Lovtidende A

2021

Udgivet den 5. maj 2021

4. maj 2021. Nr. 780.

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. 526/2013 (forordningen om cybersikkerhed) (lov om cybersikkerhedscertificering)[1)]

VI MARGRETHE DEN ANDEN, af Guds Nåde Danmarks Dronning, gør vitterligt:

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

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 informations- og kommunikationsteknologier (ikt-produkter, -tjenester og -processer), som er omfattet af en europæisk cybersikkerhedscertificeringsordning, og for overensstemmelsesvurderingsorganer.

Kapitel 2

Den nationale cybersikkerhedscertificeringsmyndighed

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

Kapitel 3

Overensstemmelsesvurderingsorganer

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

§ 5. Sikkerhedsstyrelsen kan bemyndige overensstemmelsesvurderingsorganer efter artikel 60, stk. 3, i forordningen om cybersikkerhed til at udføre opgaver i henhold til en europæisk cybersikkerhedscertificeringsordning, jf. artikel 49 i forordningen om cybersikkerhed, hvis der i den pågældende ordning er fastsat specifikke krav 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 yderligere 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.

[1)] I loven er der medtaget en bestemmelse fra 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, side 15. Herudover er forordningen medtaget som bilag til loven. Ifølge artikel 288 i EUF-traktaten gælder en forordning umiddelbart i hver medlemsstat. Gengivelsen af forordningen i loven og i lovens bilag er således udelukkende begrundet i praktiske hensyn og berører ikke forordningens umiddelbare gyldighed i Danmark.

CQ001729

Erhvervsmin., j.nr. EMN-00-01-000008

§ 6. Erhvervsministeren kan fastsætte nærmere regler om et certificeringsorgan under Sikkerhedsstyrelsen, som er udpeget efter artikel 60, stk. 2, 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 de opgaver, som er delegeret efter stk. 1.

§ 8. Erhvervsministeren kan fastsætte regler om udpegning af en udenlandsk cybersikkerhedscertificeringsmyndighed, et udenlandsk offentligt organ eller et andet udenlandsk overensstemmelsesvurderingsorgan til at varetage bestemte opgaver i henhold til en europæisk cybersikkerhedscertificeringsordning.

Kapitel 4

Tilsyn

§ 9. Sikkerhedsstyrelsen kan fra overensstemmelsesvurderingsorganer, indehavere af en europæisk cybersikkerhedsattest og udstedere af EU-overensstemmelseserklæringer kræve alle oplysninger, som er nødvendige for udførelsen af opgaven som national cybersikkerhedscertificeringsmyndighed, herunder til afgørelse af, om et forhold er omfattet af bestemmelserne i forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov eller regler fastsat i medfør af denne lov.

§ 10. Sikkerhedsstyrelsen kan udtage ethvert ikt-produkt og enhver ikt-tjeneste eller -proces, som er omfattet af en europæisk cybersikkerhedscertificeringsordning, med henblik på at lave en teknisk undersøgelse. Udtagelsen kan foretages af Sikkerhedsstyrelsen uden betaling, eller Sikkerhedsstyrelsen kan kræve udgiften refunderet, hvis udtagelsen af produktet, processen eller tjenesten har nødvendiggjort en betaling.

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

§ 12. 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 tilsyn efter dette kapitel.

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

§ 13. Sikkerhedsstyrelsen kan udstede påbud til en indehaver af en europæisk cybersikkerhedsattest eller en udsteder af en EU-overensstemmelseserklæring, der har bragt et ikt-produkt, en ikt-tjeneste eller en ikt-proces i omsætning, som ikke overholder bestemmelserne i forordningen om cybersikkerhed, regler fastsat i medfør af forordningen, denne lov eller 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.

