UDKAST

Forslag

til

Lov om supplerende bestemmelser til forordningen om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/313 (lov om certificering af cybersikkerhed)[1]

Kapitel 1
Anvendelsesområde

§ 1. Loven supplerer Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed), jf. bilag 1 til denne lov.

§ 2. Loven gælder for producenter og udbydere af IKT-produkter, -tjenester og -processer, som er omfattet af en europæisk cybersikkerhedscertificeringsordning, og for overensstemmelsesvurderingsorganer og andre certifikatudstedende organer.

Kapitel 2
Den nationale cybersikkerhedscertificeringsmyndighed

§ 3. Sikkerhedsstyrelsen udpeges som national cybersikkerhedscertificeringsmyndighed, jf. artikel 58, stk. 1, i forordningen om cybersikkerhed.

Kapitel 3
Overensstemmelsesvurderingsorganer

§ 4. DANAK akkrediterer overensstemmelsesvurderingsorganer efter artikel 60, stk. 1, i forordningen om cybersikkerhed, hvis organet opfylder kravene i bilaget til forordningen.

---

[1] Som bilag til loven er medtaget Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed), EU-Tidende 2019, nr. L 151, s. 15. Ifølge artikel 288 i EUF-traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af forordningen i lovens bilag er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

§ 5. Sikkerhedsstyrelsen kan bemyndige overensstemmelsesvurderingsorganer efter artikel 60, stk. 3, i forordningen om cybersikkerhed til at udføre opgaver i henhold til en europæisk cybersikkerhedscertificeringsordning, hvis der i den pågældende ordning er fastsat specifikke eller yderligere krav end dem, der følger af artikel 54, stk. 1, litra f, i forordningen om cybersikkerhed.

Stk.2. Konstaterer Sikkerhedsstyrelsen, at et overensstemmelsesvurderingsorgan overtræder de specifikke eller yderlige krav, som er nævnt i stk. 1, kan Sikkerhedsstyrelsen begrænse eller suspendere bemyndigelsen og fastsætte en rimelig tidsfrist for afhjælpning af de konstaterede overtrædelser.

Stk. 3. Sikkerhedsstyrelsen kan tilbagekalde bemyndigelsen efter stk. 1, hvis

1) forudsætningerne for bemyndigelsen efter stk. 1 ikke længere er opfyldt,
2) overensstemmelsesvurderingsorganet ikke afhjælper de konstaterede overtrædelser inden for den fastsatte frist i stk. 2, eller
3) overensstemmelsesvurderingsorganet gentagne gange eller ved grov forsømmelse overtræder de specifikke eller yderligere krav, som er nævnt i stk. 1.

§ 6. Erhvervsministeren kan fastsætte regler om udpegning af et certificeringsorgan under Sikkerhedsstyrelsen efter artikel 60, stk. 2, jf. artikel 56, stk. 5, litra a, og artikel 56, stk. 6, litra a, i forordningen om cybersikkerhed.

§ 7. Sikkerhedsstyrelsen kan delegere sin kompetence til at udstede europæiske cybersikkerhedsattester efter artikel 56, stk. 6, litra b, i forordningen om cybersikkerhed til et overensstemmelsesvurderingsorgan.

Stk. 2. Erhvervsministeren kan fastsætte nærmere regler om udførelsen af den opgave, som Sikkerhedsstyrelsen kan delegere til et overensstemmelsesvurderingsorgan efter artikel 56, stk. 6, litra b, i forordningen om cybersikkerhed, jf. stk. 1.

§ 8. Erhvervsministeren kan fastsætte regler om udpegning af en udenlandsk cybersikkerhedscertificeringsmyndighed, et udenlandsk offentligt organ eller et andet overensstemmelsesvurderingsorgan til at varetage opgaver i henhold til artikel 56, stk. 5 og 6, i forordningen om cybersikkerhed.

Kapitel 4
Kontrol

§ 9. Sikkerhedsstyrelsen påser og håndhæver overholdelsen af forordningen om cybersikkerhed og regler fastsat i medfør af forordningen. Sikkerhedsstyrelsen påser og håndhæver endvidere overholdelsen af denne lov og regler fastsat i medfør af denne lov.

§ 10. Sikkerhedsstyrelsen kan fra enhver kræve alle oplysninger, som er nødvendige for udførelsen af opgaven som national cybersikkerhedscertificeringsmyndighed, herunder til afgørelse af, om et forhold falder ind under bestemmelserne i forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov og regler fastsat i medfør af denne lov.

§ 11. Sikkerhedsstyrelsen kan udtage ethvert IKT-produkt, -tjeneste eller -proces, som er omfattet af en europæisk cybersikkerhedscertificeringsordning i medfør af forordningen om cybersikkerhed, med henblik på at lave en teknisk undersøgelse.

Stk. 2. Sikkerhedsstyrelsen har adgang til direkte rådgivning og anden bistand fra Center for Cybersikkerhed om sikkerhedsmæssige spørgsmål.

§ 12. Sikkerhedsstyrelsen kan auditere overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer med henblik på at verificere overholdelse af forordningen om cybersikkerhed og regler fastsat i medfør af forordningen.

§ 13. Sikkerhedsstyrelsen har til enhver tid mod behørig legitimation og uden retskendelse adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller indehavere af en europæisk cybersikkerhedsattest med henblik på at føre kontrol efter dette kapitel.

Stk. 2. Sikkerhedsstyrelsen kan være bistået af en eller flere uafhængige sagkyndige i forbindelse med adgangen efter stk. 1.

§ 14. Sikkerhedsstyrelsen kan udstede påbud til en indehaver af en europæisk cybersikkerhedsattest eller en udsteder af en EU-overensstemmelseserklæring, der har bragt en eller et IKT-produkt, -tjeneste eller -proces i omsætning, som ikke er i overensstemmelse med forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov og regler fastsat i medfør af denne lov, om at

1) gøre brugerne opmærksomme på risici,
2) standse markedsføring, der kan vildlede brugerne,
3) afhjælpe forhold, som ikke er i overensstemmelse med reglerne eller
4) standse salg, levering eller udbud af produktet, tjenesten eller processen.

§ 15. Sikkerhedsstyrelsen kan tilbagekalde en europæisk cybersikkerhedsattest, hvis indehaveren af en attest
1) ikke imødekommer Sikkerhedsstyrelsens anmodning om oplysninger, jf. § 10,
2) nægter at give Sikkerhedsstyrelsen adgang, jf. § 13,
3) ikke efterkommer et påbud fra Sikkerhedsstyrelsen, jf. § 14, eller
4) gentagne gange eller ved grov forsømmelse overtræder forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov eller regler fastsat i medfør af denne lov.

Kapitel 5
Klageadgang

§ 16. Sikkerhedsstyrelsen behandler klager over afgørelser vedrørende
1) EU-overensstemmelseserklæringer udstedt af producenter og udbydere af IKT-produkter, -tjenester og -processer i henhold til artikel 53 i forordningen om cybersikkerhed,
2) europæiske cybersikkerhedsattester udstedt af Sikkerhedsstyrelsen efter artikel 56, stk. 5, litra a, eller
3) europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med artikel 56, stk. 6, i forordningen om cybersikkerhed.

§ 17. Sikkerhedsstyrelsens afgørelser i egenskab af national cybersikkerhedscertificeringsmyndighed kan ikke indbringes for anden administrativ myndighed.

Kapitel 6
Kommunikation

§ 18. Skriftlig kommunikation til og fra Sikkerhedsstyrelsen om forhold, som er omfattet af forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov og regler fastsat i medfør af denne lov, skal foregå digitalt.

Stk. 2. Uanset stk. 1 kan Sikkerhedsstyrelsen bestemme, at skriftlig kommunikation skal foregå på anden vis, hvis det er påkrævet efter omstændighederne.

Stk. 3. Erhvervsministeren kan fastsætte nærmere regler om digital kommunikation og om anvendelse af bestemte it-systemer, særlige digitale formater eller lignende.

Stk. 4. En digital meddelelse anses for at være kommet frem på det tidspunkt, hvor meddelelsen er tilgængelig for adressaten i postløsningen.

Kapitel 7
Afsluttende bestemmelser

§ 19. Erhvervsministeren 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 cybersikkerhed, eller regler, som er nødvendige for at anvende de af Den Europæiske Union udstede retsakter på forordningens område.

§ 20. Loven træder i kraft den 28. juni 2021.

§ 21. Loven gælder ikke for Færøerne og Grønland.

Bemærkninger til lovforslaget
Almindelige bemærkninger

Indholdsfortegnelse

1. Indledning

Lovforslaget har til hensigt at bringe dansk ret i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 881/2019 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed). Forordningen har som overordnet formål at højne cybersikkerheden på det fælleseuropæiske marked i den fortsatte digitale udvikling af samfundet.

Forordningen om cybersikkerhed trådte i kraft den 27. juni 2019 og indfører bl.a. en fælles europæisk ramme for certificering af informations- og kommunikationsteknologier (”IKT”) – nærmere bestemt IKT-produkter, -tjenester og -processer. Flere bestemmelser i forordningen kræver, at der foretages visse gennemførelsesforanstaltninger for medlemsstaterne i relation til cybersikkerhedscertificering, herunder at der udpeges en national myndighed for certificering af cybersikkerhed. Disse bestemmelser finder først anvendelse fra den 28. juni 2021, hvorfor lovforslaget bør træde i kraft i overensstemmelse hermed.

Forordningen om cybersikkerhed har direkte virkning i Danmark, hvilket betyder, at der som udgangspunkt ikke må være anden dansk lovgivning, der regulerer cybersikkerhedscertificeringsordninger, i det omfang dette er reguleret i forordningen.

Danmark er således forpligtet til at indrette dansk lovgivning i overensstemmelse med forordningens bestemmelser med virkning fra den 28. juni 2021.

2. Lovforslagets baggrund

Hver gang data lagres, transmitteres og behandles elektronisk, er der en potentiel risiko for at tilgængeligheden, integriteten og fortroligheden kompromitteres. Brud på cybersikkerheden forårsager hvert år økonomisk skade på europæiske virksomheder og økonomien som helhed. Tyveri af forretningshemmeligheder, personoplysninger, forstyrrelse af tjenester og infrastrukturer undergraver borgernes grundlæggende rettigheder og svækker tilliden til brug af den teknologi som gør det muligt at få adgang til, redigere, overføre og gemme information (net- og informationsteknologi).

Området omkring certificering af cybersikkerhed har ikke tidligere været reguleret i hverken Danmark eller EU. Som en konsekvens heraf er der kun i nogle få medlemsstater effektive cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester og -processer. En virksomhed, der opererer på flere markeder inden for EU, risikerer i dag at skulle gennemgå flere certificeringsprocedurer i forskellige medlemsstater for at kunne tilbyde sit produkt.

I mangel af en harmoniseringslovgivning er der i dag forskelle i de standarder, som medlemsstaterne opretter. Det vil sige, at de tekniske og organisatoriske krav, testmetoder og certificeringsprocedurer for cybersikkerhed er divergerende og forhindrer et sammenhængende digitalt indre marked. I

værste fald kan et IKT-produkt, -tjeneste eller -proces, der opfylder cybersikkerhedskravene i én medlemsstat, ikke markedsføres i en anden. Som en konsekvens heraf kan en virksomhed i dag risikere at skulle gennemgå flere certificeringsprocedurer i forskellige medlemsstater for at kunne tilbyde et produkt på flere markeder. Som et eksempel fra kapitel 1 i forslaget til forordningen om cybersikkerhed fra 2017 følger det, at en producent af en elektronisk, trådløs enhed til fjernaflæsning (smart meter), der ønsker at sælge sit produkt i tre medlemsstater, f.eks. Tyskland, Frankrig og England, i øjeblikket skal overholde tre forskellige certificeringsordninger, herunder kommerciel produktassurance (CPA) i Storbritannien, Certification de Sécurité de Premier Niveau i Frankrig (CSPN) og en specifik beskyttelsesprofil baseret på fælles kriterier i Tyskland. Det medfører høje udgifter og administrative byrder for de pågældende virksomheder, og at det indre marked splittes op.

Som reaktion på udfordringerne med cybersikkerhed er der i EU i de senere år vedtaget forskellige retsakter for at styrke cybersikkerhedsniveauet. I 2013 blev Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) oprettet. Agenturet rådgiver og bistår Unionens institutioner om cybersikkerhed og videreføres ved vedtagelsen af forordningen, men med nyt mandat. ENISA skal – udover som hidtil at støtte de europæiske institutioner, medlemsstaterne og erhvervslivet i adressering, reaktion og især forhindring af problemer med net- og informationssikkerheden – også samle og fremme arbejdet med cybersikkerhedscertificering på EU-plan.

I 2019 blev forordningen om cybersikkerhed vedtaget. Forordningen har to overordnede formål: På den ene side skal mål, opgaver og organisatoriske forhold for fastlægges for ENISA (forordningens afsnit II), og på den anden side skal der etableresen ramme for europæisk cybersikkerhedscertificering (forordningens afsnit III). Samtlige bestemmelser i forordningens afsnit II vedrørende ENISA er allerede trådt i kraft. Med lovforslaget fastsættes der således alene bestemmelser vedrørende certificering af cybersikkerhed.

Cybersikkerhedscertificering af IKT-produkter, -tjenester og -processer. skal derfor være med til at nedbryde handelshindringer i EU og sikre den nødvendige tiltro til informations- og kommunikationsteknologien i europæisk regi. Producenter og udbydere af IKT-produkter, -tjenester og -processer, jf. artikel 2, stk. 1, nr. 12-14, får mulighed for at certificere produkter, tjenester og processer og derved attestere, at visse nærmere angivne sikkerhedskrav overholdes. Dette gælder f.eks. beskyttelsen af data mod utilsigtet

eller uautoriseret brug og genetablering af tilgængelighed i tilfælde af fysiske eller tekniske hændelser.

Certificering garanterer ikke i sig selv, at IKT-produktet, -tjenesten eller -processen er cybersikker. Der er i højere grad tale om, at procedurer og tekniske metoder omkring produktet, tjenesten eller processen er evalueret og fundet tilfredsstillende. Virksomhederne får samtidig en konkurrencefordel ved at kunne markedsføre et certificeret produkt, tjeneste eller proces, og kunder og brugere kan få præcise oplysninger om, hvilket tillidsniveau det pågældende produkt, tjeneste eller proces er certificeret på.

Certificering spiller en vigtig rolle for styrkelsen af tilliden til produkter, tjenester og processer, men kan samtidigt være omkostningskrævende. Anvendelsen af certificering af cybersikkerhed er ifølge artikel 56, stk. 2, som hovedregel frivillig. Dette skyldes, at behovet for certificering kan variere i forhold til både det enkelte produkt, tjeneste og proces, den specifikke brug heraf og ikke mindst den hurtige teknologiske forandring.

En fælleseuropæisk, harmoniseret certificeringsordning er gyldig og anerkendt i alle medlemsstater og indfører en mulighed for "one-stop-shop" for virksomheder, som ønsker at få deres produkt, tjeneste eller proces certificeret. Virksomhederne kan via certificering opnå en cybersikkerhedsattest, der bekræfter overensstemmelsen med en europæisk certificeringsordning, og som er gyldig i alle medlemsstater. Virksomhederne vil derved kunne reducere omkostninger til forskellige nationale og internationale certificeringsordninger og derved få lettere adgang til at operere grænseoverskridende på det indre marked.

