse, jf. § 3, stk. 2.

Det foreslåede vil indebære, at DANAK som udgangspunkt vil varetage vurdering og overvågning af de overensstemmelsesvurderingsorganer, som akkrediteres af DANAK med henblik på bemyndigelse efter forordningen om cyberrobusthed, mens bemyndigelse af overensstemmelsesvurderingsorganerne varetages af Styrelsen for Samfundssikkerhed som bemyndigende myndighed.

Den foreslåede vurdering vil vedrøre overensstemmelsesvurderingsorganets opfyldelse af kravene i artikel 39, stk. 2-12, i forordningen om cyberrobusthed, mens den efterfølgende overvågning også omfatter organets fortsatte opfyldelse af kravene og, hvor relevant, overholdelsen af artikel 41.

For en nærmere gennemgang af mulighederne for anvendelse af akkreditering henvises der til den foreslåede § 4 og bemærkningerne hertil.

DANAK er som Danmarks nationale akkrediteringsorgan underlagt kravene i artikel 8 i forordning (EF) nr. 765/2008, herunder krav om uafhængighed, objektivitet og uvildighed, adskillelse mellem vurdering og afgørelse om attesting af kompetence, fortrolighed og tilstrækkelige personalemæssige ressourcer. Efter artikel 9, stk. 2, i samme forordning skal medlemsstaterne regelmæssigt overvåge deres nationale akkrediteringsorganer med henblik på at sikre, at kravene i artikel 8 fortsat er opfyldt.

Det foreslås i *stk. 2*, at DANAK inden for en ramme aftalt med Styrelsen for Samfundssikkerhed kan beregne sig betaling for sine ydelser i forbindelse med

akkreditering af virksomheder. De aktuelle satser for DANAK's ydelser offentliggøres på DANAK's hjemmeside og kan erhverves hos DANAK.

Det foreslåede har til formål at sikre, at DANAK kan kræve betaling for sine ydelser i overensstemmelse med gældende praksis, herunder § 16 i bekendtgørelse nr. 913 af 25. september 2009 om akkreditering af virksomheder, hvoraf følger, at efter § 16, stk. 2, 1. pkt., i lov om erhvervsfremme kan DANAK, indenfor en ramme aftalt med Sikkerhedsstyrelsen, beregne sig betaling for sine ydelser i forbindelse med akkreditering af virksomheder. Det fremgår endvidere, at de aktuelle satser for DANAK's ydelser offentliggøres på DANAK's hjemmeside og kan erhverves hos DANAK.

Det foreslåede vil på tilsvarende vis indebære, at DANAK kan opkræve et rimeligt gebyr for vurdering af et overensstemmelsesvurderingsorgan som led i bemyndigelsen heraf, jf. det foreslåede § 3, stk. 2. Gebyret skal fastsættes på baggrund af DANAK's omkostninger til varetagelsen af denne funktion og må således ikke overstige dette. Derudover skal gebyret fremgå af DANAK's hjemmeside.

Der henvises til pkt. 3.2 i lovforslagets almindelige bemærkninger.

Til § 5

Det følger af artikel 52, stk. 2, i forordningen om cyberrobusthed, at hver medlemsstat skal udpege en eller flere markedsovervågningsmyndigheder med henblik på en virksomheds gennemførelse af forordningen. Medlemsstaterne kan i den forbindelse udpege en eksisterende eller ny myndighed til at virke som markedsovervågningsmyndighed.

Markedsovervågningsmyndighederne i henhold til forordningen om cyberrobusthed tildeles med forordningen en række direkte anvendelige håndhævelsesbeføjelser i medfør af artikel 53 om adgang til data, som er nødvendig for at vurdere de omfattede produkter. Markedsovervågningsmyndighederne tildeles herudover en række beføjelser i relation til procedurer for evaluering af produkter og iværksættelse af korrigerende eller restriktive foranstaltninger, jf. artikel 54-57, samt i relation til formel manglende overholdelse af forordningen, jf. artikel 58, fælles aktiviteter, jf. artikel 59, og koordinerede kontrolaktioner, jf. artikel 60.

For en nærmere gennemgang af markedsovervågningsmyndighedernes håndhævelsesbeføjelser kan der henvises til pkt. 3.3.1.2 i lovforslagets almindelige bemærkninger samt de foreslåede bestemmelser herom i §§ 8 og 9 og bemærkninger hertil.

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed udpeges som markedsovervågningsmyndighed i overensstemmelse med artikel 52, stk. 2, i forordningen om cyberrobusthed, jf. dog stk. 2.

Den foreslåede bestemmelse vil indebære, at Styrelsen for Samfundssikkerhed varetager markedsovervågningsopgaver i henhold til forordningen om cyberrobusthed hvilket navnlig vil indebære, at sikre en virkningsfuld gennemførelse af forordningen.

Det foreslåede vil derudover skulle ses i sammenhæng med forordningens artikel 52, stk. 3-16, om markedsovervågningsmyndighedens opgaver, som bl.a. vedrører markedsovervågning med open source software-forvalteres forpligtelser, samarbejde og informationsudveksling med relevante nationale og europæiske myndigheder, vejledning af erhvervsdrivende og deltagelse i ADCO.

Det foreslås i *stk. 2*, at markedsovervågningsmyndigheder udpeget efter forordningen om kunstig intelligens for så vidt angår systemer, der er klassificeret som højrisiko-AI-systemer i medfør af artikel 6 deri, varetager i overensstemmelse med artikel 52, stk. 14, i forordningen om cyberrobusthed markedsovervågning med produkter med digitale elementer, hvori sådanne systemer indgår.

Det foreslåede vil indebære, at den opgavefordeling, der er forudsat i artikel 52, stk. 14, i forordningen om cyberrobusthed for så vidt angår produkter med digitale elementer, hvori der indgår systemer, der er klassificeret som højrisiko-AI-systemer i henhold til artikel 6 i forordningen om kunstig intelligens, tydeliggøres.

Dette skal ses i sammenhæng med, at de kompetente myndigheder udpeges i medfør af lovgivning på Forsknings-, Uddannelses- og Digitaliseringsministeriets område, og har således til formål at sikre, at der kan tages hensyn til den forudsatte og sammenhængende markedsovervågningsopgave samtidig med, at alle markedsovervågningsmyndigheder som udgangspunkt vil have samme beføjelser.

I overensstemmelse med artikel 52, stk. 14, i forordningen om cyberrobusthed vil markedsovervågningsmyndighederne samarbejde, hvor det er relevant, og med CSIRT'en, og ENISA om tilsynet med gennemførelsen af rapporteringsforpligtelserne i henhold til forordningens artikel 14.

Som led i dette samarbejde vil Styrelsen for Samfundssikkerhed efter anmodning fra markedsovervågningsmyndigheder, der er udpeget i medfør af lovgivning på

Forsknings-, Uddannelses- og Digitaliseringsministeriets område, foretage den cybersikkerhedsfaglige vurdering af, om kravene i forordningen om cyberrobusthed er overholdt for så vidt angår de konkrete produkter eller virksomheder m.v., som den pågældende sag vedrører. Vurderingen foretages til brug for markedsovervågningsmyndighedens samlede afgørelse i sagen.

Markedsovervågningsmyndigheder udpeget i henhold til forordningen om kunstig intelligens vil også skulle underrette markedsovervågningsmyndigheder udpeget i henhold til forordningen om cyberrobusthed om ethvert resultat, der er relevant for udførelsen af deres opgaver i forbindelse med gennemførelsen af forordningen om cyberrobusthed. Dette vil f.eks. omfatte afgørelser, der er relevante for Styrelsen for Samfundssikkerhed i forhold til styrelsens udførelse af opgaver i henhold til forordningen om cyberrobusthed, f.eks. vedrørende produkters cybersikkerhed,

Denne underretningspligt vil også medvirke til at, at Styrelsen for Samfundssikkerhed som national koordinerende myndighed i medfør af det foreslåede § 7 har det nødvendige overblik over relevante afgørelser for at kunne varetage koordineringsopgaven både nationalt og i forhold til det europæiske samarbejde.

Det foreslås i *stk. 3*, at ministeren for Samfundssikkerhed og Beredskab efter forhandling med vedkommende minister vil kunne fastsætte nærmere regler om tilrettelæggelse og koordinering af markedsovervågningsopgaver omfattet af *stk. 2*.

Det foreslåede vil indebære, at ministeren for samfundssikkerhed og beredskab efter forhandling med vedkommende minister vil kunne fastsætte nærmere regler med henblik på f.eks. at sikre en hensigtsmæssig sammenhæng mellem markedsovervågningsmyndighedernes opgaver efter henholdsvis forordningen om cyberrobusthed og forordningen om kunstig intelligens, tydeliggøre den nationale myndighedsfordeling eller at imødekomme nye EU-retlige krav.

Der henvises endvidere til pkt. 3.2 i lovforslagets almindelige bemærkninger.

Til § 6

Markedsovervågningen efter forordningen om cyberrobusthed vedrører produkter med digitale elementer på tværs af produktkategorier, sektorer og anvendelsesområder.

Markedsovervågningsforordningen indeholder derudover en generel ramme for national og europæisk koordinering af markedsovervågningen, herunder regler om et

centralt forbindelseskantor i artikel 10, stk. 3 og 4, og en overordnet national markeds-
overvågningsstrategi i artikel 13.

Der foreligger dog ikke en eksisterende særskilt national ramme, der kan understøtte
en ensartet og sammenhængende markedsovervågning efter forordningen om cyber-
robusthed i tilfælde, hvor flere myndigheder udfører markedsovervågningsopgaver i
henhold til forordningen.

Det følger endvidere af artikel 52, stk. 6, i forordningen om cyberrobusthed, at mar-
kedsovervågningsmyndighederne, hvor det er relevant, skal samarbejde og regelmæs-
sigt udveksle oplysninger med markedsovervågningsmyndigheder, der er udpeget på
grundlag af anden EU-harmoniseringslovgivning. For produkter med digitale elemen-
ter, der samtidig er klassificeret som højrisiko-AI-systemer efter artikel 6 i forordnin-
gen om kunstig intelligens, følger det af artikel 52, stk. 14, i forordningen om cyber-
robusthed, at markedsovervågningsmyndighederne efter forordningen om kunstig in-
telligens er ansvarlige for markedsovervågningen efter forordningen om cyberro-
busthed. Efter artikel 52, stk. 15, oprettes der desuden en gruppe for administrativt
samarbejde (ADCO) med henblik på en ensartet anvendelse af forordningen om cy-
berrobusthed.

