



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.

§ 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 udpegnings 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 retshåndhavende 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 vidererækkende 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

IKT-produkt og ingen IKT- tjeneste helt cybersikker(t), og det er nødvendigt at fremme og prioritere grundlæggende regler for cyberhygiejne. I betragtning af den voksende tilgængelighed af tingenes internet-udstyr er der en række frivillige foranstaltninger, som den private sektor kan træffe for at styrke tilliden til IKT-produkters, -tjenesters og -processers sikkerhed.

(11) Moderne IKT-produkter og -systemer integrerer ofte og er baseret på en eller flere tredjepartsteknologier og -komponenter som f.eks. softwaremoduler, biblioteker eller programmeringsgrænseflader for applikationer. Denne »afhængighed« kan indebære yderligere cybersikkerhedsrisici, da sårbarheder konstateret i tredjepartskomponenter også kan påvirke sikkerheden i IKT-produkter, -tjenester og -processer. I mange tilfælde vil identificeringen og dokumenteringen af en sådan afhængighed gøre det muligt for slutbrugerne af IKT-produkter, -tjenester og -processer at forbedre deres aktiviteter med henblik på risikostyring af cybersikkerheden, f.eks. ved at forbedre brugernes styring af sårbarhederne i forbindelse med cybersikkerhed og hjælpeprocedurer.

(12) Organisationer, producenter eller udbydere, der er involveret i udformning og udvikling af IKT-produkter, -tjenester og -processer, bør tilskyndes til at gennemføre foranstaltninger i de tidligste faser af udformningen og udviklingen for fra starten at beskytte disse produkters, processers og tjenesters sikkerhed i videst muligt omfang på en sådan måde, at forekomsten af cyberangreb forventes, og deres konsekvenser foregribes og minimeres (»indbygget sikkerhed«). Sikkerheden bør gennem hele IKT-produktets, -tjenestens eller -processens levetid sikres, således at der sker en løbende udvikling af udformnings- og udviklingsprocesserne med henblik på at begrænse skadevirkningerne af ondsindet udnyttelse.

(13) Virksomheder, organisationer og den offentlige sektor bør konfigurere de IKT-produkter, -tjenester eller -processer, som de udformer, på en måde, der sikrer en højere grad af sikkerhed, og som bør give den første bruger mulighed for at modtage en standardkonfiguration med de sikrest mulige indstillinger (»sikkerhed gennem standardindstillinger«) og dermed mindske den byrde, det er for brugerne at skulle konfigurere et IKT-produkt, en IKT-tjeneste eller en IKT-proces hensigtsmæssigt. Sikkerhed gennem standardindstillinger bør hverken kræve omfattende konfiguration eller særlig teknisk forståelse eller en adfærd fra brugerens side, der ikke er intuitiv, og bør fungere let og pålideligt, når det anvendes. Hvis en risiko- og brugbarhedsanalyse i en konkret sag fører til den konklusion, at en sådan standardindstilling ikke er mulig, bør brugerne tilskyndes til at vælge den sikreste indstilling.

(14) Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004⁽⁶⁾ oprettede ENISA med det formål at bidrage til målene om at sikre et højt og effektivt net- og informationssikkerhedsniveau i Unionen og udvikle en net- og informationssikkerhedskultur til gavn for borgerne, forbrugerne, virksomhederne og de offentlige forvaltninger. Europa-Parlamentets og Rådets forordning (EF) nr. 1007/2008⁽⁷⁾ forlængede ENISA's mandat frem til marts 2012. Europa-Parlamentets og Rådets forordning (EU) nr. 580/2011⁽⁸⁾ forlængede ENISA's mandat yderligere frem til den 13. september 2013. Forordning (EU) nr. 526/2013 forlængede ENISA's mandat frem til den 19. juni 2020.