Certificering er en formel dokumentation for evaluering af produkter, tjenester og processer. Evalueringen foretages af et uafhængigt og akkrediteret overensstemmelsesvurderingsorgan med baggrund i et defineret sæt af kriterier. Organet udsteder et certifikat, der angiver, at IKT-produkter, -tjenester og -processer overholder specificerede krav til cybersikkerhed.

Forordningen om cybersikkerhed giver i visse tilfælde mulighed for selvvurdering af overensstemmelse. Selvvurdering vil kun være muligt for IKT-produkter, -tjenester eller -processer med lav risiko, der svarer til tillidsniveauet grundlæggende. En europæisk cybersikkerhedscertificeringsordning kan dermed som et alternativ til certificering tillade, at producenter eller udbydere af IKT-produkter, -tjenester eller -processer kan udstede en EU-overensstemmelseserklæring, hvoraf det fremgår, at kravene i en relevant

cybersikkerhedscertificeringsordning er opfyldt. Dermed indestår producenten eller udbyderen – og ikke et overensstemmelsesvurderingsorgan – for, at IKT-produktet, -tjenesten eller -processen er i overensstemmelse med den pågældende certificeringsordning.

Der fastsættes ikke med dette lovforslag direkte og operationelle certificeringsordninger, men den formelle organisation af de involverede myndigheder og deres indbyrdes samarbejde lægges fast. Det vil være selve certificeringsordningen, som identificerer de specifikke IKT-produkter, -tjenester og -processer, der er omfattet, og som fastlægger den detaljerede specifikation af kravene til cybersikkerhed, herunder relevante standarder og tekniske specifikationer, de specifikke evalueringskriterier og testmetoder samt niveauet af sikkerhed, jf. forordningens artikel 54.

De europæiske certificeringsordninger for cybersikkerhed udarbejdes af ENISA i samarbejde med interessenter og den europæiske cybersikkerhedscertificeringsgruppe (ECCG), hvor Danmark er repræsenteret ved Center for Cybersikkerhed og Erhvervsstyrelsen. Ordningerne vedtages endeligt af Kommissionen i form af gennemførelsesretsakter efter fremgangsmåden i forordningens artikel 49.

3. Lovforslagets hovedpunkter

3.1. Gældende ret

Der findes i dag ikke nationale regler om cybersikkerhedscertificering i Danmark. Med lovforslaget fastsættes derfor bestemmelser vedrørende et hidtil ulovreguleret område.

I EU er der med fastsættelsen af bestemmelser om en fælleseuropæisk cybersikkerhedscertificeringsramme også tale om ny regulering. Forordningen om cybersikkerhed erstatter forordning (EU) nr. 526/2013 om ENISA, som i sin tid erstattede forordning (EF) nr. 460/2004 om oprettelsen af et europæisk agentur for net- og informationssikkerhed. Det er således først med forordningen om cybersikkerhed, at der på EU-niveau fastsættes bestemmelser om cybersikkerhedscertificering.

Uanset den manglende regulering i Danmark og EU er certificering af cybersikkerhed noget, som danske virksomheder og offentlige myndigheder i dag benytter sig af. Det reelle omfang af certificering af cybersikkerhed i Danmark er dog ikke kortlagt.

Derudover er Danmark som stat i visse sammenhænge forpligtet til at behandle information på en nærmere bestemt måde. Det gælder f.eks. hvor Danmark i regi af NATO- eller EU-samarbejdet modtager klassificeret information, og hvor behandlingen heraf f.eks. kan kræve certificering, jf. nærmere Justitsministeriets cirkulære af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.

3.2. Udpegning af Sikkerhedsstyrelsen som national cybersikkerhedscertificeringsmyndighed

3.2.1. Gældende ret

Som anført i pkt. 3.1. findes der ikke gældende regulering af cybersikkerhedscertificering i Danmark. Det forhold, at forordningen om cybersikkerhed er ny, bevirker, at der på nuværende tidspunkt ikke eksisterer gældende ret, som dækker udpegningen af en national cybersikkerhedscertificeringsmyndighed.

3.2.2. Erhvervsministeriets overvejelser og den foreslåede ordning

Det følger af præambelbetragtning nr. 101 i forordningen om cybersikkerhed, at der bør udpeges en eller flere nationale cybersikkerhedscertificeringsmyndigheder, og at der kan være tale om en eksisterende eller ny myndighed. Derudover fremgår en række opgaver af præambelbetragtning nr. 102, som den nationale cybersikkerhedscertificeringsmyndighed bør udføre, herunder overvågning, håndhævelse, bistand til nationale akkrediteringsorganer, klagebehandling og samarbejde med andre myndigheder. Endelig følger det af præambelbetragtning nr. 99, at det er nødvendigt at indføre et peerreviewsystem mellem de nationale cybersikkerhedscertificeringsmyndigheder.

Sikkerhedsstyrelsen udfører i dag en række opgaver, som indholdsmæssigt har ligheder med de opgaver, der skal udføres efter forordningen om cybersikkerhed. Sikkerhedsstyrelsen foretager således i dag bemyndigelse af overensstemmelsesvurderingsorganer inden for f.eks. fyrværkeri og gassikkerhedsområdet, fører tilsyn med certificering inden for bl.a. metrologi- og autorisationsområdet og markedsovervåger produkters CE- og energimærkning. Dette sker bl.a. efter regler i lovbekendtgørelse nr. 2 af 3. januar 2019 om fyrværkeri og andre pyrotekniske artikler, som ændret ved lov nr. 799 af 9. juni 2020, lov nr. 61 af 30. januar 2018 om sikkerhed for gasanlæg og gasinstallationer (gassikkerhedsloven),som senest ændret ved lov nr. 799 af

9. juni 2020, lov nr. 1518 af 18. december 2018 om erhvervsfremme, som senest ændret ved lov nr. 796 af 9. juni 2020, lovbekendtgørelse nr. 30 af 11. januar 2019 om autorisation af virksomheder på el-, vvs- og kloakinstallationsområdet og lov nr. 799 af 9. juni 2020 om produkter og markedsovervågning, og regler udstedt i medfør disse love.

På den baggrund er det Erhvervsministeriets vurdering, at det er hensigtsmæssigt at udpege Sikkerhedsstyrelsen som national cybersikkerhedscertificeringsmyndighed, hvilket således foreslås med lovforslaget. I forlængelse heraf foreslås det, at Sikkerhedsstyrelsen påser overholdelse af forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov og regler fastsat i medfør af denne lov.

Rollen som cybersikkerhedscertificeringsmyndighed indebærer en række forpligtelser for Sikkerhedsstyrelsen. Sikkerhedsstyrelsen vil således skulle føre tilsyn med og håndhæve, at producenter og udbydere af IKT-produkter, -tjenester og -processer opfylder kravene i henholdsvis de specifikke europæiske cybersikkerhedscertificeringsordninger og i forordningen om cybersikkerhed.

Tilsynet og håndhævelsen af reglerne skal sikre, at IKT-produkter, -tjenester og -processer er i overensstemmelse med cybersikkerhedsattester, der er udstedt i Danmark, jf. forordningens artikel 58, stk. 7, litra a. Denne opgave skal ske i samarbejde med andre relevante tilsynsmyndigheder.

Derudover skal Sikkerhedsstyrelsen overvåge og håndhæve de forpligtelser, som påhviler danske producenter og udbydere, der foretager selvvurdering af overensstemmelse, jf. forordningens artikel 58, stk. 7, litra b. Ved selvvurdering indestår producenter og udbydere for, at IKT-produktet, -tjenesten eller -processen stemmer overens med en europæisk cybersikkerhedscertificeringsordning.

Sikkerhedsstyrelsen skal dermed føre et proaktivt tilsyn med de relevante aktører og af egen drift iværksætte disse tilsyn med aktører, der er etableret i Danmark.

Selve certificeringen og udstedelsen af en cybersikkerhedsattest skal foretages af et overensstemmelsesvurderingsorgan. Dette organ skal være akkrediteret til at foretage certificering. Akkrediteringen foretages af det nationale akkrediteringsorgan, der er udpeget i henhold til forordning (EF) nr. 765/2008 om kravene til akkreditering og markedsovervågning i forbindelse

med markedsføring af produkter, jf. artikel 60, stk. 1, i forordningen om cybersikkerhed. I Danmark er det Den Danske Akkrediteringsfond (DANAK), jf. lov nr. 1518 af 18. december 2018 om erhvervsfremme, som senest ændret ved lov nr. 796 af 9. juni 2020, og bekendtgørelse nr. 1230 af 11. december 2009 om udpegning af det nationale akkrediteringsorgan. I særlige tilfælde, hvor det er fastsat i en specifik europæisk cybersikkerhedscertificeringsordning, skal Sikkerhedsstyrelsen dog udstede certifikatet, jf. forordningens artikel 56, stk. 5.

Sikkerhedsstyrelsen skal, udover at føre tilsyn på produkt-, tjeneste-, og proces-niveau samt på producent- og udbyderniveau, bistå DANAK med at føre tilsyn med overensstemmelsesvurderingsorganerne, jf. forordningens artikel 58, stk. 7, litra c, herunder om nødvendigt gribe ind med begrænsning, suspension eller inddragelse af bemyndigelsen til at virke som overensstemmelsesvurderingsorgan, jf. forordningens artikel 58, stk. 7, litra e, 2. led.

I særlige tilfælde skal Sikkerhedsstyrelsen bemyndige overensstemmelsesvurderingsorganer til at udføre deres opgaver, hvis sådanne organer opfylder yderligere krav, der er fastsat i en europæisk cybersikkerhedscertificeringsordning, jf. forordningens 58, stk. 7, litra e, 1. led, jf. artikel 60, stk. 3.

Som led i opgaven med at føre tilsyn med certificeringen af cybersikkerhed skal Sikkerhedsstyrelsen også behandle klager over EU-overensstemmelseserklæringer, som er foretaget af producenten eller udbyderen selv, jf. forordningens artikel 53. Sikkerhedsstyrelsen kan på denne baggrund føre et reaktivt tilsyn hos aktører, der er etableret i Danmark. Det skal ske ved hjælp af efterfølgende tilsynsvirksomhed, når der klages over, at en producent eller udbyder ikke opfylder kravene i ordningen. Hvis Sikkerhedsstyrelsen undtagelsesvist har udstedt et certifikat med baggrund i en specifik ordning, og der indgives en klage herover, skal styrelsen ligeledes behandle en sådan klage.

Endelig skal Sikkerhedsstyrelsen efter forordningens artikel 59 som cybersikkerhedscertificeringsmyndighed deltage i og underkastes peerreviews af cybersikkerhedscertificeringsmyndigheder fra andre medlemsstater. Ved peerreviews skal myndighederne således vurdere hinandens procedurer, herunder bl.a. procedurer for tilsyn med og håndhævelse af reglerne for overvågning af IKT-produkter, -tjenester og -processer og procedurerne for overvågning og bemyndigelse af og tilsyn med overensstemmelsesvurderingsorganernes aktiviteter. Om nødvendigt skal resultaterne anvendes til at udstede fælles retningslinjer m.v.

3.3. Cybersikkerhedscertificeringsmyndighedens beføjelser

3.3.1. Gældende ret

Som anført i pkt. 3.1. findes der ikke gældende regulering af cybersikkerhedscertificering i Danmark. Det forhold, at forordningen om cybersikkerhed er ny, bevirker, at der på nuværende tidspunkt ikke eksisterer gældende ret, som dækker cybersikkerhedscertificeringsmyndighedens beføjelser.

3.3.2. Ministeriets overvejelser og den foreslåede ordning

Efter artikel 58, stk. 8, i forordningen om cybersikkerhed skal den nationale cybersikkerhedscertificeringsmyndighed tillægges en række minimumsbeføjelser. Som udpeget cybersikkerhedscertificeringsmyndighed efter artikel 58, stk. 1, vil Sikkerhedsstyrelsen blive ansvarlig for overvågningsopgaverne i relation til cybersikkerhedscertificering i Danmark.

Sikkerhedsstyrelsen skal derfor som minimum, jf. artikel 58, stk. 8, kunne:

- anmode overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer om at forelægge alle oplysninger, som er nødvendige for udførelsen af dens opgaver, jf. artikel 58, stk. 1, litra a,
- udføre undersøgelser i form af audit af overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer med henblik på at verificere deres overholdelse af afsnit III om rammebestemmelser for cybersikkerhedscertificering, jf. artikel 58, stk. 1, litra b,
- træffe passende foranstaltninger til at sikre, at overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer overholder bestemmelserne i forordningen eller en europæisk cybersikkerhedscertificeringsordning, jf. artikel 58, stk. 1, litra c,
- få adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller indehavere af en europæisk cybersikkerhedsattest med henblik på at udføre undersøgelser i overensstemmelse med EU-retten eller medlemsstaternes processuelle regler, jf. artikel 58, stk. 1, litra d,
- tilbagekalde europæiske cybersikkerhedsattester, der er udstedt af Sikkerhedsstyrelsen eller europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med artikel 56, stk. 6, hvis sådanne attester ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning, jf. artikel 58, stk. 1, litra e,
- pålægge sanktioner i overensstemmelse med national ret, jf. artikel 65, og at kunne kræve øjeblikkeligt ophør af overtrædelser af de

forpligtelser, der er fastsat i forordningen, jf. artikel 58, stk. 1, litra f.

Sikkerhedsstyrelsen varetager i dag opgaver på en række andre lignende områder, hvor der findes beføjelser, som svarer til de førnævnte beføjelserne. Det gælder f.eks. Sikkerhedsstyrelsens opgavevaretagelse vedr. certificering og bemyndigelse inden for områderne for metrologi og autorisation af virksomheder på el-, vvs- og kloakinstallationsområdet, og det gælder markedsovervågningen af f.eks. CE-mærkning og energimærkning.

På den baggrund er det Erhvervsministeriets vurdering, at beføjelserne i forordningens artikel 58, stk. 8, så vidt muligt gennemføres på en måde, hvor Sikkerhedsstyrelsen kan drage fordel af erfaringen med anvendelsen af lignende beføjelser.

Beføjelsen til at indhente oplysninger, jf. forordningens artikel 58, stk. 8, litra a, formuleres sådan, at Sikkerhedsstyrelsen kan kræve alle oplysninger, som er nødvendige for udførelsen af opgaven som national cybersikkerhedscertificeringsmyndighed.

Der henvises til bemærkningerne til lovforslagets § 10.

Beføjelsen til at kunne udføre undersøgelser, jf. forordningens artikel 58, stk. 8, litra b, fastsættes ved, at Sikkerhedsstyrelsen kan auditere overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer med henblik på at verificere overholdelse af forordningen om cybersikkerhed og regler fastsat i medfør af forordningen.

Der henvises til bemærkningerne til lovforslagets § 12.

Beføjelsen til at kunne træffe passende foranstaltninger, jf. forordningens artikel 58, stk. 8, litra c, gennemføres ved, at Sikkerhedsstyrelsen kan udstede påbud til en indehaver af en europæisk cybersikkerhedsattest eller en udsteder af en EU-overensstemmelseserklæring, der har bragt en eller et IKT-produkt, -tjeneste eller -proces i omsætning, som ikke er overensstemmende. Påbuddet kan bestå i en række nærmere angivne tiltag, herunder at standse markedsføring, der kan vildlede brugerne og afhjælpe ulovlige forhold. Bestemmelsen vil således også gennemføre forordningens artikel 58,

stk. 1, litra f, sidste led, idet der kan fastsættes en tidsfrist f.eks. for at afhjælpe et ulovligt forhold. På den baggrund vil der kunne kræves øjeblikkeligt ophør af en overtrædelse.

Der henvises til bemærkningerne til lovforslagets § 14.