Det følger derudover af artikel 59, stk. 1, i forordningen om cyberrobusthed, at mar-
kedsovervågningsmyndighederne kan aftale med andre relevante myndigheder at gen-
nemføre fælles aktiviteter med henblik på at sikre cybersikkerheden og beskyttelsen
af forbrugerne i relation til bestemte produkter med digitale elementer, navnlig pro-
dukter, der ofte viser sig at udgøre cybersikkerhedsrisici. Efter artikel 59, stk. 2, skal
Kommissionen eller ENISA foreslå fælles aktiviteter med henblik på at kontrollere
overholdelsen af forordningen, hvis der foreligger oplysninger om mulig manglende
overholdelse på tværs af flere medlemsstater.

Det følger endvidere af artikel 60 i forordningen om cyberrobusthed, at markedsover-
vågningsmyndighederne gennemfører samtidige, koordinerede kontrolaktioner vedrø-
rende bestemte produkter med digitale elementer eller kategorier heraf for at kontrol-
lere overholdelsen af forordningen eller afdække overtrædelser. Kontrolaktiviteterne
kan bl.a. omfatte inspektioner af produkter, der er erhvervet under dækidentitet. Det
fremgår af præambelbetragtning nr. 114, at sådanne kontrolaktioner er specifikke
håndhævelsesforanstaltninger, der navnlig bør gennemføres, hvis markedstendenser,
forbrugerklager eller andre oplysninger tyder på, at bestemte produktkategorier ofte
udgør cybersikkerhedsrisici. Det følger af artikel 60, stk. 2, at sådanne kontrolaktivi-
teter som udgangspunkt koordineres af Kommissionen, medmindre de deltagende

markedsovervågningsmyndigheder aftaler andet. ENISA kan endvidere efter artikel 60, stk. 3, foreslå kategorier af produkter med digitale elementer, for hvilke der kan gennemføres kontrolaktioner.

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed udpeges som national koordinerende myndighed for markedsovervågning efter forordningen om cyberrobusthed.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed som national koordinerende myndighed vil fungere som det nationale koordinerings- og kontaktpunkt for markedsovervågning efter forordningen om cyberrobusthed med hensyn til øvrige markedsovervågningsmyndigheder i både national sammenhæng og i forhold til andre EU-medlemslande og EU's institutioner, jf. også det foreslåede *stk. 2*. Opgaven vil ikke berøre det centrale forbindelseskontors opgaver efter markedsovervågningsforordningens artikel 10.

Det foreslås i *stk. 2*, at Styrelsen for Samfundssikkerhed som national koordinerende myndighed fastsætter en national strategisk ramme for markedsovervågningen efter forordningen om cyberrobusthed samt koordinerer samarbejdet mellem markedsovervågningsmyndighederne udpeget efter § 6, stk. 2, herunder i forbindelse med fælles aktiviteter efter forordningens artikel 59 og de koordinerede kontrolaktioner efter forordningens artikel 60.

Det foreslåede vil navnlig indebære, at Styrelsen for Samfundssikkerhed fastsætter fælles principper for den risikobaserede tilrettelæggelse og prioritering af markedsovervågningen efter forordningen om cyberrobusthed samt koordinering og udveksling af oplysninger mellem markedsovervågningsmyndighederne som omhandlet i § 6, herunder i forbindelse med fælles aktiviteter efter forordningens artikel 59 og dansk deltagelse i de koordinerede kontrolaktioner efter forordningens artikel 60.

Styrelsen for Samfundssikkerhed vil derudover koordinere Danmarks deltagelse i det europæiske samarbejde om markedsovervågning efter forordningen, herunder ADCO, jf. forordningens artikel 52, stk. 15.

Den nationale strategiske ramme vil skulle understøtte, at markedsovervågningen tilrettelægges risikobaseret og målrettes de produktområder og risici, hvor behovet for kontrol vurderes størst. Rammen vil samtidig skulle understøtte national sammenhæng i markedsovervågningen og sikre, at danske kontrolindsatser og prioriteringer kan koordineres med det europæiske samarbejde for så vidt angår forordningen om cyberrobusthed.

Bestemmelsen vil endvidere indebære, at Styrelsen for Samfundssikkerhed skal koordinere den nationale proces i tilfælde, hvor der iværksættes foranstaltninger over for produkter, der vurderes at udgøre en væsentlig cybersikkerhedsrisiko i henhold til forordningens artikel 54, eller hvor der opstår spørgsmål om indsigelser efter forordningens EU-beskyttelsesprocedure i henhold til artikel 55.

Bestemmelsen skal ses i sammenhæng med det foreslåede § 6, stk. 2, idet de myndigheder, der er omhandlet deri, vil skulle udføre markedsovervågningsopgaver inden for den strategiske ramme, herunder straks underrette Styrelsen for Samfundssikkerhed om relevante afgørelser og foranstaltninger vedrørende produkters cybersikkerhed, jf. forordningens artikel 54-58. Dette vil have til formål at sikre, at markedsovervågningsopgaver, som varetages af andre myndigheder, sker i sammenhæng med den nationale strategiske ramme for markedsovervågning efter forordningen om cyberrobusthed, men dog uden at ændre den kompetencefordeling, der følger af forordningen eller anden lovgivning.

Den strategiske ramme vil således ikke ændre myndighedernes kompetencer eller forpligtelser i henhold til anden lovgivning, herunder forordningen om cyberrobusthed og forordningen om kunstig intelligens.

For så vidt angår de koordinerede kontrolaktioner i medfør af artikel 60 i forordningen om cyberrobusthed bemærkes det, at kontrollen udføres af den markedsovervågningsmyndighed, der har kompetencen for det pågældende produkt. Vedrører kontrolaktionen et produkt med digitale elementer, der er klassificeret som et højrisiko-AI-system efter artikel 6 i forordningen om kunstig intelligens, udføres kontrollen således af den relevante markedsovervågningsmyndighed efter forordningen om kunstig intelligens, mens Styrelsen for Samfundssikkerhed som national koordinerende myndighed koordinerer den danske deltagelse og samarbejdet i ADCO. Styrelsen for Samfundssikkerhed vil dog generelt kunne bistå de myndigheder, der er omhandlet i det foreslåede § 6, stk. 2, i nødvendigt omfang på baggrund af nærmere aftale herom.

Det foreslås i *stk. 3*, at de markedsovervågningsmyndigheder, der er nævnt i § 6, stk. 2, skal tilrettelægge deres markedsovervågning efter den i stk. 2 nævnte nationale strategiske ramme og underretter straks Styrelsen for Samfundssikkerhed om afgørelser, foranstaltninger og konstateringer vedrørende produkters cybersikkerhed, der er truffet i medfør af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Det foreslåede har til formål at sikre en ensartet og koordineret markedsovervågningsindsats på tværs af markedsovervågningsmyndighederne. Det foreslås derfor, at de markedsovervågningsmyndigheder, der er nævnt i § 6, stk. 2, vil skulle tilrettelægge deres markedsovervågningsaktiviteter efter den nationale strategiske ramme, som er fastsat af Styrelsen for Samfundssikkerhed.

Med samme formål og på baggrund af den foreslåede udpegning af Styrelsen for Samfundssikkerhed som national koordinerende myndighed, vil de markedsovervågningsmyndigheder, der er nævnt i § 6, stk. 2, også straks skulle underrette Styrelsen for Samfundssikkerhed om afgørelser, foranstaltninger og konstateringer vedrørende produkters cybersikkerhed, der er truffet i medfør af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Det foreslås i *stk. 4*, at ministeren for samfundssikkerhed og beredskab efter forhandling med vedkommende minister kan fastsætte nærmere regler om samarbejde, koordinering og informationsudveksling mellem markedsovervågningsmyndighederne og markedsovervågningsmyndighederne og CSIRT'en.

Det foreslåede vil indebære, at ministeren for samfundssikkerhed og beredskab efter forhandling med vedkommende minister kan fastsætte nærmere regler om den praktiske tilrettelæggelse af samarbejdet mellem disse myndigheder, herunder om procedurer for underretning, koordinering af kontrolindsatser og udveksling af oplysninger.

Til § 7

Forordningen om cyberrobusthed forudsætter, at markedsovervågningsmyndigheden kan føre kontrol med produkter med digitale elementer og med de processer, som fabrikanter m.v. har indført for at opfylde kravene efter forordningen. Det er derfor nødvendigt, at de kompetente myndigheder får tilstrækkelig adgang til omfattede produkter, software og digitale funktioner.

Dette gælder både fysiske produkter, softwareprodukter og produkter, hvis funktioner eller komponenter kan tilgås digitalt. Det vil i den forbindelse kunne være nødvendigt, at myndigheden får adgang til produktet, herunder fysisk eller logisk adgang til software, hardware eller relevante digitale funktioner og komponenter i det produkt, der er udtaget til kontrol. Dette gælder både for fysiske produkter, softwareprodukter og produkter, hvor funktioner eller komponenter tilgås digitalt.

Det følger i den forbindelse af artikel 53 i forordningen om cyberrobusthed, at hvis det er nødvendigt for at vurdere, om produkter med digitale elementer og de processer, som fabrikanten har indført, opfylder de væsentlige cybersikkerhedskrav i bilag I, tildeles markedsovervågningsmyndighederne efter begrundet anmodning adgang til de data på et for dem let forståeligt sprog, som er nødvendige for at vurdere designet, udviklingen, produktionen og sårbarhedshåndteringen af sådanne produkter, herunder den relevante interne dokumentation fra den relevante erhvervsdrivende.

Dette skal ses i sammenhæng med artikel 63 stk. 1, hvoraf følger, at alle parter, der er involveret i anvendelsen af denne forordning, skal overholde tavshedspligten for oplysninger og data, der indhentes under udførelsen af deres opgaver og arbejde, på en sådan måde, at de navnlig beskytter: a) intellektuelle ejendomsrettigheder og fysiske eller juridiske personers fortrolige forretningsoplysninger eller forretningshemmeligheder, herunder kildekode, med undtagelse af de tilfælde, der er omhandlet i artikel 5 i Europa-Parlamentets og Rådets direktiv (EU) 2016/943 af 8. juni 2016, b) den effektive gennemførelse af denne forordning, navnlig for så vidt angår inspektioner, undersøgelser eller kontrolbesøg, c) offentlige og nationale sikkerhedsinteresser og d) strafferetlige eller administrative procedurers integritet.