§ 14. Sikkerhedsstyrelsen kan tilbagekalde en europæisk cybersikkerhedsattest, der er udstedt af Sikkerhedsstyrelsen eller et overensstemmelsesvurderingsorgan i henhold til artikel 56, stk. 5, litra a, eller stk. 6, i forordningen om cybersikkerhed, hvis indehaveren af en attest

1) ikke imødekommer Sikkerhedsstyrelsens anmodning om oplysninger, jf. § 9,
2) nægter at give Sikkerhedsstyrelsen adgang, jf. § 12,
3) ikke efterkommer et påbud fra Sikkerhedsstyrelsen, jf. § 13, 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

Kommunikation

§ 15. 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, jf. dog stk. 2.

Stk. 2. Sikkerhedsstyrelsen kan undtage en virksomhed fra digital kommunikation, når særlige omstændigheder taler for det.

Stk. 3. En digital meddelelse anses for at være kommet frem, når den er tilgængelig for adressaten for meddelelsen.

Stk. 4. Erhvervsministeren kan fastsætte nærmere regler om digital kommunikation og om anvendelse af bestemte it-systemer og særlige digitale formater.

Kapitel 6

Klageadgang

§ 16. Sikkerhedsstyrelsen behandler klager 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, og stk. 6, og
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 7

Gennemførelsesforanstaltninger

§ 18. 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 udstedte retsakter på forordningens område.

Kapitel 8

Ikrafttræden

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

Kapitel 9

Territorialbestemmelse

§ 20. Loven gælder ikke for Færøerne og Grønland.

Givet på Christiansborg Slot, den 4. maj 2021

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Simon Kollerup

Bilag 1

»Bilag1

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)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

under henvisning til forslag fra Europa-Kommissionen,

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

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[1],

under henvisning til udtalelse fra Regionsudvalget[2],

efter den almindelige lovgivningsprocedure[3], og

ud fra følgende betragtninger:

(1) Net- og informationssystemer og elektroniske kommunikationsnet og -tjenester spiller en afgørende rolle i samfundet og er blevet rygraden i den økonomiske vækst. Informations- og kommunikationsteknologier (IKT) er grundlaget for de komplekse systemer, som understøtter samfundets hverdagsaktiviteter, og sørger for, at vores økonomier fungerer inden for vigtige sektorer såsom sundhed, energi, finans og transport, og understøtter navnlig det indre markeds funktion.

(2) Borgere, organisationer og virksomheder i Unionen benytter i stort omfang net- og informationssystemer. Digitalisering og forbindelsesmuligheder er centrale elementer i et stadigt stigende antal produkter og tjenester, og med fremkomsten af tingenes internet forventes et meget højt antal forbundet digitalt udstyr at blive udbredt i hele Unionen i løbet af det næste årti. Stadigt mere udstyr er forbundet til internettet, men der tages ikke tilstrækkeligt hensyn til sikkerhed og modstandsdygtighed i udformningen, hvilket medfører utilstrækkelig cybersikkerhed. I denne forbindelse fører den begrænsede anvendelse af certificering til, at individuelle, organisatoriske og erhvervsmæssige brugere får utilstrækkelige oplysninger om IKT-produkters, -tjenesters og -processers cybersikkerhedsfunktioner, hvilket undergraver tilliden til digitale løsninger. Net- og informationssystemer er i stand til at støtte alle aspekter af vores liv og fremme Unionens økonomiske vækst. De er hjørnestenen i gennemførelsen af det digitale indre marked.

(3) Øget digitalisering og konnektivitet øger cybersikkerhedsrisici, hvilket gør samfundet som helhed mere sårbart over for cybertrusler og forværrer farerne for den enkelte, herunder også sårbare individer såsom børn. For at afbøde disse risici for samfundet bør der træffes alle nødvendige tiltag for at forbedre cybersikkerheden i Unionen, således at net- og informationssystemer, kommunikationsnet, digitale produkter, tjenester og udstyr, der anvendes af borgere, organisationer og virksomheder — fra små

og mellemstore virksomheder (SMV'er) som defineret i Kommissionens henstilling 2003/361/EF[4] til operatører af kritisk infrastruktur — er bedre beskyttet mod cybertrusler.