Beføjelsen til at opnå adgang til de erhvervsdrivendes lokaler, jf. forordningens artikel 58, stk. 8, litra d, sikres ved, at Sikkerhedsstyrelsen til enhver tid mod behørig legitimation og uden retskendelse har adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller indehavere af en europæisk cybersikkerhedsattest med henblik på at føre kontrol.

Der henvises til bemærkningerne til lovforslagets § 13.

Beføjelsen til at tilbagekalde visse cybersikkerhedsattester, jf. forordningens artikel 58, stk. 8, litra e, fastsættes ved, Sikkerhedsstyrelsen kan tilbagekalde en europæisk cybersikkerhedsattest, hvis en indehaver af en attest ikke samarbejder med Sikkerhedsstyrelsen efter flere nærmere angivne kriterier, eller hvis der er tale om gentagne overtrædelser eller grov forsømmelse.

Der henvises til bemærkningerne til lovforslagets § 15.

For så vidt angår beføjelsen til at pålægge sanktioner, jf. forordningens artikel 58, stk. 8, litra f, første led, henvises til pkt. 3.4.

3.4. Sanktioner ved overtrædelse af regler om cybersikkerhedscertificering

3.4.1. Gældende ret

Som anført i pkt. 3.1. findes der ikke gældende regulering af cybersikkerhedscertificering i Danmark. Det forhold, at forordningen om cybersikkerhed er ny, bevirker, at der på nuværende tidspunkt ikke eksisterer gældende ret, som dækker sanktionerne for overtrædelse af forordningen om cybersikkerhed.

3.4.2. Ministeriets overvejelser og den foreslåede ordning

Det følger af artikel 65 i forordningen om cybersikkerhed, at de enkelte medlemsstater skal fastsætte regler om sanktioner for overtrædelser af forordningen og de europæiske certificeringsordninger for cybersikkerhed. Det

er et krav, at sanktionerne er effektive, står i et rimeligt forhold til overtrædelsen og skal have afskrækkende virkning.

Af forordningens artikel 58, stk. 8, litra f, følger det, at Sikkerhedsstyrelsen som minimum kan kræve ophør af overtrædelser af de forpligtelser, der er fastsat i forordningen. Det følger af samme artikels litra e, at Sikkerhedsstyrelsen som minimum skal kunne tilbagekalde cybersikkerhedsattester, der er udstedt af de nationale certificeringsmyndigheder eller europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med forordningens artikel 56, stk. 6, hvis sådanne attester ikke overholder bestemmelserne i denne forordning eller i en europæisk certificeringsordning for cybersikkerhed.

Omkostningerne ved certificering varierer afhængigt af produktet, tjenesten eller processen samt evaluerings- og sikringsniveauet, men er generelt en stor udgift for virksomhederne. Et certifikat til et smart meter, der attesterer, at produktet og dets omkringliggende struktur overholder de højeste tekniske og sikkerhedsmæssige standarder (BSI "Smart Meter Gateway" certificate), beløber sig til mere end en million euro. I England og Frankrig er udgiften til certificering af et smart meter omkring 150.000 euro. Det fremgår af forslaget til forordningen om cybersikkerhed af 13. september 2017, side 9.

Da lovforslagets primære formål er at udpege en national certificeringsmyndighed, som skal føre tilsyn med en certificering, som er frivillig at underlægge sig, er det Erhvervsministeriets vurdering, at det mest effektive retsmiddel vil være at tilbagekalde cybersikkerhedsattesten, hvis den ikke overholder bestemmelserne i denne forordning eller i en europæisk certificeringsordning for cybersikkerhed. Erhvervsministeriet vurderer i den forbindelse, at det vil være nødvendigt at kunne tilbagekalde enhver cybersikkerhedsattest i tilfælde af uoverensstemmelse med reglerne, og dermed ikke alene de attester, der er udstedt af de nationale certificeringsmyndigheder eller europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med forordningens artikel 56, stk. 6.

Forsvarsministeriet har koordineret den danske holdning og deltaget i forhandlingerne, der er gået forud for vedtagelsen af forordningen og har forelagt forslaget til forordningen for Folketingets Europaudvalg den 11. maj 2018. Under forhandlingerne er det fra EU's side tilkendegivet, at økonomisk straf i form af bøde ikke har været hensigten, idet det er frivilligt for

producenter og udbydere af IKT-produkter, -tjenester og -processer at blive certificeret.

Erhvervsministeriet finder på den baggrund, at det i lovforslaget bør fastsættes, at overtrædelser af de pågældende bestemmelser i forordningen, loven og de europæiske ordninger som mest indgribende foranstaltning medfører tilbagekald af den pågældende cybersikkerhedsattest. Certificering med sikkerhedsniveauet mellem eller højt udgør i sig selv en betragtelig udgift, og da der med lovforslaget skal etableres en balanceret løsning, der både tilgodeser sikkerhedshensyn og virksomheders konkurrence- og vækstvilkår, vil sanktion i form af økonomisk straf ikke stå i rimeligt forhold hertil.

3.5. Bemyndigelse til at fastsætte regler, som er nødvendige for anvendelsen af forordningen om cybersikkerhed

3.5.1. Gældende ret

Som anført i pkt. 3.1. findes der ikke gældende regulering af cybersikkerhedscertificering i Danmark. Det forhold, at forordningen om cybersikkerhed er ny, bevirker, at der på nuværende tidspunkt ikke eksisterer gældende ret, som dækker gennemførelsesretsakter i relation til cybersikkerhedscertificering.

Kommissionen har ved lovforslagets fremsættelse ikke vedtaget gennemførelsesretsakter til forordningen om cybersikkerhed.

3.3.2. Ministeriets overvejelser og den foreslåede ordning

Kommissionens vedtagelse af gennemførelsesretsakter er afgørende for anvendelsen af forordningen om cybersikkerhed. Det følger således af forordningens artikel 49, stk. 7, at de europæiske cybersikkerhedscertificeringsordninger vedtages af Kommissionen som gennemførelsesretsakter på baggrund af ENISAs forslag.

Som følge af COVID-19 er arbejdet med de første europæiske cybersikkerhedscertificeringsordninger blevet forsinket. Det følger af forordningens artikel 47, stk. 5, at Kommissionen den 28. juni 2020 skulle have offentliggjort det rullende arbejdsprogram, som opstiller strategiske prioriteter for fremtidige europæiske cybersikkerhedscertificeringsordninger, herunder omfatte en liste over IKT-produkter, -tjenester og -processer eller kategorier heraf, der vil kunne drage fordel af at være omfattet af en ordning. Det er på nu-

værende tidspunkt ukendt, hvornår den første europæiske cybersikkerheds-certificeringsordning vedtages som en gennemførelsesretsakt, og hvilket IKT-område den vil omhandle. Det forventes dog, at cloud-løsninger, 5G og Internet of Things vil være blandt kandidaterne til certificeringsordninger.

Derudover følger det af forordningens artikel 59, stk. 5, at Kommissionen kan vedtage gennemførelsesretsakter, der fastlægger en plan for peer-reviews, som omfatter en periode på mindst fem år, og kriterierne for sammensætning af peerreviewhold, metode til peerreviews samt tidsplan, hyppighed og andre opgaver i forbindelse dermed. De nationale cybersikkerhedscertificeringsmyndigheder underkastes efter artikel 59, stk. 1, peer-reviews af andre cybersikkerhedscertificeringsmyndigheder, hvilket bl.a. skal sikre, at der anvendes ensartede standarder i hele EU for så vidt angår cybersikkerhedsattester.

Endelig følger det af forordningens artikel 61, stk. 5, at Kommissionen kan vedtage gennemførelsesretsakter, der fastlægger vilkår, formater og procedurer for de nationale certificeringsmyndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer.

For at sikre en smidig og hurtig reaktion på gennemførelsesretsakter vurderer Erhvervsministeriet, at det vil være hensigtsmæssigt, at der kan fastsættes nærmere regler herom administrativt, hvor det er påkrævet.

Med lovforslaget foreslås det derfor, at erhvervsministeren bemyndiges til at udstede regler i de tilfælde, hvor det er nødvendigt for at gennemføre forordningen om cybersikkerhed, herunder som følge af gennemførelsesretsakter.

4. Økonomiske konsekvenser og implementeringskonsekvenser for det offentlige

Det vurderes, at lovforslaget ikke i sig selv vil medføre økonomiske konsekvenser og implementeringskonsekvenser for staten.

Det bemærkes dog, at forordningen om cybersikkerhed vil have økonomiske konsekvenser og implementeringskonsekvenser for staten, idet Sikkerhedsstyrelsen med lovforslaget udpeges som national cybersikkerhedscertificeringsmyndighed. Det fremgår bl.a. af forordningens artikel 58, stk. 5, at

medlemsstaterne skal sikre, at de nationale cybersikkerhedscertificeringsmyndigheder har tilstrækkelige ressourcer til at udøve deres beføjelser og udføre deres opgaver på en virkningsfuld og effektiv måde.

Forordningens endelige ikrafttrædelse medfører dermed organisatoriske ændringer for Sikkerhedsstyrelsen, idet der forventes omstillingsomkostninger i forbindelse med udpegningen som national cybersikkerhedscertificeringsmyndighed, hvor styrelsen fremover skal varetage en ny opgave på et hidtil ulovreguleret område. Der vil desuden være driftsomkostninger i forbindelse med varetagelsen af opgaven fremadrettet. Der forventes ingen umiddelbare konsekvenser for anvendelsen af it.

Det foreslås, at certificeringen af IKT-produkter, -tjenester og -processer brugerfinansieres af de virksomheder, som benytter sig af en europæisk certificeringsordning. Myndighedsopgaven skal bevillingsfinansieres, hvilket medfører økonomiske konsekvenser for det offentlige. I årene 2021-2023 afsættes 2,7 mio. kr. årligt, hvorefter ressourcebehovet evalueres.

Forordningen om cybersikkerhed påvirker ikke kommunernes eller regionernes økonomi.

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 cybersikkerhed, hvor dette er påkrævet efter forordningens bestemmelser. Enkelte gange er det vurderet at være hensigtsmæssigt med en gengivelse af bestemmelser fra forordningen for netop at lette forståelsen af lovforslaget. Lovforslaget lægger sig dermed op ad forordningens etablering af en ensartet ramme for europæisk certificering af cybersikkerhed. Lovforslaget følger dermed princip 1 om enkle og klare regler, idet der med forordningen regler skabes bedre mulighed for anerkendelse og brug af certificering på tværs af EU-landene.

Derudover skal lovforslaget understøtte den digitale kommunikation, der som udgangspunkt er obligatorisk inden for lovforslagets anvendelsesområde. Omstændighederne vedrørende f.eks. en europæisk cybersikkerhedscertificeringsordning eller Sikkerhedsstyrelsens opgave med bemyndigelse af overensstemmelsesvurderingsorganer efter lovforslagets § 5, stk. 1, jf. artikel 60, stk. 3, i forordningen om cybersikkerhed, kan medføre, at det i visse

tilfælde er nødvendigt at afvige fra den obligatoriske digitale kommunikation. Hvis der fastsættes nærmere regler om kommunikation med hjemmel i lovforslagets § 17, stk. 3, vil anvendelsen af eksisterende offentlig it-infrastruktur blive efterstræbt. Lovforslaget er dermed i overensstemmelse med princip 2 og 6.

I egenskab af national certificeringsmyndighed vil Sikkerhedsstyrelsen føre kontrol på lovforslagets område. Kontrollen vil medføre, at der bliver behandlet relevante produkt-, tjeneste-, proces- og virksomhedsinformation. I mindre omfang vil der blive behandlet personoplysninger, f.eks. hvor styrelsen indhenter dokumentation, som er udfærdiget og underskrevet af en medarbejder hos en producent af et produkt eller hos et overensstemmelsesvurderingsorgan. Behandlingen af oplysninger sker inden for rammerne af databeskyttelseslovgivningen. Lovforslaget vil derfor følge princip 5 om tryg og sikker datahåndtering.

De øvrige principper for digitaliseringsklar lovgivning vurderes ikke at være relevante for lovforslaget. Det bemærkes i den forbindelse, at forordningen om cybersikkerhed i sig selv understøtter 7 om forebyggelsen af snyd og fejl. Forordningen har netop til formål at imødekomme de tiltagende cybersikkerhedsudfordringer i EU, bl.a. ved selve etableringen af den fælles ramme for europæisk cybersikkerhedscertificering, øge borgere og virksomheders bevidsthed om cybersikkerhed og styrke kompetencerne i medlemsstaterne og i ENISA. Alt andet lige er det på den baggrund vurderingen, at øget brug af certificering af IKT-produkter, -tjenester og -processer vil bidrage til færre risici for snyd og fejl, idet certificeringen vil kunne indgå som et positivt parameter i markedsføringen af det pågældende IKT-produkt, -tjeneste eller -proces.

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

Det bemærkes overordnet, at lovforslaget supplerer forordningen om cybersikkerhed, som har økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget forventes på den baggrund ikke i sig selv at have økonomiske eller administrative konsekvenser for erhvervslivet m.v. af betydning.

For så vidt angår lovforslagets bemyndigelsesbestemmelser vil der i forbindelse med udstedelsen af eventuelle bekendtgørelser blive foretaget en vurdering af eventuelle økonomiske og administrative konsekvenser for erhvervslivet m.v.

Lovforslaget har været sendt til Erhvervsstyrelsens Område for Bedre Regulering (OBR), der på det foreliggende grundlag har vurderet, at lovforslaget ikke i sig selv medfører administrative konsekvenser for erhvervslivet m.v.

Principperne for agil erhvervsrettede regulering
Det bemærkes igen, at lovforslaget supplerer forordningen om cybersikkerhed, som fastlægger en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger.

På den baggrund understøtter lovforslaget muligheden for anvendelsen af nye forretningsmodeller, idet forordningen skal bidrage til styrkelsen af det indre marked bl.a. ved, at der bliver bedre mulighed for anerkendelse og brug af europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer for IKT-produkter, -tjenester og -processer på tværs af medlemsstaterne. Samtidig skal lovforslaget bidrage til at sikre forordningens intention om bl.a. at styrke tilliden til IKT-produkter, -tjenester og -procedurer.

Lovforslagets formål er alene at supplere forordningen om cybersikkerhed. Der er derfor et klart fokus på enkel og formålsbestemt regulering, idet reguleringen af området i det væsentligste fastsættes med forordningen, som kun efterlader få muligheder for at fastsætte yderligere bestemmelser.

Det vurderes, at de øvrige principper for agil erhvervsrettet regulering ikke er relevante for lovforslaget.

6. Administrative konsekvenser for borgerne
Lovforslaget har ikke administrative konsekvenser for borgerne.

7. Miljømæssige konsekvenser
Lovforslaget har ikke miljømæssige konsekvenser.

8. Forholdet til EU-retten
Lovforslaget fastsætter supplerende bestemmelser til forordningen om cybersikkerhed. Hovedparten af forordningen trådte i kraft den 27. juni 2019. Artikel 58, 60, 61, 63, 64 og 65, som indeholder en række bestemmelser om certificering af cybersikkerhed finder dog først anvendelse fra den 28. juni 2021.

Forordningens fulde titel er Europa-Parlamentets og Rådets forordning (EU) 2019/88 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed), og den blev trykt i Den Europæiske Unions Tidende L 151, 62. årgang, 7. juni 2019.

Ved lovforslaget udpeges Sikkerhedsstyrelsen som national myndighed for certificering af cybersikkerhed, og der skabes et grundlag for at kunne overvåge, håndhæve og reagere på overtrædelser af forordningen om cybersikkerhed og regler fastsat i medfør heraf, herunder de europæiske cybersikkerhedscertificeringsordninger.