(15) Unionen har allerede gjort en stor indsats for at sikre cybersikkerheden og øge tilliden til de digitale teknologier. I 2013 blev Den Europæiske Unions strategi for cybersikkerhed vedtaget for at sætte retningen for Unionens politiske reaktion på cybertrusler og -risici. For at beskytte borgerne bedre online vedtog Unionen i 2016 den første retsakt inden for cybersikkerhed, nemlig Europa-Parlamentets og Rådets direktiv (EU) 2016/1148⁽⁹⁾. Ved direktiv (EU) 2016/1148 blev der indført krav vedrørende nationale kapaciteter inden for cybersikkerhed, de første mekanismer til bedre strategisk og operationelt samarbejde mellem medlemsstaterne blev oprettet, og der blev indført forpligtelser vedrørende sikkerhedsforanstaltninger og underretning af hændelser i sektorer af afgørende betydning for økonomien og samfundet såsom energi, transport, drikkevandsforsyning og -distribution, bankvirksomhed, finansmar-

kedsinfrastrukturer, sundhed og digital infrastruktur samt for centrale udbydere af digitale tjenester (dvs. søgemaskiner, cloudcomputingtjenester og onlinemarkedspladser).

ENISA fik tildelt en central rolle som støtte for gennemførelsen af nævnte direktiv. Hertil kommer, at effektiv bekæmpelse af cyberkriminalitet er en vigtig prioritet på den europæiske sikkerhedsdagsorden og bidrager til det overordnede mål om at nå et højere niveau af cybersikkerhed. Andre retsakter såsom Europa-Parlamentets og Rådets forordning (EU) 2016/679⁽¹⁰⁾ og Europa-Parlamentets og Rådets direktiv 2002/58/EF⁽¹¹⁾ og (EU) 2018/1972⁽¹²⁾ bidrager også til et højt niveau af cybersikkerhed i det digitale indre marked.

(16) Den overordnede politiske kontekst har siden vedtagelsen af Den Europæiske Unions strategi for cybersikkerhed i 2013 og den seneste revision af ENISA's mandat ændret sig væsentligt, da det globale miljø er blevet mere uforudsigeligt og mindre sikkert. På den baggrund og i forbindelse med den positive udvikling af ENISA's rolle som et referencepunkt for rådgivning og ekspertise, som formidler af samarbejde og kapacitetsopbygning samt inden for rammerne af Unionens nye cybersikkerhedspolitik er det nødvendigt at gennemgå ENISA's mandat for at fastlægge dets rolle i det forandrede cybersikkerhedssystem og for at sikre, at det bidrager effektivt til Unionens reaktioner på de cybersikkerhedsudfordringer, der opstår som følge af det radikalt ændrede cybertrusselsbillede, hvilket dets aktuelle mandat ikke er tilstrækkeligt til, som det også blev anerkendt i evalueringen af ENISA.

(17) ENISA som oprettet ved nærværende forordning bør efterfølge ENISA som oprettet ved forordning (EU) nr. 526/2013. ENISA bør udføre de opgaver, det tillægges ved nærværende forordning og andre EU-retsakter inden for cybersikkerhed, bl.a. ved at levere rådgivning og ekspertise og fungere som et center for information og viden i Unionen. Det bør fremme udveksling af bedste praksis mellem medlemsstaterne og private interessenter, foreslå politiske initiativer for Kommissionen og medlemsstaterne, agere som et referencepunkt for EU's sektorpolitiske initiativer med hensyn til cybersikkerhedsspørgsmål, fremme det operationelle samarbejde både mellem medlemsstaterne indbyrdes og mellem medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer.

(18) Inden for rammerne af afgørelse 2004/97/EF, Euratom truffet ved fælles aftale mellem repræsentanterne for medlemsstaterne, forsamlet på stats- og regeringschefniveau⁽¹³⁾, besluttede repræsentanterne for medlemsstaterne, at ENISA skulle have sit sæde i en by i Grækenland, som skulle fastlægges nærmere af den græske regering. ENISA's værtsmedlemsstat bør sikre de bedst mulige betingelser for, at ENISA kan fungere problemfrit og effektivt. For at ENISA korrekt og effektivt kan udføre sine opgaver og rekruttere og fastholde personale samt øge effektiviteten af netværksaktiviteter, er det afgørende, at ENISA er placeret på et passende sted, hvor der bl.a. er passende transportforbindelser og faciliteter for ægtefæller og børn, som følger med ENISA's personale. De nødvendige foranstaltninger bør fastlægges i en aftale, som efter godkendelse af ENISA's bestyrelse indgås mellem ENISA og værtsmedlemsstaten.