(4) Ved at stille de relevante oplysninger til rådighed for offentligheden bidrager Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) som oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 526/2013[5] til udviklingen af cybersikkerhedsindustrien i Unionen, navnlig SMV'er og nystartede virksomheder. ENISA bør tilstræbe et tættere samarbejde med universiteter og forskningsenheder for at bidrage til at reducere afhængigheden af cybersikkerhedsprodukter og -tjenester fra lande uden for Unionen og til at styrke forsyningskæder inden for Unionen.

(5) Mængden af cyberangreb er stigende og netforbundne økonomier og samfund, som er mere sårbare over for cybertrusler og -angreb, kræver stærkere forsvarsværker. Det er dog sådan, at cyberangreb ofte sker på tværs af grænser, medens cybersikkerhedsmyndigheders og retshåndhævende myndigheders beføjelser og politiske reaktion hovedsageligt er nationale. Omfattende hændelser kunne afbryde leveringen af essentielle tjenester i hele Unionen. Dette nødvendiggør en effektiv og koordineret reaktion og krisestyring på EU-plan, der bygger på målrettede politikker og videregående instrumenter for europæisk solidaritet og gensidig bistand. Det er desuden vigtigt for politikerne, erhvervslivet og brugerne, at der jævnligt foretages en vurdering af cybersikkerhedssituationen og modstandsdygtigheden i Unionen på grundlag af pålidelige EU-data samt systematiske prognoser for fremtidige udviklinger, udfordringer og trusler, både på EU-plan og globalt plan.

(6) I lyset af de tiltagende cybersikkerhedsudfordringer, som Unionen står over for, er der behov for et sammenhængende sæt foranstaltninger, som tager udgangspunkt i tidligere EU-tiltag og fremmer gensidigt forstærkende mål. Disse mål omfatter yderligere at øge medlemsstaternes og virksomhedernes kapacitet og beredskab samt at forbedre samarbejde, herunder udveksling af oplysninger, og samordning på tværs af medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer. På baggrund af cybertruslers grænseoverskridende karakter er der desuden behov for at øge kapaciteten på EU-plan, som kan supplere medlemsstaternes indsats, herunder navnlig i tilfælde af omfattende grænseoverskridende hændelser og -kriser, samtidig med, at der tages hensyn til vigtigheden af at opretholde og yderligere styrke den nationale kapacitet til at reagere på cybertrusler af ethvert omfang.

(7) Der er også behov for yderligere bestræbelser på at øge borgernes, organisationers og virksomheders bevidsthed om cybersikkerhedsspørgsmål. Eftersom hændelser undergraver tilliden til udbydere af digitale tjenester og til selve det digitale indre marked, navnlig blandt forbrugerne, bør tilliden desuden styrkes yderligere ved at give oplysninger om sikkerhedsniveauet af IKT-produkter, -tjenester og -processer på en gennemsigtig måde, idet det understreges, at selv et højt niveau af cybersikkerhedscertificering ikke kan garantere, at et IKT-produkt, en IKT-tjeneste eller en IKT-proces er fuldstændig sikker. Øget tillid kan fremmes ved certificering på EU-plan, der anvender fælles cybersikkerhedskrav og -evalueringskriterier på tværs af nationale markeder og sektorer.

(8) Cybersikkerhed er ikke kun et teknologisk spørgsmål, men ét, hvor menneskers adfærd er lige så vigtig. Der bør derfor sikres omfattende fremme af »cyberhygiejne«, dvs. enkle rutineforanstaltninger, der, når de gennemføres og regelmæssigt træffes af borgere, organisationer og virksomheder, minimerer deres eksponering for risici fra cybertrusler.

(9) Med henblik på at styrke Unionens cybersikkerhedsstrukturer er det vigtigt at opretholde og udvikle medlemsstaternes kapacitet til på en fyldestgørende måde at reagere på cybertrusler, herunder grænseoverskridende hændelser.

(10) Virksomheder og den enkelte forbruger bør modtage præcise oplysninger om, på hvilket tillidsniveau deres IKT- produkters, -tjenesters og -processers sikkerhed er blevet certificeret. Samtidig er intet