9. Hørte myndigheder og organisationer m.v.

Et udkast til lovforslag har i perioden fra den 19. oktober 2020 til den 16. november 2020 været sendt i høring hos følgende myndigheder og organisationer m.v.:

Advokatsamfundet, Arbejderbevægelsens Erhvervsråd, Arbejdsmiljørådet, Certificerede Organers Forum, DANAK – Den Danske Akkrediteringsfond, Danmarks Aktive Forbrugere, Dansk Brand- og sikringsteknisk Institut, Dansk Byggeri, Dansk Erhverv, Dansk Industri, Dansk IT, Dansk Standard, Varefakta, Danske Advokater, FABA, Fagbevægelsens Hovedorganisation, Forbrugerlaboratoriet, Forbrugerombudsmanden, Forbrugerrådet Tænk, Foreningen af Rådgivende Ingeniører, Foreningen for Dansk Internethandel, Forsikring & Pension, Ingeniørforeningen i Danmark, IT-Branchen, KL, Legetøjsbranchen LEG, SMVdanmark, TEKNIQ Arbejdsgiverne, Teknologisk Institut, Teleindustrien, TÜV Nord Danmark ApS, UL International Demko A/S, VELTEK.

10. Sammenfattende skema

	Positive konsekvenser/mindreudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)	Negative konsekvenser/merudgifter (hvis ja, angiv omfang/Hvis nej, anfør »Ingen«)
Økonomiske konsekvenser for stat, kommuner og regioner	Ingen	Myndighedsopgaven, som er påkrævet efter forordningen om cybersikkerhed, bevillingsfinansieres og i

		årene 2021-2023 afsættes 2,7 mio. kr. årligt.
Implementeringskonsekvenser for stat, kommuner og regioner	Ingen	Der forventes omstillingsomkostninger og driftsomkostninger i forbindelse med udpegningen som national cybersikkerhedscertificeringsmyndighed, hvor styrelsen fremover skal varetage en ny opgave på et hidtil ulovreguleret område.
Økonomiske konsekvenser for erhvervslivet	Lovforslaget forventes ikke at have økonomiske konsekvenser for erhvervslivet, men forordningen om cybersikkerhed forventes på samfundsniveau og for erhvervslivet generelt at have positive økonomiske konsekvenser.	Lovforslaget forventes ikke at have økonomiske konsekvenser for erhvervslivet.
Administrative konsekvenser for erhvervslivet	Lovforslaget forventes ikke at have økonomiske konsekvenser for erhvervslivet.	Lovforslaget forventes ikke at have økonomiske konsekvenser for erhvervslivet.
Administrative konsekvenser for borgerne	Ingen	Ingen
Miljømæssige konsekvenser	Ingen	Ingen
Forholdet til EU-retten	Lovforslaget supplerer Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed), der trådte i kraft den 27. juni 2019 med undtagelse af artikel 58, 60, 61, 63, 64 og 65, som gælder umiddelbart i Danmark fra den 28. juni 2021.	
Er i strid med de principper for implementering af erhvervsrettet EU-regulering/ Går videre end minimumskrav i EU-regulering	Ja	Nej X

(sæt X)	

Bemærkninger til lovforslagets enkelte bestemmelser

Til § 1

Det forhold, at forordningen om cybersikkerhed for så vidt fastsættelsen af bestemmelser om cybersikkerhedscertificering er ny, bevirker, at der ikke på nuværende tidspunkt eksisterer gældende ret, som dækker samme område.

Der foreslås i *§ 1*, at loven supplerer Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed), jf. bilag 1 til denne lov.

Med forordningen om cybersikkerhed etableres bl.a. en fælles europæisk ramme for cybersikkerhedscertificering af IKT-produkter, -tjenester og -processer. Forordningen om cybersikkerhed gælder umiddelbart i Danmark, men forordningen kræver visse gennemførelsesforanstaltninger. Med bestemmelsen fastsættes det derfor, at loven supplerer forordningen om cybersikkerhed.

Der henvises til pkt. 3 i lovforslagets almindelige bemærkninger.

Til § 2

Det forhold, at forordningen om cybersikkerhed for så vidt fastsættelsen af bestemmelser om cybersikkerhedscertificering er ny, bevirker, at der ikke på nuværende tidspunkt eksisterer gældende ret, som dækker samme område.

Den foreslåede bestemmelse vedrører lovforslagets anvendelsesområde.

Det foreslås i *§ 2*, at loven gælder for producenter og udbydere af IKT-produkter, -tjenester og -processer, som er omfattet af en europæisk cybersikkerhedscertificeringsordning, og for overensstemmelsesvurderingsorganer og andre certifikatudstedende organer.

Bestemmelsen medfører, at lovens anvendelsesområde stemmer overens med anvendelsesområdet for forordningen om cybersikkerhed. Det følger således af artikel 1, stk. 1, litra b, at der med forordningen fastlægges en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, -tjenester og -processer i EU.

På nuværende tidspunkt findes der ikke i EU eller i Danmark regler, der gør cybersikkerhedscertificering obligatorisk. Da cybersikkerhedscertificering efter artikel 56, stk. 2, skal være frivillig, medmindre andet er fastsat, er det nødvendigt at fastsætte et anvendelsesområde for loven, som tager højde herfor. Derfor foreslås det, at lovens bestemmelser alene finder anvendelse i det omfang, at der findes en europæisk cybersikkerhedscertificeringsordning, som omfatter den eller det pågældende IKT-produkt, -tjeneste og -proces, og hvor en producent eller udbyder tillige ønsker at udnytte muligheden for at opnå certificering eller foretage selvvurdering af overensstemmelse og herefter udstede en EU-overensstemmelseserklæring.

Bestemmelsen indebærer derfor også, at loven ikke finder anvendelse på IKT-produkter, -tjenester og -processer, der ikke omfattes af en europæisk cybersikkerhedscertificeringsordning, eller hvor producenter eller udbydere ikke ønsker at opnå certificering eller udstede en overensstemmelseserklæring i henhold til en europæisk cybersikkerhedscertificeringsordning.

Endelig foreslås det med bestemmelsen, at loven gælder for overensstemmelsesvurderingsorganer. Bestemmelsen forudsættes at gælde for ethvert overensstemmelsesvurderingsorgan, uanset om organet er privat eller offentligt, jf. forordningens artikel 56, stk. 5, litra b, og uanset om organet foretager overensstemmelsesvurdering på almindelige vilkår eller på baggrund af en generel delegation vedrørende cybersikkerhedscertificeringsordninger med tillidsniveau højt efter forordningens artikel 56, stk. 6, litra b, jf. lovforslagets § 7, stk. 1.

Overensstemmelsesvurderingsorganer spiller en afgørende rolle i certificeringen af et IKT-produkt, -tjeneste og -proces. Som det fremgår af forordningens præambelbetragtning 77 skyldes det, at det relevante organ ved udstedelsen af en europæisk cybersikkerhedsattest bekræfter, at et IKT-produkt, -tjeneste og -proces er blevet evalueret med henblik på overensstemmelse med specifikke sikkerhedskrav fastsat i en europæisk cybersikkerhedscertificeringsordning. Certificeringen bekræfter dermed, at de nærmere krav til et IKT-produkt, en IKT-tjeneste eller en IKT-proces er opfyldt.

Medlemsstaterne pålægges efter forordningen om cybersikkerhed at tildele en række minimumsbeføjelser til den nationale cybersikkerhedscertificeringsmyndighed, herunder bl.a. beføjelsen til at auditere overensstemmelsesvurderingsorganer efter artikel 58, stk. 8, litra b. Derudover har cybersikkerhedscertificeringsmyndigheden efter artikel 58, stk. 7, litra c, en pligt til at bistå og støtte DANAK med overvågningen af overensstemmelsesvurderingsorganernes aktiviteter.

Endelig kan det i en europæisk cybersikkerhedscertificeringsordning være fastsat, at et andet organ end et overensstemmelsesvurderingsorgan i forordningens forstand har til opgave at foretage udstedelsen af cybersikkerhedsattester. I så fald er der ikke nødvendigvis sammenfald mellem overensstemmelsesvurderingsorganet og det certifikatudstedende organ, som dermed kan være to forskellige organer.

Denne mulighed følger f.eks. af det såkaldte EU Common Criteria Scheme (EUCC – herefter kaldet Common Criteria), som er en konkret certificeringsramme for evaluering af sikkerheden i informationsteknologi. Common Criteria er i overensstemmelse med forordningens artikel 48, stk. 2, foreslået af ENISA som en europæisk cybersikkerhedscertificeringsordning. Common Criteria er på tidspunktet for lovforslagets fremsættelse endnu ikke vedtaget som en certificeringsordning i henhold til forordningen.

På ovenstående baggrund foreslås det, at loven gælder for overensstemmelsesvurderingsorganer og andre certifikatudstedende organer for så vidt angår alle organernes aktivitet i relation til forordningen om cybersikkerhed, herunder europæiske cybersikkerhedscertificeringsordninger.

Til § 3

Efter artikel 58, stk. 1, i forordningen om cybersikkerhed skal hver medlemsstat udpege en eller flere nationale cybersikkerhedscertificeringsmyndigheder på sit område eller efter aftale med en anden medlemsstat en eller flere cybersikkerhedscertificeringsmyndigheder, der er etableret i den anden medlemsstat, som ansvarlig for overvågningsopgaverne i den udpegende medlemsstat.

Det foreslås i *§ 3*, at Sikkerhedsstyrelsen udpeges som national cybersikkerhedscertificeringsmyndighed, jf. artikel 58, stk. 1, i forordningen om cybersikkerhed.

Med bestemmelsen udpeges Sikkerhedsstyrelsen dermed til at varetage overvågningsopgaverne efter forordningen om cybersikkerhed i Danmark. Sikkerhedsstyrelsen skal derfor bl.a. bistå DANAK med overvågning af overensstemmelsesvurderingsorganer og selv føre tilsyn med og håndhæve, at producenter og udbydere af IKT-produkter, -tjenester og -processer opfylder kravene i henholdsvis de specifikke europæiske cybersikkerhedscertificeringsordninger og i forordningen om cybersikkerhed. Sikkerhedsstyrelsen skal også overvåge og håndhæve de forpligtelser, som påhviler danske producenter og udbydere, der foretager selvvurdering af overensstemmelse.

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

Til § 4

Det følger af artikel 60, stk. 1, i forordningen om cybersikkerhed, at overensstemmelsesvurderingsorganerne akkrediteres af nationale akkrediteringsorganer, der er udpeget i henhold til forordning (EF) nr. 765/2008. Akkrediteringen udstedes kun, hvis overensstemmelsesvurderingsorganet opfylder kravene i bilaget til forordning om cybersikkerhed.

Det foreslås i *§ 4*, at DANAK akkrediterer overensstemmelsesvurderingsorganer efter artikel 60, stk. 1, i forordningen om cybersikkerhed, hvis organet opfylder kravene i bilaget til forordningen.

Med bestemmelsen gengives og uddybes indholdet af forordningens artikel 60, stk. 1. Bestemmelsen berører ikke forordningens umiddelbare gyldighed i Danmark, men er alene begrundet i praktiske hensyn, da det er vurderingen, at gengivelsen vil lette forståelsen af sammenhængen mellem loven og forordningen om cybersikkerhed.

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.

DANAK kan dermed udpege overensstemmelsesorganer på forordningens område, hvis et organ opfylder kravene i bilaget til forordningen. Kravene består af 20 punkter, der bl.a. vedrører krav til uafhængighed ift. vurderede IKT-produkter, -tjenester eller -processer, teknisk kompetence, fornødne

midler til at varetage opgaven, ansvarsforsikring og opfyldelse af relevante standarder.

Det følger af forordningens præambelbetragtning nr. 97, at nationale akkrediteringsorganer bør begrænse, suspendere eller tilbagekalde akkrediteringen af et overensstemmelsesvurderingsorgan, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis overensstemmelsesvurderingsorganet overtræder forordningen.

Muligheden herfor er allerede etableret i dansk ret. Dette følger således af bekendtgørelse nr. 913 af 25. september 2009 om akkreditering af virksomheder, hvor der i kapitel 3 er fastsat nærmere regler om tilsyn med akkrediterede virksomheder, herunder suspendering og ophør af akkrediteringen.

Til § 5

Det følger af artikel 60, stk. 3, i forordningen om cybersikkerhed, at hvis europæiske cybersikkerhedscertificeringsordninger fastsætter specifikke eller yderligere krav i henhold til artikel 54, stk. 1, litra f, – bestemmelsen om obligatoriske elementer i en certificeringsordning – må kun overensstemmelsesvurderingsorganer, der opfylder disse krav, bemyndiges af den nationale cybersikkerhedscertificeringsmyndighed til at udføre opgaver i henhold til sådanne ordninger.

Det er samtidig udgangspunktet efter forordningens artikel 60, stk. 1, at overensstemmelsesvurderingsorganer skal akkrediteres af DANAK, hvis et organ opfylder kravene i bilaget til forordningens.

Der henvises til bemærkningerne til § 4 for så vidt angår DANAKs akkreditering af overensstemmelsesvurderingsorganer.

Det foreslås i *§ 5, stk. 1,* at Sikkerhedsstyrelsen kan bemyndige overensstemmelsesvurderingsorganer efter artikel 60, stk. 3, i forordningen om cybersikkerhed, hvis der i en europæisk cybersikkerhedscertificeringsordning er fastsat specifikke eller yderligere krav end dem, der følger af artikel 54, stk. 1, litra f, i forordningen om cybersikkerhed.

Med bestemmelsen sikres gennemførelsen af artikel 60, stk. 3, i forordningen om cybersikkerhed. Dermed kan Sikkerhedsstyrelsen i sin egenskab af

cybersikkerhedscertificeringsmyndighed bemyndige overensstemmelsesvurderingsorganer, hvis dette er påkrævet i henhold til en europæisk cybersikkerhedscertificeringsordning.

Det følger af forordningens artikel 58, stk. 7, litra e, at den nationale cybersikkerhedscertificeringsmyndighed bl.a. skal begrænse, suspendere eller inddrage bemyndigelse i henhold til forordningens artikel 60, stk. 3, hvis et overensstemmelsesvurderingsorgan overtræder kravene i forordningen.

Det foreslås i *stk. 2*, at konstaterer Sikkerhedsstyrelsen, at et overensstemmelsesvurderingsorgan overtræder de specifikke eller yderlige krav, som er nævnt i stk. 1, kan Sikkerhedsstyrelsen begrænse eller suspendere bemyndigelsen og fastsætte en rimelig tidsfrist for afhjælpning af de konstaterede overtrædelser.

Bestemmelsen vedrører overensstemmelsesorganernes overtrædelse af forordningen om cybersikkerhed hvad angår certificering i henhold til en bemyndigelse efter forordningens artikel 60, stk. 3, og hvordan Sikkerhedsstyrelsen i givet fald kan reagere. Bortset fra gentagne eller grove overtrædelser, jf. nærmere nedenfor om stk. 3, er det vurderingen, at overensstemmelsesvurderingsorganer bør have mulighed for at rette op på overtrædelser, før en bemyndigelse kan tilbagekaldes.

Det foreslås derfor, at en bemyndigelse kan begrænses, hvilket f.eks. kan indebære, at der ikke kan foretages certificering i henhold til en eller flere nærmere angivne cybersikkerhedscertificeringsordninger. Det foreslås yderligere, at Sikkerhedsstyrelsen kan suspendere bemyndigelsen fuldstændigt, hvilket vil medføre, at organet fratages muligheden for at foretage certificering i henhold til den pågældende bemyndigelse.