Det følger derudover af artikel 63 stk. 2, at uden at det berører stk. 1, må oplysninger, der udveksles på fortrolig basis mellem markedsovervågningsmyndighederne og mellem markedsovervågningsmyndighederne og EU-Kommissionen, ikke videregives uden forudgående tilladelse fra den oprindelige markedsmyndighed.

Det følger endvidere af artikel 63 stk. 3, at stk. 1 og 2 ikke berører EU-Kommissionens, medlemsstaternes og de bemyndigede organers rettigheder og forpligtelser med hensyn til udveksling af oplysninger og udsendelse af advarsler eller de berørte personers forpligtelse til at afgive oplysninger inden for rammerne af medlemsstaternes strafferet.

Endelig følger det af 63 stk. 4, at EU-Kommissionen og medlemsstaterne om nødvendigt kan udveksle følsomme oplysninger med relevante myndigheder i tredjelande, med hvilke de har indgået bilaterale eller multilaterale aftaler om fortrolighed, der garanterer en tilstrækkelig grad af beskyttelse.

Det foreslås i § 7, at markedsovervågningsmyndighederne kan afkræve alle oplysninger, som er nødvendige for myndighedernes virksomhed, fra fysiske og juridiske personer omfattet af forordningen om cyberrobusthed, herunder til fastlæggelse af om et

forhold er omfattet af bestemmelserne i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Det foreslåede vil indebære, at det tydeliggøres, at markedsovervågningsmyndighederne vil kunne indhente alle oplysninger fra fysiske og juridiske personer, som er nødvendige for myndighedernes markedsovervågnings- og håndhævelsesforpligtelser i henhold til forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf. Alle oplysninger, der er nødvendige og kræves til udførelse af myndighedens opgaver, vil være omfattet.

De nævnte myndigheder vil således kunne kræve af fabrikanter og andre erhvervsdrivende omfattet af forordningen om cyberrobusthed at få tilsendt dokumentation relateret til produkter med digitale elementer, herunder om fremstilling, anvendelse og funktioner. Oplysningerne kan bl.a. også omfatte oplysninger om overensstemmelse, vurderinger, kildekode, testresultater, fagtekniske vurderinger og oplysninger om, hvor mange eksemplarer, der er bragt i omsætning, hvordan og til hvem. Videre kan der, hvad angår overensstemmelsesvurderingsorganer, være tale om dokumentation for uddannelse, løn, forsikring, ansættelsesvilkår, arbejdsgange, kvalitetsledelsessystemer, procedurer og arbejdsprocesser.

Det forudsættes, at de pågældende oplysninger er nødvendige for markedsovervågningsmyndighedernes aktiviteter, og at der er foretaget en konkret proportionalitetsafvejning i hver enkelt sag. Oplysningerne skal derudover være tilgængelig for de pågældende fabrikanter mv., og det kan ikke kræves, at der genereres nye data og dokumentation.

Markedsovervågningsmyndighederne vil kunne foretage kopiering af materialet eller kræve at få udleveret dette under hensyntagen til de generelle regler om fortrolighed i forbindelse med håndtering af oplysninger i medfør af artikel 63.

Bestemmelsen afgrænses af det almindelige forbud mod at udsætte andre for selvinkriminering, som det bl.a. kan udledes af Den Europæiske Menneskerettighedskonventions artikel 6 og § 10 i lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (retssikkerhedsloven). Er der konkret mistanke om, at det af oplysningerne vil fremgå, at den pågældende har begået noget strafbart, kan det således ikke kræves, at oplysningerne udleveres.

Den foreslåede bestemmelse vil navnlig være relevant i tilfælde, som falder uden for anvendelsesområdet af de øvrige foreslåede bestemmelser om kontrol af produkter og

adgang til data, herunder hvis det ikke endnu er fastslået, om forordningen om cyberrobusthed finder anvendelse.

Til § 8

Forordningen om cyberrobusthed forudsætter, at markedsovervågningsmyndigheden kan føre kontrol med produkter med digitale elementer og med de processer, som fabrikanten har indført for at opfylde kravene efter forordningen. Dette skal ses i sammenhæng med forordningens artikel 52, stk. 1, og præambelbetragtning nr. 106 om, at reglerne om EU-markedsovervågning og kontrol af produkter, der indføres på EU-markedet, i markedsovervågningsforordningen finder anvendelse på produkter med digitale elementer, der er omfattet af nærværende forordnings anvendelsesområde.

Der følger i den forbindelse en række direkte anvendelige kontrolbeføjelser af markedsovervågningsforordningen, mens bl.a. de beføjelser, der fremgår af artikel 14, stk. 4, kræver, at de er blevet tillagt markedsovervågningsmyndighederne, hvilket sker delvis med forordningen om cyberrobusthed.

Der henvises i den forbindelse til pkt. 3.3.1.2 for en nærmere gennemgang af de direkte anvendelige håndhævelsesbeføjelser i henhold til forordningen om cyberrobusthed.

Bestemmelserne i det foreslåede § 8 har dermed til formål at supplere håndhævelsesbeføjelserne i forordningen om cyberrobusthed for at sikre, at markedsovervågningsmyndighederne i henhold til forordningen om cyberrobusthed har beføjelser, der svarer til markedsovervågningsforordningen. Der findes således ikke i gældende ret supplerende regler herom på Ministeriet for Samfundssikkerhed og Beredskabs område, ligesom der f.eks. gør på Erhvervsministeriets område i medfør af lov om produkter og markedsovervågning, jf. lovbekendtgørelse nr. 22 af 8. januar 2026.

Det foreslås i *stk. 1*, at markedsovervågningsmyndighederne som led i markedsovervågning efter forordningen om cyberrobusthed, herunder evalueringer efter forordningens artikel 54, kan udtage ethvert produkt med digitale elementer, der er omfattet af forordningen om cyberrobusthed, der er omfattet af denne lovs anvendelsesområde, herunder ved brug af en skjult identitet, for at kontrollere, om produkter og de processer, som fabrikanten har indført, opfylder kravene i forordningen om cyberrobusthed.

Det foreslåede skal ses i sammenhæng med artikel 14, stk. 4, litra j, i markedsovervågningsforordningen, som bl.a. er gennemført med § 12, stk. 1, i lov om produkter og markedsovervågning. Det følger heraf, at de beføjelser, der tillægges

markedsovervågningsmyndighederne mindst skal omfatte beføjelsen til at erhverve produktprøver, herunder under en skjult identitet, til at kontrollere disse prøver og foretage reverse engineering på dem med henblik på at identificere manglende overensstemmelse og indhente dokumentation.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed og de myndigheder, der er nævnt i § 5, stk. 2, som led i markedsovervågning vil kunne udtage produkter, således at et produkt med digitale elementer kan stilles til rådighed for kontrol. Dette vil f.eks. kunne ske ved, at produktet erhverves fra offentligt tilgængelige lokaliteter såsom fysiske butikker eller fra webbutikker, hvorefter kontrolmyndigheden har ejendomsretten til de udtagne produkter.

Det forudsættes, at markedsovervågningsmyndighederne kun udtager produkter, som er nødvendige for en effektiv kontrol. Det er dog ikke en forudsætning for, at et produkt kan udtages, at kontrolmyndigheden har en konkret mistanke om, at produktet ikke er i overensstemmelse med forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

For så vidt angår brugen af skjult identitet vil det foreslåede indebære, at markedsovervågningsmyndigheden kan erhverve eller få adgang til et produkt uden at give sig til kende som myndighed, når det er nødvendigt for kontrollen. Beføjelsen vil alene kunne anvendes, når det er relevant og proportionalt for varetagelsen af opgaven med markedsovervågning.

Det foreslåede vil medføre, at der fastsættes en klar national ramme for, hvordan markedsovervågningsmyndigheden kan udtage produkter og få dem stillet til rådighed for kontrol og skal endvidere ses i sammenhæng med artikel 60, stk. 1, i forordningen om cyberrobusthed, hvorefter koordinerede kontrolaktiviteter kan omfatte inspektioner af produkter med digitale elementer, der er erhvervet under en dækidentitet.

Det foreslåede vil skulle ses i sammenhæng med reglerne om fortrolighed i artikel 63 i forordningen om cyberrobusthed, som bl.a. finder anvendelse for markedsovervågningsmyndighedernes håndtering af oplysninger. Der henvises til bemærkningerne til § 7 for en nærmere gennemgang heraf.

Det foreslås i *stk. 2*, at markedsovervågningsmyndighederne efter anmodning herom kan kræve, at erhvervsdrivende stiller et produkt med digitale elementer til rådighed for kontrol og, hvis det er relevant for kontrollen, giver adgang til relevante produkt-

relaterede udviklings-, test-, produktions- eller driftsmiljøer, som fabrikanten råder over.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed og de myndigheder, der er nævnt i § 5, stk. 2, efter anmodning herom vil kunne kræve, at erhvervsdrivende stiller et produkt med digitale elementer, der er omfattet af forordningen om cyberrobusthed til rådighed for kontrol. Dette vil for fysiske produkter f.eks. kunne ske ved indsendelse eller udlevering af produktet, mens det for softwareprodukter eller digitale funktioner efter omstændighederne vil kunne ske ved, at myndigheden gives adgang til softwaren, relevante funktioner, brugergrænseflader, testmiljøer eller andre digitale dele af produktet, der er nødvendige for kontrollen.

Det foreslåede vil bl.a. omfatte adgang til produktet, herunder fysisk eller logisk adgang til software, hardware eller relevante digitale funktioner og komponenter i det produkt, der er udtaget til kontrol. Dette gælder både for fysiske produkter, softwareprodukter og produkter, hvor funktioner eller komponenter tilgås digitalt.

Bestemmelsen vil således ikke indebære, at markedsovervågningsmyndigheden vil få generel adgang til en virksomheds systemer eller infrastruktur. Adgangen skal være knyttet til kontrollen med det konkrete produkt med digitale elementer og skal udøves under iagttagelse af de almindelige forvaltningsretlige principper om nødvendighed og proportionalitet.