(19) I betragtning af de tiltagende risici og udfordringer inden for cybersikkerhed, som Unionen står over for, bør de finansielle og menneskelige ressourcer, der er tildelt ENISA, forøges i overensstemmelse med dets udvidede rolle og opgaver og dets afgørende stilling i det økosystem af organisationer, der forsvare Unionens digitale økosystem, således at ENISA effektivt kan udføre de opgaver, som det tillægges ved denne forordning.

(20) ENISA bør udvikle og fastholde et højt ekspertiseniveau og fungere som et referencepunkt og skabe tillid til det indre marked i kraft af sin uafhængighed, kvaliteten af den rådgivning, det yder, og af de oplysninger, det videregiver, den åbenhed, der er forbundet med dets procedurer og driftsmetoder, og dets omhu ved udførelsen af sine opgaver. ENISA bør aktivt støtte den nationale indsats og proaktivt bidrage til Unionens indsats og udføre sine opgaver i fuldt samarbejde med Unionens institutioner, organer,

kontorer og agenturer samt medlemsstaterne, idet overlap undgås, og synergier fremmes. Herudover bør ENISA bygge på bidrag fra og samarbejde med den private sektor og andre relevante interessenter. Som grundlag for, hvordan ENISA skal nå sine mål, bør der fastlægges et sæt opgaver, der samtidig giver ENISA fleksibilitet i dets aktiviteter.

(21) For at kunne yde tilstrækkelig støtte til operationelt samarbejde mellem medlemsstaterne bør ENISA yderligere styrke sine tekniske og menneskelige kapaciteter og kompetencer. ENISA bør øge sin knowhow og kapacitet. ENISA og medlemsstaterne kunne på frivillig basis udvikle programmer for udstationering af nationale eksperter til ENISA, etablering af ekspertpuljer og udveksling af personale.

(22) ENISA bør bistå Kommissionen ved at levere rådgivning, udtalelser og analyser om alle EU-spørgsmål vedrørende udvikling af politik og lovgivning samt ajourføring og revision inden for cybersikkerhed og dets sektorspecifikke aspekter med henblik på at øge relevansen af EU-politikker og -lovgivning med en cybersikkerhedsdimension og muliggøre ensartethed i gennemførelsen heraf på nationalt plan. ENISA bør fungere som et referencepunkt for rådgivning og ekspertise for Unionens sektorspecifikke politikker og lovgivningsinitiativer i tilfælde, hvor cybersikkerhed er involveret. ENISA bør regelmæssigt orientere Europa-Parlamentet om sine aktiviteter.

(23) Den offentligt tilgængelige kerne af det åbne internet, dvs. dets vigtigste protokoller og infrastruktur, som er et globalt offentligt gode, sikrer internettet som helhed dets grundlæggende funktioner og understøtter dets normale drift. ENISA bør støtte sikkerheden for den offentlige tilgængelige kerne af det åbne internet og stabiliteten i dets drift, herunder, men ikke kun, de vigtigste protokoller (navnlig DNS, BGP og IPv6), driften af domænenavnsystemet (såsom driften af alle topdomæner) og driften af rodzonen.

(24) ENISA's grundlæggende opgave er at fremme en ensartet gennemførelse af den relevante retlige ramme, navnlig en effektiv gennemførelse af direktiv (EU) 2016/1148 og andre relevante retlige instrumenter med cybersikkerhedsaspekter, hvilket er afgørende for at øge cyberrobustheden. På baggrund af det hurtigt skiftende cybertrusselsbillede står det klart, at medlemsstaterne skal støttes med en mere samlet tværpolitisk tilgang til opbygningen af cyberrobusthed.

(25) ENISA bør bistå medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer i deres bestræbelser på at opbygge og forbedre deres kapacitet og beredskab med sigte på at forebygge, opdage og imødegå cybertrusler og -hændelser og i forbindelse med sikkerheden af net- og informationssystemer. ENISA bør navnlig støtte udvikling og forbedring af de i direktiv (EU) 2016/1148 fastsatte enheder, der håndterer IT-sikkerhedshændelser (»CSIRT'er«), på nationalt niveau og EU-niveau for at nå et højt fælles niveau af deres modenhed i Unionen. Aktiviteter, der udføres af ENISA vedrørende medlemsstaternes operationelle kapacitet, bør aktivt støtte medlemsstaternes indsats for at overholde deres forpligtelser i henhold til direktiv (EU) 2016/1148 og bør derfor ikke erstatte dem.