I begge tilfælde kan Sikkerhedsstyrelsen fastsætte en tidsfrist til afhjælpning af de konstaterede overtrædelser. En tidsfrist skal fastsættes efter en konkret og individuel vurdering ud fra overtrædelsens karakter, den tidsmæssige mulighed for at afhjælpe overtrædelsen og indholdet af den relevante cybersikkerhedscertificeringsordning.

Det foreslås i *stk. 3*, at Sikkerhedsstyrelsen kan tilbagekalde bemyndigelsen efter stk. 1. Det foreslås i *nr. 1*, at dette kan ske, hvis forudsætningerne for bemyndigelsen efter stk. 1 ikke længere er opfyldt. I det foreslåede *nr. 2* kan tilbagekaldelse ske, hvis overensstemmelsesvurderingsorganet ikke afhjæl-

per de konstaterede overtrædelser inden for den fastsatte frist i stk. 2. Endelig forslås det i *nr. 3*, at Sikkerhedsstyrelsen kan tilbagekalde bemyndigelsen, hvis overensstemmelsesvurderingsorganet gentagne gange eller ved grov forsømmelse overtræder de specifikke eller yderligere krav, som er nævnt i stk. 1.

Med bestemmelsen foreslås det således, at Sikkerhedsstyrelsen i tre tilfælde kan tilbagekalde en bemyndigelse i henhold til forordningens artikel 60, stk. 3.

For det første kan en bemyndigelse tilbagekaldes, hvis forudsætningerne ikke længere er opfyldt. Forudsætningerne for en bemyndigelse vil afhænge af de specifikke eller yderligere krav, der er fastsat i en cybersikkerhedscertificeringsordning i forordningens artikel 54, stk. 1, litra f. Forudsætningerne kan dermed variere alt efter indholdet af den enkelte cybersikkerhedscertificeringsordning.

For det andet kan bemyndigelsen tilbagekaldes, hvis overensstemmelsesvurderingsorganet ikke afhjælper konstaterede overtrædelser som beskrevet ovenfor vedrørende stk. 2. Dette gælder således, hvis et organ ikke inden for en fastsat frist har afhjulpet overtrædelsen.

Endelig kan en bemyndigelse tilbagekaldes, hvis der er tale om gentagen eller grov forsømmelse af de specifikke eller yderligere krav til en cybersikkerhedscertificeringsordning, der følger af forordningens artikel 54, stk. 1, litra f. Bestemmelsen skal sikre, at Sikkerhedsstyrelsen kan gribe ind over for gentagne eller grove overtrædelser, idet sådanne overtrædelser kan underminere formålet med en cybersikkerhedscertificeringsordning. Bestemmelsen forventes alene at blive anvendt i særlige tilfælde, og hvor det samtidig er vurderingen, at bestemmelsen i stk. 2 er utilstrækkelig.

Til § 6

Det følger af artikel 60, stk. 2, i forordningen om cybersikkerhed at i tilfælde, hvor en europæisk cybersikkerhedsattest udstedes af en national cybersikkerhedscertificeringsmyndighed i henhold til artikel 56, stk. 5, litra a, og artikel 56, stk. 6, akkrediteres den nationale cybersikkerhedscertificeringsmyndigheds certificeringsorgan som et overensstemmelsesvurderingsorgan i henhold til artikel 60, stk. 1. Det fremgår af artikel 60, stk. 1, at overensstemmelsesvurderingsorganer akkrediteres af nationale akkrediteringsorganer, hvilket i Danmark vil sige DANAK.

Det foreslås i *§ 6*, at erhvervsministeren kan fastsætte regler om udpegning af et certificeringsorgan under Sikkerhedsstyrelsen efter artikel 60, stk. 2, i forordningen om cybersikkerhed.

På nuværende tidspunkt er der endnu ikke vedtaget nogen europæiske cybersikkerhedscertificeringsordninger. Dermed findes der ikke endnu nogle tilfælde, hvor en cybersikkerhedsattest kun må udstedes af et offentligt organ, jf. forordningens artikel 56, stk. 5, litra a, eller af et overensstemmelsesvurderingsorgan, hvor cybersikkerhedscertificeringsmyndigheden har forhåndsgodkendt attesten eller har delegeret kompetencen til udførelsen af opgaven til et organ, jf. forordningens artikel 56, stk. 6.

Bestemmelsen skal sikre, at det i Danmark er muligt at have et certificeringsorgan under den nationale cybersikkerhedscertificeringsmyndighed, hvis de rette omstændigheder er til stede, herunder i form af den rette tekniske kompetence. Det foreslås derfor, at erhvervsministeren bemyndiges til at kunne fastsætte regler om udpegning af et certificeringsorgan under Sikkerhedsstyrelsen. I tilfælde hvor en cybersikkerhedsattest alene kan udstedes af et offentligt organ, jf. forordningens artikel 56, stk. 5, litra a, og artikel 56, stk. 6, vil bestemmelsen således kunne anvendes til at fastsætte de påkrævede regler herom.

Det er imidlertid ikke en forudsætning for anvendelsen af bestemmelsen, at der faktisk er vedtaget en europæisk cybersikkerhedscertificeringsordning, som vedrører forordningens artikel 56, stk. 5, litra a, eller artikel 56, stk. 6. Bestemmelsen kan således anvendes i det omfang erhvervsministeren finder det hensigtsmæssigt at etablere et certificeringsorgan under Sikkerhedsstyrelsen, f.eks. med henblik på sikre varetagelsen af opgaver, som visse europæiske cybersikkerhedscertificeringsordninger potentielt kan medføre i fremtiden.

I forlængelse heraf forudsættes det ikke med lovforslaget, at bemyndigelsen nødvendigvis udnyttes af erhvervsministeren, uanset om der vedtages en europæisk cybersikkerhedscertificeringsordning, som vedrører forordningens artikel 56, stk. 5, litra a, eller artikel 56, stk. 6. Danmark er således efter forordningen ikke forpligtet til at udbyde certificering af enhver europæisk cybersikkerhedscertificeringsordning, som vedtages i henhold til forordningen. Det vil derfor bero på en vurdering af den enkelte cybersikkerhedscertificeringsordning, om forudsætningerne er til stede til at certificeringen kan ske i Danmark. Hvis det ikke er tilfældet kan producenter og udbydere af

IKT-produkter, -tjenester og -processer under alle omstændigheder benytte sig af muligheden for certificering i andre medlemsstater, hvor certificering efter den pågældende cybersikkerhedscertificeringsordning udbydes.

Det fremgår af forordningens artikel 58, stk. 4, at medlemsstaterne skal sikre, at de nationale cybersikkerhedscertificeringsmyndigheders aktiviteter vedrørende udstedelse af europæiske cybersikkerhedsattester omhandlet i artikel 56, stk. 5, litra a, og artikel 56, stk. 6, er strengt adskilt fra deres tilsynsaktiviteter i artikel 58 i øvrigt, og at aktiviteterne udføres uafhængigt af hinanden.

Det fremgår desuden af artikel 60, stk. 2, at i tilfælde, hvor en europæisk cybersikkerhedsattest udstedes af en national cybersikkerhedscertificeringsmyndighed i henhold til artikel 56, stk. 5, litra a, og artikel 56, stk. 6, akkrediteres den nationale cybersikkerhedscertificeringsmyndigheds certificeringsorgan som et overensstemmelsesvurderingsorgan i henhold artikel 60, stk. 1.

I udmøntningen af den foreslåede bestemmelse vil der således skulle indgå en række overvejelser, herunder organisatoriske og økonomiske forhold. Som følge af forordningens artikel 58, stk. 4, og 60, stk. 2, vil der for et certificeringsorgan skulle sikres uafhængighed fra Sikkerhedsstyrelsens øvrige opgaver som tilsynsførende cybersikkerhedscertificeringsmyndighed, og Sikkerhedsstyrelsen vil skulle opfylde kravene i forordningens bilag for at blive akkrediteret af DANAK på lige fod mod andre overensstemmelsesvurderingsorganer.

Til § 7

Det følger af artikel 56, stk. 6, i forordningen om cybersikkerhed, at i tilfælde, hvor en europæisk cybersikkerhedscertificeringsordning indeholder krav om tillidsniveau højt kan den europæiske cybersikkerhedsattest i henhold til den pågældende ordning kun udstedes af en national cybersikkerhedscertificeringsmyndighed eller af et overensstemmelsesvurderingsorgan, hvis a) den nationale cybersikkerhedscertificeringsmyndighed på forhånd har godkendt hver enkelt europæisk cybersikkerhedsattest, som er udstedt af et overensstemmelsesvurderingsorgan, eller b) på grundlag af den nationale cybersikkerhedscertificeringsmyndigheds generelle delegation af opgaven med at udstede sådanne europæiske cybersikkerhedsattester til et overensstemmelsesvurderingsorgan.

Forordningens artikel 58, stk. 6, medfører, at en cybersikkerhedscertificeringsmyndighed – hvis denne ikke ønsker eller ikke har mulighed for at blive akkrediteret – kan forhåndsgodkende et overensstemmelsesvurderingsorgans udstedelse af visse cybersikkerhedsattester eller delegere kompetence til organet.

Det foreslås i *§ 7, stk. 1*, at Sikkerhedsstyrelsen kan delegere sin kompetence til at udstede europæiske cybersikkerhedsattester efter artikel 56, stk. 6, litra b, i forordningen om cybersikkerhed til et overensstemmelsesvurderingsorgan.

Det foreslås i *stk. 2*, at erhvervsministeren kan fastsætte nærmere regler om udførelsen af den opgave, som Sikkerhedsstyrelsen kan delegere til et overensstemmelsesvurderingsorgan efter artikel 56, stk. 6, litra b, i forordningen om cybersikkerhed, jf. stk. 1.

På nuværende tidspunkt er der endnu ikke vedtaget nogen europæiske cybersikkerhedscertificeringsordninger. Der er derfor uklart, om eller hvornår det kan blive nødvendigt for en cybersikkerhedscertificeringsmyndighed at forhåndsgodkende udstedelsen af en cybersikkerhedsattest eller delegere kompetence til et overensstemmelsesvurderingsorgan efter forordningens artikel 56, stk. 6.

Med stk. 1 sikres det, at Sikkerhedsstyrelsen som cybersikkerhedscertificeringsmyndighed har mulighed for at delegere kompetencen til at udstede cybersikkerhedsattester, når der vedtages en europæisk cybersikkerhedscertificeringsordning med højt tillidsniveau. Det foreslås derfor, at erhvervsministeren kan delegere sin kompetence til at udstede europæiske cybersikkerhedsattester efter forordningens artikel 56, stk. 6, litra b, og at erhvervsministeren kan fastsætte nærmere regler herom.

Ligesom det er tilfældet med bestemmelsen i lovforslagets § 6, så forudsættes det ikke med lovforslaget, at bestemmelsen nødvendigvis udnyttes. Det vil således afhænge af en konkret vurdering af den enkelte cybersikkerhedscertificeringsordning, og om de rette omstændigheder er til stede, herunder om der findes et overensstemmelsesvurderingsorgan i Danmark, som er i stand til og ønsker at løfte opgaven.

Bestemmelsen i stk. 2 omhandler de tilfælde, hvor Sikkerhedsstyrelsen udnytter sin adgang, jf. den foreslåede bestemmelse i stk. 1, til at delegere op-

gaven i henhold til artikel 56, stk. 6, til et eller flere overensstemmelsesvurderingsorganer. Der består i disse tilfælde ikke et over-/underordnelsesforhold mellem erhvervsministeren og det pågældende organ. Der vil herefter være behov for, at erhvervsministeren fastsætter regler om rammerne for, hvorledes organet, som bemyndiges efter stk. 1, skal varetage de delegerede beføjelser, herunder rækkevidden af delegationen.

Til § 8

Det følger af artikel 58, stk. 1, i forordningen om cybersikkerhed, at hver medlemsstat udpeger en eller flere nationale cybersikkerhedscertificeringsmyndigheder på sit område eller udpeger efter aftale med en anden medlemsstat en eller flere nationale cybersikkerhedscertificeringsmyndigheder, der er etableret i denne anden medlemsstat, som ansvarlig for overvågningsopgaverne i den udpegende medlemsstat. Det følger ligeledes af stk. 2, at hver medlemsstat underretter Kommissionen om de udpegede nationale cybersikkerhedscertificeringsmyndigheders identitet. Hvis en medlemsstat udpeger mere end én myndighed, underretter den også Kommissionen om de opgaver, som hver af disse myndigheder er blevet pålagt.

Det foreslås i *§ 8*, at erhvervsministeren kan fastsætte regler om udpegning af en udenlandsk cybersikkerhedscertificeringsmyndighed, et udenlandsk offentligt organ eller et andet overensstemmelsesvurderingsorgan til at varetage opgaver i henhold til artikel 56, stk. 5 og 6, i forordningen om cybersikkerhed.

På nuværende tidspunkt er der endnu ikke vedtaget nogen europæiske cybersikkerhedscertificeringsordninger. Der er derfor uklart, om eller hvornår det bliver nødvendigt for en cybersikkerhedscertificeringsmyndighed at 1) udstede cybersikkerhedsattester, hvis det er fastsat i en europæisk cybersikkerhedscertificeringsordning, jf. forordningens artikel 56, stk. 5, eller 2) forhåndsgodkende udstedelsen af en cybersikkerhedsattest eller delegere kompetence til et organ efter artikel 56, stk. 6, hvis der er tale om en cybersikkerhedscertificeringsordning med højt tillidsniveau.

Efter lovforslagets § 6 kan erhvervsministeren fastsætte regler om udpegning af et certificeringsorgan under Sikkerhedsstyrelsen. Af lovforslagets § 7 følger en mulighed for Sikkerhedsstyrelsen til at delegere kompetencen til at udstede europæiske cybersikkerhedsattester til et overensstemmelsesvurderingsorgan. Der henvises til bemærkningerne til lovforslagets §§ 6 og 7.

Med den forslåede bestemmelse i § 8 etableres imidlertid en mulighed for, at erhvervsministeren kan fastsætte regler om udpegning af en udenlandsk cybersikkerhedscertificeringsmyndighed, et udenlandsk offentligt organ eller et andet overensstemmelsesvurderingsorgan til at varetage opgaver i henhold artikel 56, stk. 5 og 6.

Bestemmelsen skal sikre, at det er muligt for danske virksomheder at opnå certificering i de tilfælde, som følger af forordningens artikel 56, stk. 5 og 6. Anvendelsen af bestemmelsen vil således bero på en afvejning af, om der er de nødvendige økonomiske og tekniske forudsætninger, herunder efterspørgsel i markedet, for at udføre opgaven i Danmark, eller om det er mere oplagt at anvende en anden cybersikkerhedscertificeringsmyndighed, et offentligt organ eller et overensstemmelsesvurderingsorgan, som ved generel delegation er kompetent til at udstede de pågældende europæiske cybersikkerhedsattester, der alle er etableret i en anden medlemsstat.

På den baggrund vil bestemmelsen kunne anvendes til at fastsætte regler om, at en anden cybersikkerhedscertificeringsmyndighed, et offentligt organ eller et overensstemmelsesvurderingsorgan skal udføre de konkrete opgaver, der følger af forordningens artikel 56, stk. 5 og 6. Den pågældende opgavevaretagelse vil skulle ske efter aftale med den anden cybersikkerhedscertificeringsmyndighed, det offentlige organ eller overensstemmelsesvurderingsorganet.