Det foreslåede vil skulle ses i sammenhæng med præambelbetragtning nr. 107, hvoraf følger, at erhvervsdrivende bør samarbejde fuldt ud med markedsovervågningsmyndigheder og andre kompetente myndigheder, hvilket således indebærer, at de omfattede erhvervsdrivende vil skulle stille produktet til rådighed for kontrol ved indsendelse, udlevering eller ved at give adgang til produktet, softwaren eller relevante digitale funktioner, herunder også logiske og fysiske adgange.

Derudover vil markedsovervågningsmyndighederne kunne kræve at få adgang til relevante produktrelaterede udviklings-, test-, produktions- eller driftsmiljøer, som fabrikanten råder over, når det er nødvendigt for kontrollen med produktet eller de processer, som fabrikanten har indført. For hardwareprodukter vil dette kunne omfatte faciliteter og systemer, der anvendes ved fremstillingen og afprøvningen af produktet, mens det for softwareprodukter f.eks. vil kunne omfatte miljøer, der anvendes til udvikling, test, opbygning og frigivelse af softwaren.

Det foreslås i *stk. 3*, at markedsovervågningsmyndighederne som led i den kontrol, der er nævnt i *stk. 1*, kan foretage eller få foretaget tekniske undersøgelser af produktet og i den forbindelse indhente teknisk eller anden faglig bistand i relevant omfang.

Det foreslåede skal ses i sammenhæng med markedsovervågningsforordningens artikel 11, *stk. 3*, hvoraf det bl.a. fremgår, at markedsovervågningsmyndighederne gennemfører passende kontrol af produkternes egenskaber i et passende omfang ved hjælp af dokumentbaseret kontrol og, hvis det er relevant, fysisk kontrol og laboratorieundersøgelser baseret på et passende antal prøver.

Det foreslåede vil således indebære, at det tydeliggøres, at markedsovervågningsmyndighederne kan foretage eller få foretaget tekniske undersøgelser, herunder manuel gennemgang af dokumentation, med henblik på at vurdere, om produktet og de processer, som fabrikanten har indført, opfylder kravene i forordningen om cyberrobusthed.

Undersøgelserne vil bl.a. kunne omfatte dokumentbaseret kontrol samt fysiske og logiske funktions- og sikkerhedstest, laboratorieundersøgelser samt analyse af hardware og software, herunder firmware og anden indlejret software, samt fysisk eller logisk undersøgelse af produktet, analyse af grænseflader, kommunikationsprotokoller og netværkstrafik. Tekniske undersøgelser vil endvidere kunne omfatte sårbarhedsscanning, test af adgangskontrol og opdateringsfunktioner samt, hvor det er nødvendigt, penetrationstest eller reverse engineering. Valget af undersøgelsesmetode vil skulle bero på produktets karakter og formålet med kontrollen og derudover være nødvendigt og proportionalt. De foreslåede tekniske undersøgelser vil bl.a. kunne være relevante i forbindelse med evalueringer.

Markedsovervågningsmyndighederne vil derudover kunne indhente teknisk eller anden faglig bistand og anvende eksterne testmiljøer, herunder i udlandet, med henblik på at udføre de fornødne undersøgelser i forbindelse med varetagelsen af funktionen som markedsovervågningsmyndighed.

Den eksterne bistand vil bl.a. kunne indhentes fra andre myndigheder, prøvningslaboratorier, udbydere af cybersikkerhedsfaglige testmiljøer og andre uafhængige sagkyn-dige. I den forbindelse vil myndighederne, i det omfang det er nødvendigt for undersøgelsen, kunne stille det pågældende produkt eller en produktprøve samt de relevante oplysninger, data og dokumentation til rådighed for den, der yder bistanden.

Det bemærkes, at artikel 63 om tavshedspligt i forordningen om cyberrobusthed finder anvendelse for alle parter, der er involveret i anvendelsen af forordningen. Videregivelse af produkter, oplysninger, data og dokumentation vil derudover skulle ske under iagttagelse af de øvrige gældende regler om tavshedspligt, forretningshemmeligheder og beskyttelse af personoplysninger.

Det foreslås i *stk. 4*, at markedsovervågningsmyndighederne kan kræve omkostninger forbundet med kontrol refunderet af den erhvervsdrivende, hvis der træffes afgørelse om manglende overensstemmelse med krav i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Det foreslåede skal ses i sammenhæng med artikel 15, stk. 1, i markedsovervågningsforordningen, hvoraf følger, at medlemsstaterne kan tillade deres markedsovervågningsmyndigheder at opkræve alle omkostninger ved deres aktiviteter fra den relevante erhvervsdrivende for så vidt angår tilfælde af manglende overensstemmelse.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed og de myndigheder, der er nævnt i § 5, stk. 2, f.eks. vil kunne kræve alle omkostninger forbundet med kontrol refunderet af den erhvervsdrivende, som en afgørelse om manglende overensstemmelse med forordningen om cyberrobusthed er rettet mod.

Dette omfatter f.eks. markedsovervågningsmyndighedens nødvendige udgifter til udtagning af produkter, transport til den lokalitet, som markedsovervågningsmyndigheden anviser, prøvning, herunder eksterne tekniske undersøgelser og oplagring. Den foreslåede mulighed for at kræve omkostninger refunderet vil således have karakter af et gebyr.

Der henvises til pkt. 3.3 i lovforslagets almindelige bemærkninger.

Til § 9

Det følger af artikel 14, stk. 4, litra d og e, i markedsovervågningsforordningen, at markedsovervågningsmyndighederne mindst skal have beføjelse til at gennemføre uanmeldte kontrolbesøg og fysisk kontrol af produkter samt til at få adgang til lokaler, arealer eller transportmidler, som den pågældende erhvervsdrivende anvender erhvervsmæssigt, med henblik på at konstatere manglende overholdelse med forordningen om cyberrobusthed og indhente dokumentation.

Dette skal ses i sammenhæng med artikel 52, stk. 1, i forordningen om cyberrobusthed, hvoraf følger, at markedsovervågningsforordningen finder anvendelse på produkter med digitale elementer, der er omfattet af nærværende forordnings anvendelsesområde.

Det foreslås i *stk. 1*, at markedsovervågningsmyndighederne, i det omfang det er nødvendigt for kontrol eller evaluering vedrørende et produkt med digitale elementer omfattet af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf, mod behørig legitimation og uden retskendelse skal have adgang til erhvervsmæssige lokaliteter, hvor produktet findes eller kan antages at findes, herunder hvor produktet er installeret eller taget i brug, eller hvor der findes eller kan antages at findes oplysninger, dokumentation, systemer, data eller andet materiale, som er nødvendigt for kontrollen med produktet.

Det foreslåedes har således til formål at sikre, at markedsovervågningsmyndighederne i henhold til forordningen om cyberrobusthed har den tilsvarende adgang til lokaliteter mv., som følger af markedsovervågningsforordningen.

Det foreslåede vil indebære, at markedsovervågningsmyndighederne, i det omfang det er nødvendigt for kontrol vedrørende et produkt med digitale elementer omfattet af denne lov, mod behørig legitimation og uden retskendelse, vil have adgang til erhvervsmæssige lokaliteter, hvor produktet findes eller kan antages at findes, herunder hvor produktet er installeret eller taget i brug, eller hvor der findes eller kan antages at findes oplysninger, dokumentation, systemer, data eller andet materiale, som er nødvendigt for kontrollen med produktet.

Adgangen vil således kunne omfatte besigtigelse af produktets faktiske installation, konfiguration, tilslutninger, opdateringsfunktioner og andre digitale funktioner, når disse forhold har betydning for vurderingen af produktets overholdelse af forordningen. Efter omstændighederne kan bestemmelsen også omfatte erhvervsmæssige lokaliteter, hvor en fjerndatabehandlingsløsning drives, eller hvor data med tilknytning til det konkrete produkt behandles eller lagres, hvis adgangen er nødvendig for kontrollen.

Bestemmelsen skal ses i lyset af, at produkter med digitale elementer ikke altid kan kontrolleres alene ved gennemgang af dokumentation.

Bestemmelsen vil dog ikke give markedsovervågningsmyndigheden en generel adgang til en virksomheds eller kundes systemer, driftsmiljø eller øvrige infrastruktur,

alene fordi et produkt med digitale elementer er installeret eller taget i brug dér. Adgangen skal være knyttet til kontrollen med det konkrete produkt og begrænset til de forhold, oplysninger, data eller systemer, der er nødvendige for kontrollen. Beføjelsen skal udøves under iagttagelse af nødvendighed og proportionalitet.

Ved vurderingen af nødvendigheden skal der bl.a. lægges vægt på, om kontrollen kan gennemføres tilstrækkeligt ved gennemgang af dokumentation, udtagning af et produkt eller fjernadgang til relevante digitale funktioner. Adgang til en erhvervsmæssig lokation bør kun anvendes, når mindre indgribende kontrolmetoder ikke giver et tilstrækkeligt grundlag for kontrollen.

Den foreslåede adgang vil generelt skulle ske under hensyntagen til bestemmelserne i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (herefter retssikkerhedsloven), herunder de almindelige regler om fravigelse af varsling af tilsyn. Herudover skal særligt retssikkerhedslovens § 10, om retten til ikke at inkriminere sig selv, iagttages ved anvendelsen af bestemmelsen. Det gør sig især gældende i tilfælde, hvor bestemmelsen anvendes, fordi myndigheden har en mistanke om et strafbart forhold.

Det foreslås i *stk. 2*, at markedsovervågningsmyndighederne som led i den kontrol, der er omtalt i *stk. 1*, kan fotografere og optage video, herunder skærbilleder og skærmoptagelser, når det er nødvendigt for at dokumentere kontrollen eller evalueringen.

Det foreslåede har til formål at sikre, at Styrelsen for Samfundssikkerhed og de myndigheder, der er nævnt i § 5, *stk. 2*, på dette område har beføjelser, der svarer til Erhvervsstyrelsens tilsvarende beføjelser i medfør af den gældende bestemmelse i § 11, *stk. 3*, i lov om produkter og markedsovervågning. Det følger heraf, at kontrolmyndigheden som en del af dokumentationen af kontrolbesøget kan fotografere og optage video samt medtage prøver til nærmere analyse eller undersøgelse.