(26) ENISA bør også bistå med udviklingen og ajourføringen af Unionens og medlemsstaternes strategier for net- og informationssystemers sikkerhed på EU-niveau og efter anmodning på medlemsstatsniveau, herunder navnlig cybersikkerhed, og bør fremme udbredelse af sådanne strategier og følge fremskridtene med deres gennemførelse. ENISA bør også bidrage til at dække behovet for uddannelse og uddannelsesmateriale, herunder offentlige organers behov, og, når det er relevant, i vid udstrækning »uddanne underviserne« på grundlag af den digitale kompetenceramme for borgerne med sigte på at bistå medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer med at udvikle deres egne uddannelseskapaciteter.

(27) ENISA bør støtte medlemsstaterne på området bevidstgørelse om og uddannelse i cybersikkerhed ved at fremme en tættere koordinering og udveksling af bedste praksis mellem medlemsstaterne. En sådan støtte kunne bestå i udvikling af et netværk af nationale uddannelseskontaktpunkter og af en platform for

cybersikkerhedsuddannelse. Netværket af nationale uddannelseskontaktpunkter kunne operere inden for netværket af nationale forbindelsesofficerer og udgøre et udgangspunkt for den fremtidige koordinering i medlemsstaterne.

(28) ENISA bør bistå den samarbejdsgruppe, der er nedsat ved direktiv (EU) 2016/1148, med udførelsen af dens opgaver, navnlig ved at levere ekspertise og rådgivning og ved at fremme udvekslingen af bedste praksis vedrørende risici og hændelser, bl.a. med hensyn til medlemsstaternes identificering af operatører af væsentlige tjenester samt i forbindelse med grænseoverskridende afhængighed.

(29) Med sigte på at stimulere samarbejdet mellem den offentlige og den private sektor samt inden for den private sektor, navnlig for at støtte beskyttelsen af kritiske infrastrukturer, bør ENISA støtte informationsudveksling i og mellem sektorer, navnlig de sektorer, der er anført i bilag II til direktiv (EU) 2016/1148, ved at stille bedste praksis og vejledning om tilgængelige værktøjer og om procedurer til rådighed samt ved at vejlede om håndtering af reguleringsmæssige spørgsmål relateret til informationsudveksling, for eksempel gennem lettelse af etablering af centre for informationsudveksling og analyse.

(30) Eftersom de potentielle negative konsekvenser af sårbarheder i IKT-produkter, -tjenester og -processer øges konstant, er det vigtigt at finde og afhjælpe sådanne sårbarheder for at reducere den overordnede cybersikkerhedsrisiko. Det har vist sig, at et samarbejde mellem organisationer, producenter eller udbydere, der leverer sårbare IKT-produkter, -tjenester og -processer, og medlemmer af det forskningsfællesskab inden for cybersikkerhed og de regeringer, der finder sårbarheder, forbedrer såvel opdagelsen som afhjælpningen af sårbarheder i IKT-produkter, -tjenester og -processer markant. Ved koordineret offentliggørelse af sårbarheder forstås en struktureret samarbejdsproces, hvor sårbarheder meddeles til ejeren af informationssystemet, hvilket giver organisationen mulighed for at diagnosticere og afhjælpe sårbarheden, inden mere detaljerede sårbarhedsoplysninger videregives til tredjemand eller offentligheden. Processen giver også mulighed for koordinering mellem den, der finder sårbarheden, og organisationen i forbindelse med offentliggørelsen af sårbarhederne. Politikkerne for koordineret offentliggørelse af sårbarheder kan spille en vigtig rolle i medlemsstaternes indsats for at styrke cybersikkerheden.