Bestemmelsen ændrer ikke på, at det er Sikkerhedsstyrelsen, der udpeges som national cybersikkerhedscertificeringsmyndighed i Danmark, og som derfor er ansvarlig for overvågningsopgaverne i medfør af forordningen om cybersikkerhed. Der henvises til bemærkningerne til lovforslagets §§ 3 og 9.

Til § 9

Efter artikel 58, stk. 1, i forordningen om cybersikkerhed skal hver medlemsstat udpege en eller flere nationale cybersikkerhedscertificeringsmyndigheder på sit område eller efter aftale med en anden medlemsstat en eller flere cybersikkerhedscertificeringsmyndigheder, der er etableret i den anden medlemsstat, som ansvarlig for overvågningsopgaverne i den udpegende medlemsstat.

Det foreslås i *§ 9, 1. pkt.*, at Sikkerhedsstyrelsen påser og håndhæver overholdelsen af forordningen om cybersikkerhed og regler fastsat i medfør af

forordningen. Det foreslås i *2. pkt.*, at Sikkerhedsstyrelsen endvidere påser og håndhæver overholdelsen af denne lov og regler fastsat i medfør af denne lov.

Tilsynsmyndigheden tillægges i dette lovforslags kapitel 4 i §§ 9-15 en række muligheder for at føre kontrol med, om de vedtagne regler overholdes, herunder indhente de nødvendige oplysninger, foretage audit og få adgang til lokaler i kontroløjemed. Sikkerhedsstyrelsen får desuden hjemmel til at træffe afgørelse, udstede påbud og tilbagekalde cybersikkerhedsattester.

Sikkerhedsstyrelsens opgaver som national certificeringsmyndighed er opdelt i tre hovedområder, som dækker tilsyn, særlige opgaver som følge af specifikke ordninger (udstedelse af certifikater, bemyndigelse og delegation) og behandling af klager, hvor det første område forventes at udgøre langt størstedelen af Sikkerhedsstyrelsens virksomhed inden for certificering af cybersikkerhed i medfør af forordningen om cybersikkerhed.

De tilsynsopgaver, som Sikkerhedsstyrelsen bliver ansvarlig for som national certificeringsmyndighed, er:

- Tilsyn med om et IKT-produkt, -tjeneste eller -proces overholder kravene i en cybersikkerhedsattest, jf. forordningens artikel 54, stk. 1, litra j, jf. artikel 58, stk. 7, litra a.
- Overvågning af om en producent eller udbyder, der foretager selvvurdering af overensstemmelse, overholder sine forpligtelser, jf. artikel 53, stk. 2 og 3, og de i ordningen fastsatte regler, jf. forordningens artikel 54, stk. 1, litra j, jf. artikel 58, stk. 7, litra b.
- Tilsyn med og overvågning af om de aktiviteter, der knytter sig til Sikkerhedsstyrelsens udstedelse af certifikater på baggrund af en ordnings specifikke krav herom, jf. forordningens artikel 56, stk. 5, jf. artikel 58, stk. 7, litra d.

I de to førstnævnte tilfælde vil Sikkerhedsstyrelsen ligeledes kunne håndhæve reglerne over for henholdsvis producenter og udbydere, jf. artikel 58, stk. 7, litra a og b, i forordningen om cybersikkerhed. Som reaktionsmulighed foreslås det, at Sikkerhedsstyrelsen kan udstede forskellige påbud til en indehaver af en europæisk cybersikkerhedsattest eller en udsteder af en EU-overensstemmelseserklæring.

Der henvises til lovforslagets § 14 og de specielle bemærkninger hertil.

Som led i tilsynsopgaven skal Sikkerhedsstyrelsen også have hjemmel til at gennemføre audit hos såvel overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer, jf. artikel 58, stk. 8, litra b.

Der henvises til bemærkningerne til lovforslagets § 12 og de specielle bemærkninger hertil.

Som det andet område skal Sikkerhedsstyrelsen have forskellige beføjelser, hvis der i en konkret europæisk cybersikkerhedscertificeringsordning fastsættes specifikke og yderligere krav til overensstemmelsesvurderingsorganet end dem, der fremgår af bilaget til forordningen. Sikkerhedsstyrelsen skal som national certificeringsmyndighed kunne:

- Udstede certifikater i de tilfælde, hvor det fastsættes i en ordning, at et certifikat alene må udstedes af et offentligt organ, jf. forordningens artikel 56, stk. 5, jf. artikel 58, stk. 7, litra d.
- Bemyndige et overensstemmelsesvurderingsorgan, jf. forordningens artikel 60, stk. 3, hvis specifikke eller yderligere krav i en ordning gør det påkrævet, jf. artikel 54. stk. 1, litra f.
- Delegere opgaven med at udstede en europæisk cybersikkerhedsattest med tillidsniveauet højt til et overensstemmelsesvurderingsorgan, hvor dette fastsættes i en ordning, jf. forordningens artikel 56, stk. 6, litra b.

Som det tredje område skal Sikkerhedsstyrelsen behandle klager over de europæiske cybersikkerhedsattester og overensstemmelseserklæringer. Det drejer sig om følgende:

- Attester som styrelsen selv udsteder, jf. forordningens artikel 56, stk. 5, jf. artikel 58, stk. 7, litra f.
- Attester udstedt af et overensstemmelsesvurderingsorgan efter en generel bemyndigelse, jf. forordningens artikel 56, stk. 6, litra b, jf. artikel 58, stk. 7, litra f.
- Overensstemmelseserklæringer udstedt efter selvvurdering, jf. forordningens artikel 53, jf. artikel 58, stk. 7, litra f.

Til § 10

Det følger af artikel 58, stk. 8, litra a, i forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden skal kunne anmode overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer om at forelægge alle oplysninger, som er nødvendige for udførelsen af dens opgaver.

Det foreslås i *§ 10*, at Sikkerhedsstyrelsen kan fra enhver kræve alle oplysninger, som er nødvendige for udførelsen af opgaven som national cybersikkerhedscertificeringsmyndighed, herunder til afgørelse af, om et forhold falder ind under bestemmelserne i forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov og regler fastsat i medfør af denne lov.

Med bestemmelsen forpligtes enhver til efter anmodning at stille alle de oplysninger til rådighed for Sikkerhedsstyrelsen, som er nødvendige for at påse overholdelse af kravene i de nævnte retsakter. Alle oplysninger, der er nødvendige og kræves til udførelse af myndighedens opgaver inden for Sikkerhedsstyrelsens tre hovedområder, jf. bemærkningerne til § 7, er omfattet.

Sikkerhedsstyrelsen kan f.eks. kræve af indehavere og udstedere at få tilsendt dokumentation for en eller et IKT-produkt, -tjeneste eller -proces' udformning, fremstilling eller konstruktion, markedsføring, installation, konfiguration, anvendelse, drift og vedligeholdelse. Oplysningerne kan bl.a. også omfatte oplysninger om overensstemmelse, risiko- og sikkerhedsvurderinger, testresultater, fagtekniske vurderinger og oplysninger om, hvor mange eksemplarer, der er bragt i omsætning, hvordan og til hvem. Videre kan der, hvad angår overensstemmelsesvurderingsorganerne, være tale om dokumentation for uddannelse, løn, forsikring, ansættelsesvilkår, arbejdsgange, kvalitetsledelsessystemer, procedurer- og arbejdsprocesser.

I de nævnte tilfælde kan der være tale om behandling af personoplysninger. Det er Erhvervsministeriets vurdering, at denne behandling af oplysninger kan ske efter databeskyttelsesforordningens artikel 6, stk. 1, litra e, da behandlingen er nødvendig af hensyn til udførelsen af Sikkerhedsstyrelsens opgave som cybersikkerhedscertificeringsmyndighed.
Oplysningspligten er af væsentlig betydning for, at Sikkerhedsstyrelsen kan udføre et effektivt tilsyn. Vurderingen af, hvilke oplysninger der vil blive indhentet, vil altid bero på en proportionalitetsvurdering og karakteren af den dokumentation, der kan kræves, vil variere fra sag til sag. De oplysninger, Sikkerhedsstyrelsen vil kunne kræve, skal være relevante for den arbejdsopgave, Sikkerhedsstyrelsen varetager, og være tilgængelige for producenter og udbydere. Der er således ikke tale om, at Sikkerhedsstyrelsen kan kræve, at producenter og udbydere generer ny data og dokumentation. Udbydere og producenter kan ikke nægte at meddele Sikkerhedsstyrelsen

oplysningerne under henvisning til, at der er tale om forretningshemmeligheder. De almindelige bestemmelser om tavshedspligt for offentligt ansatte i straffelovens 16. kapitel finder anvendelse.

Sikkerhedsstyrelsen har ansvaret for, at oplysningerne behandles på en forsvarlig og korrekt måde. Dette gælder således for alle slags oplysninger, der behandles, herunder f.eks. personoplysninger og forretningshemmeligheder. Det gælder også, hvis der er tale om klassificeret information, hvor en særlig sikkerhedsbeskyttelse af informationen er påkrævet. I så fald er Sikkerhedsstyrelsen forpligtet til at kunne sikkerhedsbeskytte den klassificerede information, jf. nærmere Justitsministeriets cirkulære af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.

Endelig skal oplysningerne, der modtages i henhold til bestemmelsen, som udgangspunkt indsendes digitalt, jf. lovforslagets § 18, og eventuelt inden for en nærmere angivet tidsfrist.

Til § 11

Det følger af artikel 58, stk. 8, litra c, i forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden i overensstemmelse med national ret skal kunne træffe passende foranstaltninger til at sikre, at overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer overholder bestemmelserne i denne forordning eller en europæisk cybersikkerhedscertificeringsordning.

Det foreslås i *§ 11, stk. 1*, at Sikkerhedsstyrelsen kan udtage ethvert IKT-produkt, -tjeneste eller -proces, som omfattes af en europæisk cybersikkerhedscertificeringsordning i medfør af forordningen om cybersikkerhed, med henblik på at lave en teknisk undersøgelse.

Udtagelse foregår uden betaling. Muligheden for at udtage et produkt, tjeneste eller proces gælder sideløbende med den dokumentkontrol, der er hjemlet i lovforslagets § 9, og hvor den ledsagende dokumentation og andre formelle krav til produktet, tjenesten og processen kontrolleres. Det kan i særlige tilfælde vise sig nødvendigt, at udvælge, udtage og visuelt og/eller

teknisk at inspicere et IKT-produkt, -tjeneste eller -proces, herunder foranledige en hel eller delvis test af produktet for derved at konstatere, om produktet overholder kravene i den europæiske cybersikkerhedsattest.

I *§ 11, stk. 2*, foreslås det, at Sikkerhedsstyrelsen har adgang til direkte rådgivning og anden bistand fra Center for Cybersikkerhed om sikkerhedsmæssige spørgsmål.

Center for Cybersikkerhed under Forsvarsministeriet er som national it-sikkerhedsmyndighed det nationale kompetencecenter på cybersikkerhedsområdet og råder over ekspertise, kompetencer og personale med særlige kvalifikationer, som ikke er en del af Sikkerhedsstyrelsens organisation. Der udarbejdes efter lovforslagets vedtagelse en formel samarbejdsaftale mellem Sikkerhedsstyrelsen og Center for Cybersikkerhed om faglig bistand og rådgivning i forbindelse med Sikkerhedsstyrelsens tilsyns- og kontrolopgave, herunder undersøgelse af udtagne produkter, tjenester og processer.

Til § 12

Det følger af artikel 58, stk. 8, litra b, i forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden skal kunne udføre undersøgelser i form af audit af overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer med henblik på at verificere deres overholdelse af afsnit III om rammebestemmelser for cybersikkerhedscertificering i forordningen om cybersikkerhed.

Det foreslås i *§ 12,* at Sikkerhedsstyrelsen kan auditere overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer med henblik på at verificere overholdelse af forordningen om cybersikkerhed og regler fastsat i medfør af forordningen.

Med bestemmelsen kan Sikkerhedsstyrelsen dermed foretage audit i overensstemmelse med det anførte i forordningens artikel 58, stk. 8, litra b. Det præciseres ikke nærmere i forordningen, hvad audit indebærer.

Ved auditbesøg efterprøver Sikkerhedsstyrelsen, om såvel overensstemmelsesvurderingsorganer, indehavere og udstedere anvender og efterlever de principper og rammebestemmelser, der er anført i afsnit III i forordningen

om cybersikkerhed. Audits foretages med passende intervaller, der ud fra en konkret vurdering kan fastsættes til f.eks. at være årlige eller halvårlige.

Overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer skal berigtige de afvigelser, som Sikkerhedsstyrelsen konstaterer, ved korrigerende handlinger, og Sikkerhedsstyrelsen skal verificere resultatet af de korrigerende handlinger. Hvis Sikkerhedsstyrelsen efterfølgende konstaterer, at der ikke er fulgt op på anmærkningen med en handling inden for en fastsat frist, vil det føre til en afvigelse, som videregives til DANAK, jf. forordningens artikel 58, stk. 7, litra c.

Til § 13

Det følger af artikel 58, stk. 8, litra d, i forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden skal kunne få adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller indehavere af en europæisk cybersikkerhedsattest med henblik på at udføre undersøgelser i overensstemmelse med EU-retten eller medlemsstaternes processuelle regler.

Det foreslås i § *13, stk. 1*, at Sikkerhedsstyrelsen til enhver tid mod behørig legitimation og uden retskendelse har adgang til alle lokaler hos overensstemmelsesvurderingsorganer eller indehavere af en europæisk cybersikkerhedsattest med henblik på at føre kontrol efter lovens kapitel 4. Det foreslås i *stk. 2*, at Sikkerhedsstyrelsen kan være bistået af en eller flere uafhængige sagkyndige i forbindelse med adgangen efter stk. 1.

Det er kun muligt for Sikkerhedsstyrelsen at anvende bestemmelsen i § 13 til at tilvejebringe oplysninger til brug for et tilsyn. Det betyder, at bestemmelsen kan anvendes med henblik på at konstatere, om overensstemmelsesvurderingsorganer og indehavere af en europæisk cybersikkerhedsattest agerer i overensstemmelse med reglerne og lever op til deres forpligtelser. Det skal således være formålet med adgangen, at der skal indhentes oplysninger, der er nødvendige for selve tilsynet.

Adgangshjemlen gælder både i relation til proaktive kontroller, hvor Sikkerhedsstyrelsen har planlagt tilsynsopgaven på forhånd, og reaktive tilsynsopgaver, som oftest sker efter en udefrakommende begivenhed, som f.eks. en klage over en attest eller en EU-overensstemmelseserklæring. Anvendelsen af bestemmelsen skal ske under hensyntagen til bestemmelserne i lovbekendtgørelse nr. 1121 af 12. november 2019 om retssikkerhed ved

forvaltningens anvendelse af tvangsindgreb og oplysningspligter, herunder reglerne om fravigelse af varsling af tilsyn, jf. § 5, stk. 4-7.

Sikkerhedsstyrelsen kan anvende den foreslåede bestemmelse, hvis det skønnes nødvendigt for at føre et effektiv tilsyn, uden der på forhånd er en konkret formodning om, at attester eller EU-overensstemmelseserklæring ikke er i overensstemmelse med reglerne. For at Sikkerhedsstyrelsen kan føre et effektivt tilsyn, er det nødvendigt at få adgang til steder, hvor myndigheden ikke på forhånd ved, at der er ikke-overensstemmende IKT-produkter, -tjenester eller -processer. På den måde bliver tilsynet med certificeringen udført på baggrund af en risikobaseret tilgang til indsamlet data og kvalificering af risikobilledet, så tilsynet kan sættes ind der, hvor der er størst risiko for f.eks. kompromittering af cybersikkerheden og tilrettelægges så effektivt som muligt.