Det foreslåede vil således indebære, at det tydeliggøres, at disse myndigheder i forbindelse med den kontrol, der er omtalt i *stk. 1*, vil kunne fotografere og optage video, herunder skærbilleder og skærmoptagelser, når det er nødvendigt for at dokumentere kontrollen eller evalueringen, herunder med henblik på at dokumentere produktets mærkning, installation, konfiguration, brugergrænseflade, opdateringsfunktioner, sikkerhedsindstillinger eller andre forhold, der er relevante for vurderingen af produktets overholdelse af forordningen.

Det foreslåede har ikke derudover til formål at udelukke, at Styrelsen for Samfundssikkerhed og de myndigheder, der er nævnt i § 5, stk. 2, i øvrigt kan fotografere og optage video m.v. som led i tilsynet med produkter med digitale elementer i medfør af andre bestemmelser herom i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf. Derudover vil produkter m.v. kunne medtages i medfør af de foreslåede bestemmelser i § 9, stk. 1 og 2, om at udtage produkter og at kræve, at de stilles til rådighed for kontrol.

Til § 10

Det følger af artikel 33, stk. 1, i forordningen om cyberrobusthed, at medlemsstaterne, hvor det er relevant, iværksætter følgende tiltag skræddersyet til mikrovirksomheders og små virksomheders behov: Tilrettelæggelse af specifikke oplysnings- og uddannelsesaktiviteter om anvendelsen af denne forordning, jf. litra a, oprettelse af en særlig kommunikationskanal for mikrovirksomheder og små virksomheder og, i det omfang det er relevant, lokale offentlige myndigheder med henblik på at yde rådgivning og besvare spørgsmål om gennemførelsen af denne forordning, jf. litra b, og støtte af afprøvnings- og overensstemmelsesvurderingsaktiviteter, herunder, hvor det er relevant, med støtte fra Det Europæiske Kompetencecenter for Cybersikkerhed, jf. litra c.

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed, hvor det er relevant, iværksætter følgende tiltag skræddersyet til mikrovirksomheders og små virksomheders behov: 1) Tilrettelæggelse af specifikke oplysnings- og uddannelsesaktiviteter om anvendelsen af forordningen om cyberrobusthed. 2) Oprettelse af en særlig kommunikationskanal for mikrovirksomheder og små virksomheder og, i det omfang det er relevant, lokale offentlige myndigheder med henblik på at yde rådgivning og besvare spørgsmål om gennemførelsen af forordningen om cyberrobusthed. 3) Støtte af afprøvnings- og overensstemmelsesvurderingsaktiviteter, herunder, hvor det er relevant, med støtte fra Det Europæiske Kompetencecenter for Cybersikkerhed.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed skal fastsætte de i nr. 1-3 nævnte støtteforanstaltninger for mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder, hvor det vurderes at være relevant.

I den forbindelse vil Styrelsen for Samfundssikkerhed, i overensstemmelse med præambelbetragtning nr. 94, med henblik herpå kunne udvikle initiativer, der er rettet mod fabrikanter, der er mikrovirksomheder eller små virksomheder, herunder for så vidt angår aktiviteter vedrørende uddannelse, bevidstgørelse, kommunikation af oplysninger, afprøvning og tredjepartsoverensstemmelsesvurdering samt oprettelse af

sandkasser. Det vil også kunne bestemmes, at et af de sprog, som anvendes og accepteres til de relevante fabrikanters dokumentation og til kommunikation med fabrikanter, er et sprog, der forstås bredt af det størst mulige antal brugere.

Det foreslås i *stk. 2*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om oprettelse af reguleringsmæssige sandkasser for cyberrobusthed i overensstemmelse med artikel 33, stk. 2, i forordningen om cyberrobusthed.

Det foreslåede skal ses i sammenhæng med artikel 33, stk. 2, i forordningen om cyberrobusthed, hvoraf følger, at medlemsstaterne, hvor det er relevant, kan oprette reguleringsmæssige sandkasser for cyberrobusthed, og at sådanne reguleringsmæssige sandkasser skal sikre kontrollerede afprøvningsmiljøer for innovative produkter med digitale elementer for at lette deres udvikling, design, validering og afprøvning med henblik på at overholde denne forordning i en begrænset periode, inden de bringes i omsætning. Kommissionen og, hvor det er relevant, ENISA kan yde teknisk støtte og rådgivning samt tilvejebringe værktøjer til oprettelse og drift af reguleringsmæssige sandkasser. De reguleringsmæssige sandkasser oprettes under direkte tilsyn, vejledning og støtte fra markedsovervågningsmyndighederne.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed vil have mulighed for at oprette reguleringsmæssige sandkasser for cyberrobusthed, hvor det vurderes at være relevant. Det bemærkes i den forbindelse, at der på Erhvervsministeriets område er udstedt bekendtgørelse nr. 108 af 15. januar 2026 om nationalt kontaktpunkt for oprettelse af regulatoriske sandkasser og sandkasseforløb i medfør af § 3 i lov om erhvervsfremme.

Det følger derudover af artikel 33, stk. 2, i forordningen om cyberrobusthed, at medlemsstaterne underretter Kommissionen og de øvrige markedsovervågningsmyndigheder om oprettelsen af en reguleringsmæssig sandkasse gennem ADCO.

De reguleringsmæssige sandkasser vil ikke berøre de kompetente myndigheders tilsynsbeføjelser eller korrigerende beføjelser.

I forbindelse med oprettelse af reguleringsmæssige sandkasser, skal der sikres en åben, retfærdig og gennemsigtig adgang hertil, og at navnlig adgangen for mikrovirksomheder og små virksomheder, herunder nyetablerede virksomheder, lettes.

Det foreslås i *stk. 3*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om tiltag, jf. stk. 1, og regulatoriske sandkasser, jf. stk. 2

Det foreslåede har til formål at sikre, at der kan fastsættes supplerende regler om den nærmere udmøntning af de tiltag, der er nævnt i stk. 1, nr. 1-3, eller regulatoriske sandkasse, som nævnt i stk. 2.

Dette kan bl.a. omfatte udpegning af ansvarlige myndigheder, ansøgningsprocesser eller de nærmere kriterier for at blive omfattet.

Til § 11

Forordningen om cyberrobusthed fastsætter i en række bestemmelser underretningspligter, der på forskellige vis indebærer, at medlemsstaternes kompetente myndigheder, skal videregive oplysninger om produkter eller fysiske og juridiske personer til andre medlemsstaters myndigheder eller EU's institutioner, herunder EU-Kommissionen og ENISA.

Dette er bl.a. tilfældet i forhold til underretningsforpligtelserne i henhold til artikel 14-16 for så vidt angår CSIRT'en og reglerne om underretning i forbindelse med bemyndigelse af overensstemmelsesvurderingsorganer og efterfølgende ændringer heraf i forordningens kapitel IV, samt reglerne om markedsovervågningsmyndighedernes underretningspligter i kapitel V.

Det foreslås i § 11, at Styrelsen for Samfundssikkerhed, de myndigheder, der er omhandlet i § 5, stk. 2, og CSIRT'en kan videregive oplysninger til andre myndigheder eller virksomheder, herunder i andre medlemsstater, og til institutioner i Den Europæiske Union for at varetage myndighedsopgaver i medfør af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Det foreslåede vil indebære, at Styrelsen for Samfundssikkerhed vil kunne videregive oplysninger i sin egenskab af både bemyndigende myndighed og markedsovervågningsmyndighed. Det samme vil gælde for de markedsovervågningsmyndigheder, der er omhandlet i § 5, stk. 2, og CSIRT'en som led i varetagelsen af myndighedsopgaver i medfør af forordningen om cyberrobusthed mv., når der opstår behov for at videregive oplysninger til andre relevante nationale myndigheder samt myndigheder i andre EU-medlemsstater eller institutioner i EU.

Det foreslåede vil også muliggøre, at f.eks. markedsovervågningsmyndighederne i relevant omfang og med henblik på effektiv håndhævelse vil kunne videregive oplysninger til de kompetente myndigheder i medfør af NIS 2-loven, ligesom der også vil

kunne ske videregivelse til virksomheder, f.eks. hvis der opstår behov for at varsle om et væsentligt sikkerhedsbrud.

De oplysninger, der vil kunne videregives i medfør af den foreslåede bestemmelse, vil både kunne have karakter af personoplysninger og oplysninger, herunder af teknisk karakter, om f.eks. produkter og virksomheder.

Det foreslåede vil skulle ses i sammenhæng med artikel 63 i forordningen om cyberrobusthed, hvoraf følger, at alle parter, der involveret i anvendelsen af denne forordning, skal overholde tavshedspligten for oplysninger og data, der indhentes under udførelsen af deres opgaver og arbejde, på en sådan måde, at de navnlig beskytter: a) intellektuelle ejendomsrettigheder og fysiske eller juridiske personers fortrolige forretningsoplysninger eller forretningshemmeligheder, herunder kildekode, med undtagelse af de tilfælde, der er omhandlet i artikel 5 i Europa-Parlamentets og Rådets direktiv (EU) 2016/943 om beskyttelse af fortrolig knowhow og fortrolige forretningsoplysninger (forretningshemmeligheder) mod ulovlig erhvervelse, brug og videregivelse, b) den effektive gennemførelse af denne forordning, navnlig for så vidt angår inspektioner, undersøgelser eller kontrolbesøg, c) offentlige og nationale sikkerhedsinteresser og d) strafferetlige eller administrative procedurers integritet.

Det følger derudover af artikel 63, stk. 2, at oplysninger, der udveksles på fortrolig basis mellem markedsovervågningsmyndighederne og mellem markedsovervågningsmyndighederne og Kommissionen, ikke må videregives uden forudgående tilladelse fra den oprindelige markedsmyndighed.

Det følger af artikel 63, stk. 3, at stk. 1 og 2, ikke berører Kommissionens, medlemsstaternes og de bemyndigede organers rettigheder og forpligtelser med hensyn til udveksling af oplysninger og udsendelse af advarsler eller de berørte personers forpligtelse til at afgive oplysninger inden for rammerne af medlemsstaternes strafferet.