(31) ENISA bør samle og analysere frivilligt delte nationale rapporter fra CSIRT'er og den interinstitutionelle IT-beredskabsenhed for Unionens institutioner, organer og agenturer, som er oprettet ved aftalen mellem Europa-Parlamentet, Det Europæiske Råd, Rådet for Den Europæiske Union, Europa-Kommissionen, Den Europæiske Unions Domstol, Den Europæiske Centralbank, Den Europæiske Revisionsret, Tjenesten for EU's Optræden Udadtil, Det Europæiske Økonomiske og Sociale Udvalg, Det Europæiske Regionsudvalg og Den Europæiske Investeringsbank om organisation og drift af en IT-beredskabsenhed for Unionens institutioner, organer og agenturer (CERT-EU)⁽¹⁴⁾ med det formål at bidrage til at indføre fælles procedurer, sprog og terminologi med henblik på udveksling af oplysninger. ENISA bør i den sammenhæng inddrage den private sektor inden for rammerne af direktiv (EU) 2016/1148, som fastsætter grundlaget for frivillig udveksling af tekniske oplysninger på det operationelle plan inden for det ved nævnte direktiv nedsatte netværk af enheder, der håndterer IT-sikkerhedshændelser («CSIRT-netværket»).

(32) ENISA bør bidrage til en reaktion på EU-niveau i tilfælde af væsentlige grænseoverskridende hændelser og -kriser relateret til cybersikkerhed. Denne opgave bør udføres i overensstemmelse med ENISA's mandat i henhold til denne forordning og en tilgang, der skal godkendes af medlemsstaterne i forbindelse med Kommissionens henstilling (EU) 2017/1584⁽¹⁵⁾ og Rådets konklusioner af 26. juni 2018 om en koordineret EU-reaktion på væsentlige cybersikkerhedshændelser og -kriser. Opgaven kan omfatte indsamling af relevante oplysninger og formidling af kontakt mellem CSIRT-netværket og tekniske kredse samt mellem de beslutningstagere, der er ansvarlige for krisestyringen. Derudover bør ENISA, når en eller flere medlemsstater anmoder herom, støtte operationelt samarbejde mellem medlemsstaterne

i forbindelse med håndteringen af hændelser fra et teknisk synspunkt ved at fremme udveksling af relevante tekniske løsninger mellem medlemsstaterne og ved at komme med input til kommunikation med offentligheden. ENISA bør støtte operationelt samarbejde ved at afprøve ordningerne for et sådant samarbejde gennem regelmæssige cybersikkerhedsøvelser.

(33) I forbindelse med støtte til operationelt samarbejde bør ENISA gøre brug af den tilgængelige tekniske og operationelle ekspertise hos CERT-EU gennem struktureret samarbejde. Sådant struktureret samarbejde kan opbygge ENISA's ekspertise. Hvor det er hensigtsmæssigt, bør der indføres specifikke ordninger mellem de to enheder med henblik på at fastlægge den praktiske gennemførelse af et sådant samarbejde og undgå overlap af aktiviteter.

(34) Ved udførelsen af dets opgaver med at støtte operationelt samarbejde inden for CSIRT-netværket bør ENISA være i stand til at yde støtte til medlemsstaterne på deres anmodning, f.eks. ved at yde rådgivning om, hvordan de kan forbedre deres kapacitet til at forebygge, opdage og reagere på hændelser, ved at lette den tekniske håndtering af hændelser, der har betydelige eller væsentlige konsekvenser, eller ved at sikre, at trusler og hændelser analyseres. ENISA bør lette den tekniske håndtering af hændelser, der har betydelige eller væsentlige konsekvenser, navnlig ved at støtte frivillig deling af tekniske løsninger mellem medlemsstaterne eller ved at tilvejebringe kombinerede tekniske oplysninger, såsom tekniske løsninger, der frivilligt deles af medlemsstaterne. Det anbefales i henstilling (EU) 2017/1584, at medlemsstaterne samarbejder i god tro og hurtigst muligt udveksler oplysninger med hinanden og med ENISA om væsentlige hændelser og -kriser relateret til cybersikkerhed. Sådanne oplysninger vil hjælpe ENISA yderligere med at udføre opgaven med at støtte operationelt samarbejde.