Om det er nødvendigt at føre tilsyn på lukkede lokaliteter, f.eks. producenters fabrikations-, salgs- eller lagerlokaler m.v. vil afhænge bl.a. afhænge af, om Sikkerhedsstyrelsen ellers vil kunne få et tilstrækkeligt retvisende billede af regelefterlevelsen. Derudover indgår en vurdering af, om det er muligt at skaffe oplysningerne på anden måde, om det er nødvendigt, at myndigheden umiddelbart selv kan udvælge de områder, som tilsynet skal dække, herunder dokumentationen herfor, eller om det er tilstrækkeligt, at den producenten eller udbyderen udvælger og eventuelt fremsender dokumentationen.

Det indgår derfor også i vurderingen, om den fremsendte dokumentation må anses for at være dækkende og repræsentativ til at foretage en vurdering af, om reglerne er opfyldt. Er dette ikke tilfældet kan det være nødvendigt for Sikkerhedsstyrelsen at få adgang til de steder, hvor et IKT-produkt, -tjeneste eller -proces er tilgængeligt for at kunne foretage en fyldestgørende vurdering. Endelig vil det indgå i vurderingen, hvordan tilsynet udføres mest effektivt. Der er her tale om en proportionalitetsafvejning.

Hvis det ud fra en samlet betragtning af bl.a. ovenstående elementer vurderes, at det vil være nødvendigt at føre tilsyn på ikke-offentligt tilgængelige lokaliteter, vil Sikkerhedsstyrelsen således kunne anvende bestemmelsen. Hvis det derimod ikke skønnes at være nødvendigt, herunder proportionalt med det Sikkerhedsstyrelsen vil opnå ved at få adgang til de pågældende lokaler, vil bestemmelsen ikke kunne anvendes. Sikkerhedsstyrelsen vil i sådanne tilfælde alene kunne føre varslede tilsyn, jf. § 5, stk. 1-3, i lovbe-

kendtgørelse om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter, føre tilsyn på de steder, der er offentligt tilgængelige, eller bede om at få tilsendt dokumentation, jf. lovforslagets § 10.

Til § 14

Det følger af artikel 58, stk. 8, litra c, i forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden i overensstemmelse med national ret skal kunne træffe passende foranstaltninger til at sikre, at overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer overholder bestemmelserne i denne forordning eller en europæisk cybersikkerhedscertificeringsordning.

Det følger af artikel 58, stk. 8, litra f, at cybersikkerhedscertificeringsmyndigheden skal kunne pålægge sanktioner i overensstemmelse med national ret, jf. forordningens artikel 65, og at kunne kræve øjeblikkeligt ophør af overtrædelser af de forpligtelser, der er fastsat i denne forordning.

Det foreslås i *§ 14*, at Sikkerhedsstyrelsen kan udstede påbud til en indehaver af en europæisk cybersikkerhedsattest eller en udsteder af en EU-overensstemmelseserklæring, der har bragt en eller et IKT-produkt, -tjeneste eller -proces i omsætning, som ikke i overensstemmelse med forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov og regler fastsat i medfør af denne lov.

Der kan udstedes påbud om en række foranstaltninger, som fremgår af bestemmelsens nr. 1-4. Det foreslås i *nr. 1*, at Sikkerhedsstyrelsen kan udstede påbud om at gøre brugerne opmærksomme på risici. Det foreslås i *nr. 2*, at Sikkerhedsstyrelsen kan udstede påbud om at standse markedsføring, der kan vildlede brugerne. Det foreslås i *nr. 3*, at Sikkerhedsstyrelsen kan udstede påbud om afhjælpe forhold, som ikke er i overensstemmelse med reglerne. Det foreslås i *nr. 4*, at Sikkerhedsstyrelsen kan udstede påbud om at standse salg, levering eller udbud af produktet, tjenesten eller processen.

De fire reaktionsmuligheder kan benyttes enkeltvis, men bestemmelsen er formuleret, så de mindst indgribende foranstaltninger nævnes først, mens de mest indgribende nævnes til sidst. I overensstemmelse med det forvaltningsretlige proportionalitetsprincip bør der ikke bruges mere indgribende foranstaltninger end nødvendigt for at opnå formålet. Afhængigt af omfanget og

karakteren af regelbruddet, kan bestemmelserne anvendes på samme tid for at sikre, at der træffes den mest effektive foranstaltning.

I nogle tilfælde er det tilstrækkeligt at informere brugerne om de risici, der er ved en eller et IKT-produkt, -tjeneste eller -proces, der er bragt i omsætning, og som ikke opfylder de krav, der stilles.

Bestemmelsen i nr. 1 vedrører IKT-produkter, -tjenester eller -processer, hvor der er risiko for, at cybersikkerheden kompromitteres, herunder navnlig risiko for, at fortroligheden af data, der er lagret, overført eller behandlet, er brudt eller på anden vis ladt ubeskyttet. Bestemmelsen kan dermed anvendes i tilfælde, hvor det ses som en passende reaktion, at en indehaver eller en udsteder forpligtes til at oplyse, at brug af varen er behæftet med risici. Informationen kan f.eks. gives på hjemmesider og apps, der sælger/udbyder/anvender produktet, tjenesten eller processen eller på anden måde, som myndigheden måtte finde nødvendig for at oplyse brugerne om risikoen. Der kan være tale om bl.a. at angive relevante sikkerhedsforanstaltninger, der skal udøves af brugeren. Der kan opstå behov for at anvende andre kanaler for meddelelse af informationen, end det normalt vil være tilfældet, for at sikre at den når ud til modtagergruppen. Målgruppen er efter denne bestemmelse brugerne af produktet, tjenesten eller processen og omfatter ikke information til andre led i en forhandlingskæde.

Efter bestemmelsen i nr. 2 kan Sikkerhedsstyrelsen påbyde at stoppe markedsføring, der kan vildlede brugerne. Bestemmelsen skal sikre, at det er muligt at hindre fortsat markedsføring af et IKT-produkt, -tjeneste eller -proces, der ikke er i overensstemmelse med de gældende regler. Markedsføring forstås i den henseende som reklame, kampagne, emballering, udstilling m.v., og som kan give brugere og andre erhvervsdrivende et fejlagtigt indtryk af, at produktet, tjenesten eller processen er i overensstemmelse med reglerne, hvis det fortsat markedsføres med en attest, mærkat, erklæring eller lignende, afhængigt af den pågældende certificeringsordning. For så vidt angår påbud om at stoppe tilgængeliggørelsen af IKT-produkter, -tjenester eller -processer på markedet henvises til nr. 4.

Efter bestemmelsen i nr. 3 kan Sikkerhedsstyrelsen træffe afgørelse om at afhjælpe forhold, som ikke er i overensstemmelse med reglerne. Dette gælder både afhjælpning af forhold vedrørende en europæisk cybersikkerhedsattest eller en EU-overensstemmelseserklæring. Det vil være relevant at kræve afhjælpning i situationer, hvor det efter en proportionalitetsvurdering

ikke findes hensigtsmæssigt, eksempelvis at standse salg, levering eller udbud af produktet, tjenesten eller processen, og hvis fejlen kan afhjælpes på en mindre indgribende måde. Afhjælpning kan både ske ved, at det tilbydes brugeren, at manglen på produktet afhjælpes af indehaveren eller udstederen, eller ved at brugeren selv foretager en udskiftning af enkle dele for at opnå den fornødne sikkerhed. Denne løsning er som udgangspunkt egnet til ukomplicerede afhjælpninger. Det er indehaveren eller udstederen, som afholder udgifterne til udbedring af manglerne ved produktet, tjenesten eller processen. Påbud om afhjælpning kan både være relevant over for produkter, tjenester eller processer, som allerede er solgt til brugeren, og over for, produkter, tjenester eller processer, som er videresolgt til andre erhvervsdrivende i en omsætningskæde og/eller varer, der befinder sig på et lager.

Efter bestemmelsen i nr. 4 kan indehavere eller udstedere påbydes at stoppe salg, levering eller udbud. Forbud mod salg angår de produkter, tjenester eller processer, som indehaveren eller udstederen fortsat har rådighed over og vedrører altså ikke de produkter, tjenester eller processer, som allerede er omsat og indgår i en omsætningskæde, f.eks. de distributører og detailbutikker, som et produkt måtte være solgt til. Der er altså ikke tale om hverken traditionelt tilbagekald, hvor varen tilbagekaldes fra den endelige bruger eller traditionel tilbagetrækning, hvor en vare fjernes fra markedet og handelskæden, inden det når ud til slutbrugeren.

I situationer hvor producenter og udbydere selv sælger, leverer eller udbyder produktet, tjenesten eller processen, vil salgstoppet i særdeleshed være relevant, da produktet, tjenesten eller processen afsættes direkte til brugeren. Påbuddet kan rette sig mod indehaveren af en europæisk cybersikkerhedsattest eller den, der har udstedt en EU-overensstemmelseserklæring.

Muligheden for at give et påbud efter § 14 retter sig ikke mod overensstemmelsesvurderingsorganer, men alene mod indehavere og udstedere af attester, selvom overensstemmelsesvurderingsorganer er specifikt nævnt i forordningens artikel 58, stk. 8, litra c. De foranstaltninger, der skal anvendes, skal ifølge denne bestemmelse i forordningen være i overensstemmelse med national ret, og der findes allerede i dansk ret en række regelfastsatte sanktionsmuligheder over for disse organer.

I medfør af § 16, stk. 1, i lov nr. 1518 af 18. december 2018 om erhvervsfremme, som senest ændret ved lov nr. 796 af 9. juni 2020, har erhvervsministeren fastsat regler om udpegning af et nationalt akkrediteringsorgan og

dets opgavevaretagelse, som er nødvendige for anvendelsen af Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om bl.a. kravene til akkreditering. I bekendtgørelse nr. 913 af 25. september 2009 om akkreditering af virksomheder er der i kapitel 3 fastsat nærmere regler om tilsyn med akkrediterede virksomheder, herunder suspendering og ophør af akkrediteringen. Som følge heraf er der efter Erhvervsministeriets opfattelse allerede i dansk ret et etableret system og fuldt ud fyldestgørende grundlag for at træffe passende foranstaltninger over for akkrediterede virksomheder – og dermed også overensstemmelsesvurderingsorganer – som ikke overholder reglerne.

Hvis forudsætningerne for, at et overensstemmelsesvurderingsorgan ikke kan opretholde en akkreditering inden for cybersikkerhedscertificering er tilstede, vil det derfor være DANAK, der skal vurdere og håndtere de konstaterede afvigelser. I denne proces vil også de afvigelser, som måtte være konstateret af Sikkerhedsstyrelsen indgå.

Der henvises til bemærkningerne til lovforslagets § 12.

Til § 15

Det følger af artikel 58, stk. 8, litra e, i forordningen om cybersikkerhed, at cybersikkerhedscertificeringsmyndigheden i overensstemmelse med national ret skal kunne tilbagekalde europæiske cybersikkerhedsattester, der er udstedt af de nationale cybersikkerhedscertificeringsmyndigheder eller europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med forordningens artikel 56, stk. 6, hvis sådanne attester ikke overholder bestemmelserne i forordningen eller i en europæisk cybersikkerhedscertificeringsordning.

Det foreslås i *§ 15*, at Sikkerhedsstyrelsen kan tilbagekalde en europæisk cybersikkerhedsattest, hvis en indehaver af en attest ikke samarbejder med Sikkerhedsstyrelsen om tilsyn, eller hvis indehaveren af en attest gentagne gange eller ved grov forsømmelse overtræder denne lov, regler fastsat i medfør af denne lov, forordningen om cybersikkerhed eller regler udstedt i medfør af forordningen. De nærmere reaktionsmuligheder fremgår af bestemmelsens nr. 1-4 og behandles nedenfor.

Samarbejde med tilsynsmyndighederne er det generelle udgangspunkt for de erhvervsdrivende, som bringer alle slags produkter, tjenester og processer i omsætning på det danske marked. Det er helt essentielt, at erhvervsdrivende handler ansvarligt og lever op til de forpligtelser, de er underlagt. Også indenfor cybersikkerhed er villigheden til at stille oplysninger til rådighed og sikre transparens om kvalitet afgørende for brugernes tillid til udbydere af digitale tjenester og til selve det digitale indre marked. Der skal derfor være en konsekvens af unddrage sig dette samarbejde, da et effektivt tilsyn fra myndighedernes side i høj grad er baseret på de erhvervsdrivendes samarbejde.

Det foreslås i *nr. 1*, at en europæisk cybersikkerhedsattest kan tilbagekaldes, hvis en indehaver ikke imødekommer Sikkerhedsstyrelsens anmodning om oplysninger, jf. § 10. Dermed sanktioneres indehaveren af en attest, hvis vedkommende undlader at indsende eller udlevere de oplysninger, som er nødvendige for, at Sikkerhedsstyrelsen kan gennemføre tilsyn, jf. lovforslagets § 9. Det er væsentligt for Sikkerhedsstyrelsens mulighed for at kunne tage stilling til, om IKT-produkter, -tjenester og -processer er overensstemmende med reglerne, at den ønskede dokumentation stilles til rådighed uden unødig forsinkelse. Modtager Sikkerhedsstyrelsen ikke de krævede oplysninger, kan det hindre myndigheden i at udøve effektivt tilsyn. Det er derfor nødvendigt, at tilsidesættelse af denne pligt kan sanktioners med et tilbagekald af attesten af hensyn til den præventive effekt.

Det foreslås i *nr. 2*, at en europæisk cybersikkerhedsattest kan tilbagekaldes, hvis en indehaver nægter at give Sikkerhedsstyrelsen adgang, jf. § 13. Dermed sanktioneres det, hvis en attestindehaver undlader at give Sikkerhedsstyrelsen adgang til alle erhvervsmæssige lokaliteter, hvor der er oplysninger om IKT-produkter, -tjenester og -processer, som er omfattet af anvendelsesområde for forordningen om cybersikkerhed.

Det foreslås i *nr. 3*, at en europæisk cybersikkerhedsattest kan tilbagekaldes, hvis et påbud fra Sikkerhedsstyrelsen ikke efterkommes, jf. § 14. En indehaver af en europæisk cybersikkerhedsattest kan derfor mødes med en sanktion, hvis Sikkerhedsstyrelsens afgørelser ikke efterleves. Et tilbagekald af en attest i denne situation skal være med til at sikre regelefterlevelsen blandt attestindehaverne og være med til at understøtte effektiviteten i tilsynet med IKT-produkter, -tjenester og -processer.

Det foreslås i *nr. 4*, at gentagne og grove forsømmelser ligeledes kan afstedkomme et tilbagekald af en europæisk cybersikkerhedsattest. Når grovheden

skal fastsættes kan det inddrages, om overtrædelsen har fremkaldt fare for sikkerhed, sundhed eller miljø eller om overtrædelsen er begået som led i en systematisk overtrædelse af reglerne. Ligeledes kan det tillægges vægt, om der er tilsigtet en berigelse i forbindelse med overtrædelsen. Det vil bero på Sikkerhedsstyrelsens konkrete vurdering af hver enkelt sag. Gentagne overtrædelser omhandler de tilfælde, hvor en attestindehaver inden for de seneste år har begået en anden overtrædelse. Overtrædelserne behøver ikke være identiske. Hvis Sikkerhedsstyrelsen eksempelvis tidligere har udstedt flere påbud til attestindehaveren, jf. lovforslagets § 14, vil dette være at betragte som en gentagelse. Der er altså tale om, at Sikkerhedsstyrelsen flere gange har behandlet sager, hvor den pågældende indehaver af en attest har vist sig ikke at optræde i overensstemmelse med reglerne.