Det følger derudover af artikel 63, stk. 4, at Kommissionen og medlemsstaterne kan om nødvendigt udveksle følsomme oplysninger med relevante myndigheder i tredjelande, med hvilke de har indgået bilaterale eller multilaterale aftaler om fortrolighed, der garanterer en tilstrækkelig grad af beskyttelse.

Til § 12

Der er ikke i gældende ret fastsat nærmere regler om kommunikation med de kompetente myndigheder for så vidt angår forhold omfattet af forordningen om cyberrobusthed.

Det følger dog af § 15 i lov om cybersikkerhedscertificering, der udgør et nært beslægtet og sammenligneligt område (producenter og udbydere af informations- og kommunikationsteknologier omfattet af en europæisk cybersikkerhedscertificeringsordning og overensstemmelsesvurderingsorganer), at der i denne sammenhæng er krav om digital kommunikation, jf. stk. 1, mulighed for undtagelse herfra, jf. stk. 2, bestemmelser om fremkomst, jf. stk. 3, og mulighed for at fastsætte nærmere regler herom, jf. stk. 4.

Det foreslås i *stk. 1*, at skriftlig kommunikation til og fra Styrelsen for Samfundssikkerhed, de myndigheder, der er nævnt i § 5, stk. 2, og CSIRT'en om forhold, som er omfattet af forordningen om cyberrobusthed, denne lov eller regler fastsat i medfør heraf, skal foregå digitalt, jf. dog stk. 2.

Den foreslåede bestemmelse vil indebære, at kommunikation mellem de nævnte myndigheder og relevante aktører, herunder fabrikanter af produkter omfattet af forordningen om cyberrobusthed, skal foregå digitalt. Dette vil f.eks. kunne omfatte korrespondance pr. mail eller kommunikation via en anvist selvbetjeningsløsning.

Det bemærkes i den forbindelse, at en digital meddelelse vil skulle anses for at være kommet frem på det tidspunkt, hvor meddelelsen er tilgængelig for adressaten. En meddelelse anses for at være tilgængelig, selvom den pågældende ikke kan skaffe sig adgang til meddelelsen, hvis dette skyldes hindringer, som det er op til den pågældende at overvinde. Dette vil også svare til den tilsvarende ordning i § 15, stk. 3, i lov om cybersikkerhedscertificering.

Det foreslås i *stk. 2, 1. pkt.*, at de myndigheder, der er nævnt i stk. 1, kan undtage en virksomhed fra digital kommunikation, når særlige omstændigheder taler for det.

Det foreslåede vil indebære, at de nævnte myndigheder på baggrund af en konkret vurdering kan træffe afgørelse om at undtage en virksomhed herfra, hvis der f.eks. er tale om, at virksomheden eller den relevante repræsentant er fritaget fra Digital Post, eller at virksomheden har hjemsted i udlandet og dermed ikke har adgang til den nødvendige danske digitale identifikations- eller signaturløsning.

Der kan også være tilfælde, hvor lignende tekniske eller praktiske forhold gør det uforholdsmæssigt vanskeligt at anvende den digitale kommunikationsform. Det samme

kan efter omstændighederne gælde, hvis særlige forhold hos virksomhedens ejer eller ledelse betyder, at digital kommunikation ikke kan varetages, og der ikke er andre, der kan gøre det på virksomhedens vegne.

Det foreslåede skal dog ses i lyset af, at digital kommunikation bør være udgangspunktet, hvorfor det foreslåede vil skulle fortolkes indskrænkende, og at der således udvises tilbageholdenhed med at træffe afgørelse om undtagelse herfra.

Det foreslås i *stk. 2, 2. pkt.*, at en sådan undtagelse dog ikke kan ske for så vidt angår indberetninger efter artikel 14 i forordningen om cyberrobusthed.

Det foreslåede vil indebære, at der ikke kan ske undtagelse efter 1. pkt. for så vidt angår fabrikanternes rapporteringsforpligtelser over for CSIRT'en og ENISA i henhold til artikel 14 i forordningen om cyberrobusthed om enhver aktivt udnyttet sårbarhed i produkter med digitale elementer, som fabrikanten får kendskab til.

Uanset om en virksomhed er blevet undtaget i medfør af 1. pkt., vil det foreslåede 2. pkt. således indebære, at fabrikanten fortsat i medfør af artikel 14 vil skulle underrette om den aktivt udnyttede sårbarhed via den fælles indberetningsplatform, der er oprettet af ENISA i henhold til artikel 16.

Det foreslås i *stk. 3*, at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om digital kommunikation og om anvendelse af bestemte it-systemer og særlige digitale formater og lignende, herunder digital signatur.

Det foreslåede vil indebære, at vedkommende minister efter forhandling med ministeren for samfundssikkerhed og beredskab vil kunne fastsætte nærmere regler om kommunikationsmåden i forbindelse med kommunikation til og fra de relevante markeds- og overvågningsmyndigheder eller CSIRT'en om alle forhold, der er omfattet af forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov eller regler fastsat i medfør heraf.

Det vil i den forbindelse f.eks. kunne gøres obligatorisk for enheder at anvende bestemte internetløsninger, herunder selvbetjeningsløsninger.

Dette skal ses i sammenhæng med, at det på sigt vil kunne komme på tale at udvikle digitale løsninger, herunder selvbetjeningsløsninger til brug for kommunikation om forhold, som er omfattet af forordningen om cybersikkerhed, denne lov eller regler

udstedt i medfør heraf. I den forbindelse vil der således administrativt kunne fastsættes nærmere regler om anvendelsen heraf, herunder hvem der omfattes af pligten til at kommunikere digitalt, om hvilke forhold, og på hvilken måde.

Bestemmelsen forventes bl.a. anvendt til at fastsætte regler om, at ansøgninger om bemyndigelse i henhold til artikel 42 skal indgives skriftligt til Styrelsen for Samfundssikkerhed ved anvendelse af en digital selvbetjeningsløsning, som Styrelsen for Samfundssikkerhed anviser.

Det forudsættes derudover, at den foreslåede bemyndigelse anvendes i overensstemmelse med de til enhver tid gældende regler om den danske nationale eID-løsning og den fællesoffentlige digitale infrastruktur.

Det foreslås i *stk. 4*, at ministeren for samfundssikkerhed og beredskab kan fastsætte nærmere regler om et adgangspunkt for fabrikanters elektroniske underretninger til CSIRT'en.

Den foreslåede bestemmelse vil indebære, at ministeren for samfundssikkerhed og beredskab bemyndiges til at fastsætte et adgangspunkt for fabrikanternes elektroniske underretninger til CSIRT'en i forbindelse med varetagelsen af funktionen som koordinator, f.eks. via virk.dk.

Det foreslåede skal ses i sammenhæng med artikel 14 og 15 i forordningen om cyberrobusthed om henholdsvis fabrikanternes rapporteringsforpligtelser og frivillige indberetninger. For en nærmere gennemgang heraf henvises der til pkt. 2.2.4 i lovforslagets almindelige bemærkninger.

Det foreslåede vil derudover skulle ses i sammenhæng med forordningens artikel 16, stk. 1, hvoraf følger, at ENISA opretter en fælles indberetningsplatform med nationale elektroniske adgangspunkter for underretning. ENISA forvalter endvidere den daglige drift og opretholdelse af den fælles indberetningsplatform.

Det forventes således, at det adgangspunkt, som der kan fastsættes nærmere regler om i medfør af det foreslåede, vil skulle forbindes med den elektroniske underretning via den fælles indberetningsplatform, som ENISA opretter i henhold til forordningens artikel 16.

Til § 13

Det foreslås i § 13, at fabrikanters underretninger i medfør af artikel 14 i forordningen om cyberrobusthed og frivillige indberetninger, som omhandlet i forordningens artikel 15, er undtaget fra aktindsigt efter lov om offentlighed i forvaltningen og partsaktindsigt efter forvaltningsloven.

Det foreslåede vil indebære, at både fabrikanters obligatoriske underretninger om udnyttede sårbarheder mv., jf. artikel 14, samt fabrikanter såvel som andre fysiske eller juridiske personers indberetninger på frivillig basis, jf. artikel 15, til CSIRT'en om en sårbarhed i et produkt med digitale elementer eller om cybertrusler, der kan påvirke risikoprofilen for et sådant produkt, vil være undtaget fra reglerne om aktindsigt.

Det foreslåede skal ses i sammenhæng med, at oplysninger om f.eks. sårbarheder ved fabrikanters produkter, vil kunne skade disse fabrikanters omdømme, hvilket i praksis kan afholde dem fra at underrette CSIRT'en om relevante forhold. Derfor foreslås det, at underretningerne i deres helhed undtages fra aktindsigt, herunder partsaktindsigt efter forvaltningsloven.

Der kan i forlængelse heraf henvises til artikel 15, stk. 5, i forordningen om cyberrobusthed, hvoraf følger, at de CSIRT'er, der er udpeget som koordinatore, såvel som ENISA sikrer fortroligheden og den passende beskyttelse af de oplysninger, der afgives af en fysisk eller juridisk person. Det fremgår derudover af bestemmelsen, at uden at det berører forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger, må frivillig indberetning ikke medføre, at en underrettende fysisk eller juridisk person pålægges nogen yderligere forpligtelser, som vedkommende ikke ville være underlagt, hvis den ikke havde foretaget underretningen.

Undtagelsen fra aktindsigt omfatter derimod ikke fysiske eller juridiske personers adgang til at gøre sig bekendt med oplysninger, der vedrører deres egne forhold, ligesom det vil bero på en konkret vurdering, om der vil kunne ske undtagelse fra udlevering af oplysninger i medfør af lov om aktindsigt i miljøoplysninger, jf. lovbekendtgørelse nr. 980 af 16. august 2017.

Endelig bemærkes det, at det følger af § 8 i lov om Center for Cybersikkerhed, jf. lovbekendtgørelse nr. 836 af 7. august 2019, at Center for Cybersikkerhed er undtaget fra bl.a. lov om offentlighed i forvaltningen, bortset fra lovens § 13, samt forvaltningslovens kapitel 4 om partens aktindsigt. Disse regler vil således supplere de foreslåede regler om undtagelse fra aktindsigt i det omfang, at de finder anvendelse.

Til § 14

Kommissionen har i medfør af en række bestemmelser i forordningen om cyberrobusthed mulighed for at vedtage delegerede retsakter i overensstemmelse med de betingelser, der følger af artikel 61. Derudover kan Kommissionen vedtage en række gennemførelsesretsakter efter undersøgelsesproceduren i artikel 62, stk. 2.