(35) Som led i det regelmæssige samarbejde på teknisk niveau til støtte for Unionens situationsbevidsthed bør ENISA i tæt samarbejde med medlemsstaterne regelmæssigt udarbejde en tilbundsående teknisk EU-cybersikkerhedsrapport om hændelser og cybertrusler, der er baseret på offentligt tilgængelige oplysninger, ENISA's egen analyse og rapporter tilsendt ENISA af medlemsstaternes CSIRT'er eller de nationale centrale kontaktpunkter for sikkerheden i net- og informationssystemer (»centrale kontaktpunkter«), der er omhandlet i direktivet (EU) 2016/1148, begge på frivillig basis. Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol, CERT-EU og, hvor det er relevant, Den Europæiske Unions Efterretnings- og Situationscenter (INTCEN) ved Tjenesten for EU's Optræden Udadtil. Rapporten bør stilles til rådighed for de relevante instanser i Rådet, Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik og CSIRT-netværket.

(36) ENISA's støtte til efterfølgende tekniske undersøgelser af hændelser med betydelige eller væsentlige konsekvenser, som foretages på de berørte medlemsstaters anmodning, bør fokusere på forebyggelse af fremtidige hændelser. De berørte medlemsstater bør give de nødvendige oplysninger og yde den nødvendige bistand, så ENISA effektivt kan støtte de efterfølgende tekniske undersøgelser.

(37) Medlemsstaterne kan opfordre de virksomheder, der er berørt af hændelsen, til at samarbejde ved at give ENISA de nødvendige oplysninger og den nødvendige bistand, uden at det berører deres ret til at beskytte kommercielt følsomme oplysninger og oplysninger, der er relevante for den offentlige sikkerhed.

(38) For bedre at forstå udfordringerne inden for cybersikkerhed og med sigte på at levere strategisk langsigtet rådgivning til medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer er ENISA nødt til at analysere både nuværende og nye cybersikkerhedsrisici. Med dette mål for øje bør ENISA i samarbejde med medlemsstaterne og, alt efter hvad der er relevant, statistiske organer og andre organer indsamle relevante offentligt tilgængelige eller frivilligt delte oplysninger og udføre analyser af nye teknologier og tilvejebringe emnespecifikke vurderinger af de forventede samfundsmæssige, retlige, økonomiske og reguleringsmæssige konsekvenser af teknologiske innovationer for net- og infor-

mationssikkerheden, navnlig cybersikkerhed. ENISA bør desuden bistå medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer med at identificere nye risici og forebygge hændelser ved at udføre analyser af trusler, sårbarheder og hændelser.

(39) Med henblik på at øge Unionens modstandsdygtighed bør ENISA udvikle ekspertise inden for cybersikkerhed for infrastrukturer, navnlig for at understøtte de sektorer, som er anført i bilag II til direktiv (EU) 2016/1148, og dem, der anvendes af de udbydere af digitale tjenester, som er anført i bilag III til nævnte direktiv, ved at yde rådgivning, udstede retningslinjer og udveksle bedste praksis. Med sigte på at sikre lettere adgang til bedre strukturerede oplysninger om cybersikkerhedsrisici og mulige løsninger bør ENISA udvikle og opretholde Unionens »informationsknudepunkt«, en one-stop-shop-portal, som giver offentligheden oplysninger om cybersikkerhed, der hidrører fra Unionens og de nationale institutioner, agenturer og organer. Lettere adgang til mere strukturerede oplysninger om cybersikkerhedsrisici og mulige løsninger kan også hjælpe medlemsstaterne med at styrke deres kapacitet og tilpasse deres praksis og derved øge deres samlede modstandsdygtighed over for cyberangreb.

(40) ENISA bør bidrage til at øge offentlighedens bevidsthed om cybersikkerhedsrisici, herunder gennem en oplysningskampagne på EU-plan og uddannelsesfremme, og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere, organisationer og virksomheder. ENISA bør også bidrage til at fremme bedste praksis og løsninger, herunder cyberhygiejne og cyberfærdigheder, på borger-, organisations- og virksomhedsniveau ved at indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og ved at sammenstille og offentliggøre rapporter og vejledning til borgere, organisationer og virksomheder samt forbedre deres generelle niveau af beredskab og modstandsdygtighed. ENISA bør desuden tilstræbe at give forbrugere relevante oplysninger om gældende certificeringsordninger, f.eks. ved at give vejledning og anbefalinger. ENISA bør herudover i overensstemmelse med handlingsplanen for digital uddannelse fastsat i Kommissionens meddelelse af 17. januar 2018 og i samarbejde med medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer tilrettelægge regelmæssige informations- og oplysningskampagner rettet mod slutbrugere for at fremme en mere sikker adfærd på nettet blandt enkeltpersoner og fremme digitale færdigheder, øge bevidstheden om de potentielle cybertrusler, herunder kriminelle aktiviteter online, såsom phishingangreb, botnet, økonomisk svig og banksvindel, databedrageri, samt fremme grundlæggende multifaktorautentificering, patching, kryptering, anonymisering og databeskyttelsesrådgivning.