Tilbagekald af et cybersikkerhedscertifikat ugyldiggør et certifikat før det planlagte udløb af gyldighedsperioden. Det betyder, at producenten eller indehaveren må ansøge på ny, hvis virksomheden på et senere tidspunkt igen opfylder kriterierne for at få et certifikat.

Tilbagekald vil ikke have betydning for gyldigheden af certifikatet inden tilbagekaldet. Ved tilbagekald skal producenter og udbydere af et certificeret IKT-produkter øjeblikkeligt afbryde al brug af certifikatet. Certifikatet kan ikke gøres gyldigt igen, når det først er tilbagekaldt.

I overensstemmelse med de principper, der er nævnt i lovforslagets § 14 om Sikkerhedsstyrelsens mulighed for at udstede påbud, fordres det, at en attestindehaver i forbindelse med et tilbagekald af en attest af egen drift iværksætter et eller flere tiltag. Det vil sige, at (slut)brugerne af en eller et IKT-produkt, -tjeneste eller -proces i relevant omfang informeres om, at attesten er tilbagekaldt. Informationen kan gives som en generel information på hjemmesider og apps, der sælger, udbyder eller anvender produktet, tjenesten eller processen. Er produktet, tjenesten eller processen videregivet til distributør inden for EU, som enten sælger produktet, tjenesten eller processen videre til forhandlere eller direkte til brugerne, skal disse distributører på samme vis informeres. Dette skal ske som en specifik information rettet direkte til den enkelte aftager og som sætter den pågældende distributør i stand til enten at videregive information til forhandlere eller til slutbrugerne.

På samme vis skal indehaveren af en tilbagekaldt attest standse al markedsføring, der kan vildlede brugerne. Det vil sige, at salg, levering, distribution eller udbud af produktet, tjenesten eller processen som certificeret skal af-

brydes fra den dato, hvor tilbagekaldet er dateret. Herudover skal indehaveren af en tilbagekaldt attest i det omfang, det er muligt, tilbyde brugeren, at den mangel, der har afstedkommet tilbagekaldet, afhjælpes.

Til § 16

Ifølge artikel 58, stk. 7, litra f, skal de nationale cybersikkerhedscertificeringsmyndigheder behandle klager fra fysiske eller juridiske personer i forbindelse med europæiske cybersikkerhedsattester udstedt af de nationale cybersikkerhedscertificeringsmyndigheder eller med europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med artikel 56, stk. 6, eller i forbindelse med EU-overensstemmelseserklæringer udstedt i henhold til artikel 53.

Det følger af forordningens artikel 63, stk. 1, at fysiske og juridiske personer har ret til at klage til udstederen af en europæisk cybersikkerhedsattest eller, når klagende vedrører en cybersikkerhedsattest udstedet af et overensstemmelsesvurderingsorganer i overensstemmelse med artikel 56, stk. 6, til den relevante cybersikkerhedscertificeringsmyndighed.

Udgangspunktet er således, at en klage skal indgives til udstederen af attesten, hvilket i de fleste tilfælde vil være overensstemmelsesvurderingsorganerne.

Det foreslås i *§ 16,* at Sikkerhedsstyrelsen behandler klager over afgørelser vedrørende bestemte typer af klager over bestemte attester, afhængigt af hvem der har udstedt attesterne.

Det foreslås på den baggrund i *nr. 1*, at Sikkerhedsstyrelsen skal behandle klager over EU-overensstemmelseserklæringer udstedt af producenter og udbydere af IKT-produkter, -tjenester og -processer i henhold til artikel 53 i forordningen om cybersikkerhed.

Det foreslås i *nr. 2*, at Sikkerhedsstyrelsen skal behandle klager over europæiske cybersikkerhedsattester udstedt af den nationale cybersikkerhedscertificeringsmyndighed. Efter artikel 56, stk. 5, er dette tilfældet, hvis det fastsættes i en specifik europæisk cybersikkerhedscertificeringsordning.

Det foreslås i *nr. 3*, at Sikkerhedsstyrelsen skal behandle klager over europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsor-

ganer i overensstemmelse med artikel 56, stk. 6, i forordningen om cybersikkerhed. Det følger heraf, at hvis det fastsættes i en specifik europæisk cybersikkerhedscertificeringsordning, som indeholder krav om tillidsniveau højt, skal den cybersikkerhedsattesten udstedes af en national cybersikkerhedscertificeringsmyndighed eller af et overensstemmelsesvurderingsorgan, hvis attesten enten forhåndsgodkendes i hvert enkelt tilfælde eller opgaven delegeres til organet.

Fælles for nr. 2 og 3 er, at Sikkerhedsstyrelsen skal behandle klager over en attest, som styrelsen mere eller mindre er direkte involveret i udstedelsen af; enten som direkte afsender eller på baggrund af en generel delegation, jf. § lovforslagets 7.

Der er alene i forordningen om cybersikkerhed vedtaget en bestemmelse om, at den nationale cybersikkerhedscertificeringsmyndigheds udstedelse af europæiske cybersikkerhedsattester omhandlet i artikel 56, stk. 5, litra a, og artikel 56, stk. 6, skal være strengt adskilt fra myndighedens tilsynsaktiviteter, og aktiviteterne skal udføres uafhængigt af hinanden, jf. artikel 58, stk. 4.

I forordningen er der derimod ikke et krav om, at den nationale cybersikkerhedscertificeringsmyndigheds udstedelse af attester holdes adskilt fra myndighedens behandling af klager, ligesom der ikke i forordningen er et krav om, at den nationale cybersikkerhedscertificeringsmyndigheds tilsyn skal holdes adskilt fra myndighedens klagebehandling.

I overensstemmelse med forordningens artikel 58, stk. 7, litra f, og artikel 63, stk. 1, indebærer bestemmelsen derfor, at Sikkerhedsstyrelsen kan behandle klager, hvor styrelsen i sin egenskab af cybersikkerhedscertificeringsmyndighed har udstedt en cybersikkerhedsattest eller delegeret kompetencen hertil til et overensstemmelsesvurderingsorgan.

Sikkerhedsstyrelsen vil ved behandlingen af klager i medfør af lovforslagets § 16 fungere som egentlig klageinstans og vil ikke med hjemmel i denne bestemmelse have kompetence til af egen drift at iværksætte undersøgelser af f.eks. producenter og udbyderes, der har udfærdiget en overensstemmelseserklæring. Det skyldes, at en sådan rolle varetages af Sikkerhedsstyrelsen som led i styrelsens rolle som tilsynsmyndighed, jf. lovforslagets § 8. Den viden, som Sikkerhedsstyrelsen indsamler på baggrund af de modtagne kla-

ger, kan fremover få betydning for Sikkerhedsstyrelsens udvælgelse af tilsynstemaer over for de producenter og udbydere, der foretager selvvurdering.

Klagen vil danne rammen for den undersøgelse af sagen, som Sikkerhedsstyrelsen foretager i overensstemmelse med officialprincippet, og for Sikkerhedsstyrelsens afgørelse. Sikkerhedsstyrelsen skal som følge af officialprincippet sikre, at sagen er tilstrækkeligt oplyst, herunder at det fornødne cybersikkerhedsfaglige grundlag foreligger, inden der træffes afgørelse i sagen. Der forudsættes det, at Sikkerhedsstyrelsen alene kan tage stilling til om gældende regler er opfyldt – med udgangspunkt i klagens tema.

Det er ikke muligt på forhånd at angive, i hvilke tilfælde Sikkerhedsstyrelsen vil komme frem til, at gældende regler er overtrådt. Vurderingen heraf kan - ud over en ren juridisk bedømmelse - forudsætte et vist it-fagligt skøn. Dette skøn, herunder specifikke vurderinger af cybersikkerheden, vil fordre, at Sikkerhedsstyrelsen sikrer sig, at den fornødne faglige viden er til stede ved styrelsens behandling af klagesagerne. Sikkerhedsstyrelsen vil i den forbindelse i fornødent omfang inddrage sagkyndige bistand.

Sikkerhedsstyrelsen er ved behandlingen af enkelte klagesager ikke undergivet instruktion om de enkelte sagers behandling og afgørelse. Med en klageadgang til Sikkerhedsstyrelsen sikres uvildige afgørelser. Sikkerhedsstyrelsen træffer endelige administrative afgørelser. Sikkerhedsstyrelsen vil dog ligesom andre offentlige myndigheder være undergivet kontrol af Folketingets Ombudsmand, ligesom afgørelserne vil kunne indbringes for domstolene efter de civilretlige regler herom.

Lovforslaget indebærer, at en klage over en overensstemmelsesvurderingserklæring, jf. forordningens artikel 53, en europæisk cybersikkerhedsattest udstedt af Sikkerhedsstyrelsen efter artikel 56, stk. 5, litra a, eller en europæiske cybersikkerhedsattest udstedt af overensstemmelsesvurderingsorganer i overensstemmelse med forordningens artikel 56, stk. 6, efter en bemyndigelse, kan behandles samtidigt med, at Sikkerhedsstyrelsen fører tilsyn med samme udsteder eller selvvurderende producent eller udbyder.

Til § 17

Det foreslås i *§ 17,* at Sikkerhedsstyrelsens afgørelser i egenskab af national cybersikkerhedscertificeringsmyndighed ikke kan indbringes for anden administrativ myndighed.

Bestemmelsen afskærer klageadgangen fra kontrolmyndigheden til Erhvervsministeriets departement eller andre administrative myndigheder. Udførelsen er opgaven som national cybersikkerhedscertificeringsmyndighed kræver en ikke ubetydelig og faglig indsigt i området. Denne indsigt findes som udgangspunkt hos Sikkerhedsstyrelsen selv.

Samtidig følger det af artikel 58, stk. 7, litra f, i forordningen om cybersikkerhed, at myndigheden skal behandle klager vedrørende cybersikkerhedsattester udstedt af myndigheden selv, visse cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer, hvor myndigheden har forhåndsgodkendt attesten eller delegeret kompetencen til udstedelse, eller vedrørende EU-overensstemmelseserklæringer på baggrund af producenten eller udbyderens selvvurdering.

Derudover følger det af forordningens artikel 63, at fysiske og juridiske personer har ret til at klage til udstederen af en europæisk cybersikkerhedsattest eller til cybersikkerhedscertificeringsmyndigheden, hvis der er tale om en attest, hvor myndigheden har forhåndsgodkendt attesten eller delegeret kompetencen til udstedelse.

Der henvises til bemærkningerne til lovforslagets § 16.

Endelig regulerer forordningens artikel 64 fysiske og juridiske personers ret til effektive retsmidler. Adgangen til effektive retsmidler følger af de almindelige betingelser for domstolsprøvelse i dansk ret.

En afskæring af den administrative klageadgang findes på baggrund af en samlet vurdering at være i overensstemmelse med de almindelige forvaltningsretlige principper, og vurderes dermed ikke at have retssikkerhedsmæssige konsekvenser.

Til § 18

Det forhold, at forordningen om cybersikkerhed for så vidt fastsættelsen af bestemmelser om cybersikkerhedscertificering er ny, bevirker, at der ikke på nuværende tidspunkt eksisterer gældende ret, som dækker samme område.

Det foreslås i *§ 18, stk. 1*, at skriftlig kommunikation til og fra Sikkerhedsstyrelsen om forhold, som er omfattet af forordningen om cybersikkerhed og denne lov, skal foregå digitalt.

Det foreslås i *stk. 2*, at Sikkerhedsstyrelsen uanset stk. 1 kan bestemme, at skriftlig kommunikation skal foregå på anden vis, hvis det er påkrævet efter omstændighederne.

Bestemmelsen understøtter princippet om digital kommunikation, som er et af de syv principper for digitaliseringsklar lovgivning. Derfor er det som udgangspunkt obligatorisk med digital skriftlig kommunikation til og fra Sikkerhedsstyrelsen, medmindre særlige forhold taler herfor. Efter omstændighederne kan der således opstå tilfælde, hvor digital kommunikation ikke bør anvendes.

Det foreslås i *stk. 3*, at erhvervsministeren kan fastsætte nærmere regler om digital kommunikation og om anvendelse af bestemte it-systemer, særlige digitale formater eller lignende.

Bestemmelsen vedrører kommunikationsmåden i forbindelse med kommunikation til og fra Sikkerhedsstyrelsen om alle forhold, der er omfattet af forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, lovforslaget og regler fastsat i medfør af lovforslaget.

På sigt kan det komme på tale at udvikle digitale løsninger, herunder selvbetjeningsløsninger til brug for kommunikation om forhold, som er omfattet af forordningen om cybersikkerhed, loven eller regler fastsat i medfør af forordningen eller loven. Det foreslås derfor, at erhvervsministeren kan fastsætte nærmere regler herom administrativt. Erhvervsministerens anvendelse af bemyndigelsen vil ske 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 en digital meddelelse anses for at være kommet frem på det tidspunkt, hvor meddelelsen er tilgængelig for adressaten i postløsningen.

Bestemmelsen fastsættes for at tydeliggøre, hvornår en meddelelse anses for at være kommet frem. Bestemmelsen stemmer overens med § 10 i lov om Digital Post fra offentlige afsendere.

Til § 19

Det forhold, at forordningen om cybersikkerhed for så vidt fastsættelsen af bestemmelser om cybersikkerhedscertificering er ny, bevirker, at der ikke på nuværende tidspunkt eksisterer gældende ret, som dækker samme område.

Det foreslås i *§ 19*, at erhvervsministeren 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 cybersikkerhed, eller regler, som er nødvendig for at anvende de af Den Europæiske Union udstede retsakter på forordningens område.

Det foreslås hermed, at erhvervsministeren bemyndiges til at fastsætte de nødvendige administrative bestemmelser til opfyldelse af de gennemførelsesforanstaltninger, som Kommissionen måtte vedtage efter proceduren i henhold til forordningens artikel 66, jf. nærmere artikel 49, stk. 7, om udarbejdelsen af visse europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester og -processer, artikel 59, stk. 5, om peerreview-ordninger for nationale cybersikkerhedscertificeringsordninger og artikel 61, stk. 5, om den nationale certificeringsmyndigheds anmeldelser til Kommissionen af overensstemmelsesvurderingsorganer.

Af bestemmelsen følger det endvidere, at erhvervsministeren kan fastsætte regler, som er nødvendige for at anvende de af unionen udstedte retsakter på området for forordningen om cybersikkerhed.

Til § 20

Det fremgår af artikel 69, stk. 2, i forordningen om cybersikkerhed, at artikel 58, 60, 61, 63, 64 og 65 finder anvendelse fra den 28. juni 2021.

Det foreslås i *§ 20*, at loven træder i kraft den 28. juni 2021.

Bestemmelsen skal ses i lyset af, at forordningen om cybersikkerhed finder endelig anvendelse – og at dansk lovgivning dermed skal være i overensstemmelse hermed – fra denne dato.

Til § 21

Bestemmelsen vedrører lovens territoriale gyldighed.

Det foreslås i *§ 21*, at loven ikke skal gælde for Færøerne og Grønland.

Forordningen om cybersikkerhed finder ikke anvendelse for Færøerne og Grønland, der ikke er medlem af EU. Hvis bestemmelser svarende til forordningen om cybersikkerhed skal gennemføres for Færøerne og Grønland, vil det skulle ske ved lov. Da lovforslaget er en supplerende lov til forordningen findes det mest hensigtsmæssigt, at de supplerende bestemmelser sættes i kraft ved lov sammen med forordningen.