Det foreslås i § 14, at ministeren for samfundssikkerhed og beredskab kan fastsætte regler, som er nødvendige for at gennemføre de af Den Europæiske Union udstedte beslutninger, som træffes med henblik på gennemførelse af forordningen om cyberrobusthed, eller regler, som er nødvendige for at anvende de af Den Europæiske Union udstedte retsakter på forordningens område.

Det foreslåede vil indebære, at ministeren for samfundssikkerhed og beredskab bemyndiges til at fastsætte nødvendige administrative bestemmelser til opfyldelse af gennemførelsesforanstaltninger vedtaget i henhold til forordningen om cyberrobusthed.

Til § 15

Det følger af artikel 48 i forordning om cyberrobusthed, at medlemsstaterne skal sikre, at der findes en procedure for klager over de bemyndigede organers afgørelser.

Det foreslås i *stk. 1*, at Styrelsen for Samfundssikkerhed behandler klager over afgørelser truffet af bemyndigede overensstemmelsesvurderingsorganer og DANAK i henhold til forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Den foreslåede bestemmelse vil indebære, at der indføres en mulighed for at klage til Styrelsen for Samfundssikkerhed over afgørelser, der er truffet af et bemyndiget overensstemmelsesorgan, i det omfang, at klagen vedrører forhold, som er reguleret i forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf. Tilsvarende vil gælde afgørelser, som DANAK måtte træffe som led i den vurdering og overvågning, der er omhandlet i det foreslåede § 4 i det omfang, at Styrelsen for Samfundssikkerhed er ansvarlig herfor.

Det foreslåede vil gælde uanset, om der måtte være tale om en afgørelse i forvaltningslovens forstand, da det afgørende er, om der er tale om forhold, som er reguleret i forordningen om cyberrobusthed, og kan f.eks. også være mere generelle klager over

det bemyndigede organs virke, herunder behandling af en sag, eller DANAK's vurderinger.

Vedrører klagen højrisiko AI-systemer, der er klassificeret som sådanne i medfør af artikel 6 i forordningen om kunstig intelligens, vil disse også skulle behandles af Styrelsen for Samfundssikkerhed henset til, at funktionen som bemyndigende myndighed i medfør af det foreslåede § 3 vil have tværgående karakter. De kompetente myndigheder for så vidt angår højrisiko AI-systemer samarbejder dog i disse tilfælde med Styrelsen for Samfundssikkerhed, herunder gennem faglig bistand.

Det foreslås i *stk. 2*, at klager efter *stk. 1* skal indgives skriftligt til Styrelsen for Samfundssikkerhed. Klagen skal være modtaget senest 4 uger fra tidspunktet, hvor afgørelsen er meddelt. Udløber klagefristen på en lørdag, søndag eller helligdag, udskydes udløbet af fristen til den følgende hverdag. Klagen afvises, hvis den ikke indgives i overensstemmelse hermed, jf. dog *stk. 3*.

Det foreslåede vil indebære, at klager over afgørelser truffet af bemyndigede overensstemmelsesvurderingsorganer og DANAK vil skulle indgives skriftligt til Styrelsen for Samfundssikkerhed senest 4 uger fra det tidspunkt, hvor afgørelsen er meddelt. Klagefristen vil således løbe fra det tidspunkt, hvor afgørelsen kom frem til adressaten, og det dermed var muligt at gøre sig bekendt med indholdet heraf.

Det foreslåede vil derudover indebære, at hvis klagefristen udløber på en lørdag, søndag eller helligdag, udskydes udløbet af fristen til den følgende hverdag, og at klagen afvises, hvis den ikke indgives i overensstemmelse med de nævnte betingelser. Dette vil f.eks. være tilfældet, hvor klagen ikke indgives skriftligt eller først indgives efter udløbet af klagefristen, medmindre det foreslåede *stk. 3* finder anvendelse.

Det foreslås i *stk. 3*, at de relevante myndigheder kan se bort fra en fristoverskridelse, eller at klagen i øvrigt ikke er indgivet i overensstemmelse med *stk. 2*, hvis særlige omstændigheder taler herfor.

Det foreslåede vil indebære, at der kan ses bort fra den manglende overholdelse af kravene i *stk. 2*, hvis det vurderes, at der foreligger særlige omstændigheder. Dette vil f.eks. kunne være hindringer for at indgive klagen som følge af netværksnedbrud, strømafbrydelse eller lignende.

Det foreslås i *stk. 4*, at de relevante myndigheder i forbindelse med behandling af en klage kan indhente alle oplysninger, der er nødvendige for behandling af klagen, fra

erhvervsdrivende omfattet af loven, det nationale akkrediteringsorgan, bemyndigede overensstemmelsesvurderingsorganer og andre myndigheder, der træffer afgørelse efter forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

Det foreslåede vil indebære, at de relevante myndigheder i forbindelse med behandling af en klage kan indhente alle oplysninger, der er nødvendige for behandlingen heraf, herunder oplysninger om produkter og fabrikanter mv., uanset at der også måtte indgå personoplysninger i materialet.

Der henvises til pkt. 3.4 i lovforslagets almindelige bemærkninger.

Til § 16

Det foreslås i § 16, at afgørelser truffet af Styrelsen for Samfundssikkerhed eller de myndigheder, der er omtalt i § 5, stk. 2, efter forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf ikke kan indbringes for anden administrativ myndighed.

Den foreslåede bestemmelse vil bl.a. indebære, at Styrelsen for Samfundssikkerheds afgørelser efter forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf ikke kan påklages til Ministeriet for Samfundssikkerhed og Beredskab eller andre administrative myndigheder. Dette gælder uanset, om der er tale om en afgørelse, der er truffet i styrelsens egenskab af bemyndigende myndighed eller markeds-
overvågningsmyndighed.

Sådanne afgørelser vil i stedet kunne indbringes for domstolene efter grundlovens § 63, ligesom Styrelsen for Samfundssikkerhed også vil være omfattet af Folketingets Ombudsmands generelle kompetence.

Dette skal ses i sammenhæng med, at opgaven som henholdsvis bemyndigende myndighed og markedsovervågningsmyndighed kræver en ikke ubetydelig og faglig indsigt i området, der som udgangspunkt vurderes alene at foreligge hos disse myndigheder, herunder Styrelsen for Samfundssikkerhed.

Der henvises i øvrigt til pkt. 3.4 i lovforslagets almindelige bemærkninger.

Til § 17

Det følger af artikel 64, stk. 1, i forordning om cyberrobusthed, at medlemsstaterne skal fastsætte regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af

bestemmelserne i forordningen, samt skal træffe alle nødvendige foranstaltninger for at sikre, at de anvendes.

Det foreslås i *stk. 1*, at medmindre højere straf er forskyldt efter anden lovgivning, straffes med bøde den, der begår en overtrædelse som nævnt i nr. 1-3. Dette vil således omfatte de erhvervsdrivende, der er omfattet af de pågældende bestemmelser i forordningen, herunder fabrikanter, importører og distributører.

Det foreslås i *nr. 1*, at den, der undlader at overholde de væsentlige cybersikkerhedskrav, der følger af bilag I i forordningen om cyberrobusthed, eller fabrikanternes forpligtelser i henhold til forordningens artikel 13 eller underretningsforpligtelser i henhold til artikel 14, straffes med bøde.

Det foreslåede vil indebære, at der kan idømmes bødestraf for overtrædelse af forordningens bestemmelser om overholdelse af de væsentlige cybersikkerhedskrav i bilag I om produkternes egenskaber (del I) samt fabrikanternes håndtering af sårbarheder (del II), og fabrikanternes øvrige forpligtelser efter artikel 13, herunder at foretage en vurdering af produktets cybersikkerhedsrisici og tage dette i betragtning samt at overholde de nærmere angivne oplysningskrav. Derudover vil fabrikanter kunne idømmes bødestraf for manglende underretning efter artikel 14 vedrørende visse sårbarheder i de omfattede produkter, herunder af CSIRT'en, ENISA og de berørte brugere.

Det foreslåede vil skulle ses i sammenhæng med forordningens artikel 64, stk. 2, hvorefter følger, at bødeniveauet for overtrædelse af disse bestemmelser er op til 15.000.000 euro eller, hvis lovovertræderen er en virksomhed, op til 2,5 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det foreslås i *nr. 2*, at den, der undlader at overholde forpligtelserne i forordningens artikel 18-23, artikel 28, artikel 30, stk. 1-4, artikel 31, stk. 1-4, artikel 32, stk. 1, 2 og 3, artikel 33, stk. 5, og artikel 39, 41, 47, 49 og 53, straffes med bøde.

Det foreslåede vil indebære, at der kan idømmes bødestraf for manglende opfyldelse af forpligtelserne for bemyndigede repræsentanter, importører, distributører, personer der foretager væsentlige ændringer (artikel 18-22), manglende identifikation, jf. artikel 23, samt kravet om at udfærdige overensstemmelseserklæringer, jf. artikel 28, anbringelse af CE-mærkning, jf. artikel 30, stk. 1-4, kravene til teknisk dokumentation, jf. artikel 31, stk. 1-4, foretagelse af overensstemmelsesvurderinger, jf. artikel 31, stk. 1-3, de særlige krav til mikrovirksomheders dokumentation, jf. artikel 33, stk. 5, kravene

til de bemyndigede organer, jf. artikel 39, herunder dattervirksomheder og underleverandører, jf. artikel 41, bemyndigede organers operationelle forpligtelser og oplysningspligt, jf. artikel 47 og 49, og manglende tildeling af adgang til oplysninger og dokumentation over for markedsovervågningsmyndigheder, jf. artikel 53.

Det foreslåede vil skulle ses i sammenhæng med forordningens artikel 64, stk. 3, hvoraf følger, at bødeniveauet for overtrædelse af disse bestemmelser er op til 10.000.000 euro eller, hvis lovovertræderen er en virksomhed, op til 2 % af dens samlede globale årsomsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det foreslås derudover i *nr. 3*, at den, der afgiver ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning, også kan straffes med bøde.

Det foreslåede vil indebære, at afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger til bemyndigede organer og markedsovervågningsmyndigheder som svar på en anmodning vil kunne straffes med bøde.

Det foreslåede vil skulle ses i sammenhæng med forordningens artikel 64, stk. 4, hvoraf følger, at bødeniveauet for overtrædelse af disse bestemmelser er op til 5.000.000 euro eller, hvis lovovertræderen er en virksomhed, op til 1 % af dens samlede globale årlige omsætning i det foregående regnskabsår, alt efter hvilket beløb der er størst.

Det bemærkes, at strafudmålingen for de foreslåede overtrædelser, skal ses i lyset af artikel 64, stk. 5, i forordningen om cyberrobusthed, hvoraf følger, at ved fastsættelsen af bødens størrelse, tages der i hvert enkelt tilfælde hensyn til alle relevante omstændigheder i den specifikke situation, og der tages behørigt hensyn til a) overtrædelsens art, grovhed og varighed samt dens konsekvenser, b) hvorvidt de samme eller andre markedsovervågningsmyndigheder allerede har pålagt den samme erhvervsdrivende administrative bøder for en lignende overtrædelse og c) størrelsen på, navnlig med hensyn til mikrovirksomheder og små og mellemstore virksomheder, herunder nyetablerede virksomheder, og markedsandelen for den erhvervsdrivende, der har begået overtrædelsen. Straffelovens § 51, stk. 3, og 10. kapitel om straffens fastsættelse finder i øvrigt anvendelse.

Fastsættelsen af straffen vil dog fortsat bero på domstolenes konkrete vurdering i det enkelte tilfælde af samtlige omstændigheder i sagen under hensyntagen til bl.a.

skærpende eller formildende omstændigheder, jf. herved de almindelige regler om straffens fastsættelse i straffelovens kapitel 10.

Det foreslåede om, at højere straf kan være forskyldt efter anden lovgivning, har til formål at sikre, at handlinger, der tillige indebærer en overtrædelse af bestemmelser, der kan medføre højere straf, kan henføres under sådanne bestemmelser. Hvis det strafbare forhold eksempelvis omfattes af straffelovens §§ 162 og 163 om afgivelse af urigtige oplysninger til offentlige myndigheder, henhører forholdet således under den bestemmelse, hvorefter den højeste straf er forskyldt.

Det foreslås i *stk. 2*, at *stk. 1* ikke finder anvendelse i de tilfælde, der er nævnt i det foreslåede nr. 1 og 2.

Det følger af det foreslåede *nr. 1*, at de foreslåede regler om straf i *stk. 1* ikke finder anvendelse for fabrikanters manglende overholdelse af den frist, som er omhandlet i forordningen om cyberrobustheds artikel 14, *stk. 2*, litra a, og *stk. 4*, litra a, når disse fabrikanter betragtes som mikrovirksomheder eller små virksomheder.

Det følger derudover af det foreslåede *nr. 2*, at de foreslåede regler om straf i *stk. 1* ikke finder anvendelse for enhver overtrædelse af forordningen om cyberrobusthed begået af open source software-forvaltere.

De foreslåede undtagelser skal ses i sammenhæng med artikel 64, *stk. 10*, i forordningen om cyberrobusthed, hvoraf følger, at uanset artikel 64, *stk. 3-9*, finder de administrative bøder, der er omhandlet i disse stykker, ikke anvendelse på følgende: a) fabrikanter, der betragtes som mikrovirksomheder eller små virksomheder for så vidt angår manglende overholdelse af den frist, som er omhandlet i artikel 14, *stk. 2*, litra a, eller artikel 14, *stk. 4*, litra a, og b) enhver overtrædelse af denne forordning begået af open source software-forvaltere.

Der kan derudover henvises til præambelbetragtning nr. 5 i forordningen om cyberrobusthed, hvoraf følger, at for så vidt angår mikrovirksomheder og små og mellemstore virksomheder bør bestemmelserne i bilaget til Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder anvendes i deres helhed ved fastlæggelsen af, hvilken kategori en virksomhed falder ind under. Ved beregningen af antal beskæftigede og finansielle tærskler til afgrænsning af virksomhedskategorierne, bør bestemmelserne i artikel 6 i bilaget til henstillingen om fastsættelse af oplysninger om virksomheden under

hensyntagen til specifikke typer virksomheder, f.eks. partnervirksomheder eller tilknyttede virksomheder, derfor også finde anvendelse.

Det foreslås i *stk. 3*, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Det foreslåede vil indebære, at der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel for overtrædelse af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf.

For så vidt angår offentlige myndigheder bemærkes det, at det fremgår af artikel 64, stk. 7, i forordningen om cyberrobusthed, at hver medlemsstat fastsætter regler om, i hvilket omfang administrative bøder kan pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat.

Det foreslås i den forbindelse, at undlade at regulere dette særskilt, hvilket vil indebære, at udgangspunktet i straffelovens § 27, stk. 2, vil udgøre den forudsatte regulering således, at statslige myndigheder og kommuner alene kan straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private. Offentlige myndigheder kan således alene ifalde strafansvar efter reglerne i straffelovens kapitel 5, i det omfang myndigheden optræder på en måde, der kan sammenlignes med virksomhed, der udøves af en privatperson eller af et selskab, herunder i egenskab af driftsherre.

Reglerne i straffelovens kapitel 5 omfatter derimod ikke lovovertrædelser, der begås som led i myndighedsudøvelse. I sådanne tilfælde kan der alene blive tale om personligt strafansvar for de ansvarlige enkeltpersoner.

Det foreslås i *stk. 4*, at i forskrifter, der udstedes i medfør af loven, kan der fastsættes straf af bøde for overtrædelse af bestemmelser i forskrifterne.

Det foreslås i *stk. 5*, at forældelsesfristen for overtrædelse af forordningen om cyberrobusthed, denne lov, eller regler udstedt i medfør heraf er 5 år.

Af straffelovens § 93, stk. 1, følger de almindelige forældelsesfrister for strafbare lovovertrædelser, der skal beregnes efter det strafmaksimum, der er foreskrevet for lovovertrædelsen. Det er således strafferammen for den pågældende lovovertrædelse og ikke den konkrete forskyldte straf, som er afgørende for beregningen af

forældelsesfristen. Forældelsesfristen er efter straffelovens § 93, stk. 1, nr. 1, 2 år, når der ikke er hjemlet højere straf end fængsel i 1 år for overtrædelsen.

Den foreslåede bestemmelse vil indebære, at forældelsesfristen for overtrædelse af forordningen om cyberrobusthed, denne lov eller regler udstedt i medfør heraf fastsættes til 5 år under hensyntagen til, at de omfattede straffesager kan antage en vis størrelse og kompleksitet.

Det bemærkes, at artikel 64 om sanktioner i forordningen om cyberrobusthed finder anvendelse fra den 11. december 2027. Den foreslåede straffebestemmelse foreslås derfor tilsvarende først at træde i kraft den 11. december 2027, jf. det foreslåede § 25, stk. 2.

Der henvises i øvrigt til pkt. 3.4 i lovforslagets almindelige bemærkninger.

Til § 18

Det fremgår af artikel 71, stk. 2, at forordningen finder anvendelse fra den 11. december 2027. Artikel 14 finder dog anvendelse fra den 11. september 2026, og kapitel IV (artikel 35 til 51) finder anvendelse fra den 11. juni 2026.

Det foreslås i *stk. 1*, at loven træder i kraft den 1. marts 2027, jf. dog *stk. 2*.

Det foreslåedes vil indebære, at loven træder i kraft den 1. januar 2027 med undtagelse af de bestemmelser, der er nævnt i *stk. 2*.

Ikrafttrædelsestidspunktet vil betyde, at fastsættelsen af de supplerende bestemmelser for så vidt angår forordningens kap. IV vil ske med en vis forsinkelse i forhold til anvendelsestidspunktet.

Det foreslåede skal ses i sammen med overgangsbestemmelserne i forordningen om cyberrobustheds artikel 69.

Det følger af artikel 69, stk. 1, at udstedte EU-typeafprøvningsattester og afgørelser om godkendelse vedrørende cybersikkerhedskrav til produkter med digitale elementer, der er omfattet af anden EU-harmoniseringslovgivning end forordningen om cyberrobusthed, forbliver gyldige indtil den 11. juni 2028, medmindre de udløber inden denne dato, eller medmindre andet er angivet i sådan anden EU-harmoniseringslovgivning, i hvilket tilfælde de forbliver gyldige som omhandlet i den pågældende lovgivning.

Det følger derudover af artikel 69, stk. 2, at produkter med digitale elementer, der er bragt i omsætning inden den 11. december 2027, kun er omfattet af kravene i forordningen om cyberrobusthed, hvis disse produkter fra denne dato er genstand for væsentlige ændringer.

Afslutningsvis følger det af artikel 69, stk. 3, at uanset artikel 69, stk. 2, finder de forpligtelser, der er fastsat i artikel 14 om fabrikanternes rapporteringsforpligtelser, anvendelse på alle produkter med digitale elementer, der er omfattet af forordningen om cyberrobustheds anvendelsesområde, og som er bragt i omsætning inden den 11. december 2027.

Det foreslås i *stk. 2*, at §§ 5-11 og 17 træder i kraft den 11. december 2027.

Det foreslåede vil således indebære, at udpegningen af markedsovervågningsmyndigheder i medfør af det foreslåede § 6 og de hertil knyttede bestemmelser i §§ 7-11 samt den foreslåede straffebestemmelse i § 17 først vil træde i kraft den 11. december 2027.

Det udskudte ikrafttrædelsestidspunkt skal ses i lyset af, at de pågældende bestemmelser i forordningen om cyberrobusthed først finder anvendelse fra denne dato.

Til § 19

Det foreslås i § 19, at loven ikke skal gælde for Færøerne og Grønland.

Det foreslåede vil indebære, at loven ikke vil gælde for Færøerne og Grønland og heller ikke vil kunne sættes i kraft for Færøerne og Grønland.

Dette skal ses i sammenhæng med, at forordningen om cyberrobusthed ikke finder anvendelse for Færøerne og Grønland. Hvis bestemmelser svarende til forordningen om cyberrobusthed skal gennemføres for Færøerne og Grønland, vil det skulle ske ved lov. Da det foreslåede er en supplerende lov til forordningen findes det mest hensigtsmæssigt, at de supplerende bestemmelser i så fald sættes i kraft ved lov sammen med forordningen.