(41) ENISA bør spille en central rolle i bestræbelserne på at højne slutbrugernes bevidsthed om udstyrs sikkerhed og om sikker brug af tjenester og bør fremme indbygget sikkerhed og indbygget privatlivsbeskyttelse på EU-plan. Ved forfølgelsen af dette mål bør ENISA udnytte forhåndenværende bedste praksis og erfaring, navnlig bedste praksis og erfaring fra akademiske institutioner og IT-sikkerhedsforskere, bedst muligt.

(42) For at støtte de virksomheder, der er aktive i cybersikkerhedssektoren, samt brugerne af cybersikkerhedsløsninger bør ENISA udvikle og opretholde et »markedsobservatorium« ved at gennemføre regelmæssige analyser og formidling af de vigtigste tendenser på markedet for cybersikkerhed, både på efterspørgsels- og udbudssiden.

(43) ENISA bør bidrage til Unionens indsats for at samarbejde med internationale organisationer samt inden for relevante internationale samarbejdsrammer inden for cybersikkerhed. ENISA bør navnlig, hvor det er hensigtsmæssigt, bidrage til samarbejdet med organisationer såsom OECD, OSCE og NATO. Et sådant samarbejde kunne omfatte fælles cybersikkerhedsovelser og fælles koordinering af reaktionen på hændelser. Disse aktiviteter skal udføres under fuld overholdelse af principperne om inklusivitet, gensidighed og Unionens beslutningsautonomi, uden at dette berører den særlige karakter af den enkelte medlemsstats sikkerheds- og forsvarspolitik.

(44) For at sikre, at det når sine mål fuldt ud, bør ENISA etablere kontakt med relevante EU-tilsynsmyndigheder og andre kompetente myndigheder i Unionen, Unionens institutioner, organer, kontorer og agenturer, herunder CERT-EU, EC3, Det Europæiske Forsvarsagentur (EDA), Det Europæiske GNSS-Agentur (GSA), Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu- LISA), Den Europæiske Centralbank (ECB), Den Europæiske Banktilsynsmyndighed (EBA), Det Europæiske Databeskyttelsesråd, Agenturet for Samarbejde mellem Energireguleringsmyndigheder (ACER), Det Europæiske Luftfartssikkerhedsagentur (EASA) og ethvert andet EU-agentur, der er involveret i cybersikkerhed. ENISA bør også etablere kontakt med myndigheder med ansvar for databeskyttelse for at udveksle knowhow og bedste praksis, og det bør yde rådgivning om cybersikkerhedsspørgsmål, der kan have betydning for deres arbejde. Repræsentanter for de retshåndhævende myndigheder og databeskyttelsesmyndigheder på nationalt plan og EU-plan bør kunne være repræsenteret i ENISA-Rådgivningsgruppen. I sine kontakter med retshåndhævende myndigheder vedrørende net- og informationssikkerhedsspørgsmål, der kan have indflydelse på disse myndigheders arbejde, bør ENISA respektere eksisterende informationskanaler og etablerede netværk.

(45) Der kunne etableres partnerskaber med akademiske institutioner, som har forskningsinitiativer på de relevante områder, og der bør være passende kanaler til bidrag fra forbrugerorganisationer og andre organisationer, som bør tages i betragtning.

(46) ENISA bør i sin rolle som CSIRT-netværkets sekretariat støtte medlemsstaternes CSIRT'er og CERT-EU i det operationelle samarbejde i forbindelse med CSIRT-netværkets relevante opgaver som omhandlet i direktiv (EU) 2016/1148. ENISA bør endvidere fremme og støtte samarbejdet mellem de relevante CSIRT'er i tilfælde af hændelser, angreb på eller afbrydelser af net eller infrastruktur, der styres eller beskyttes af CSIRT'erne, og som berører eller vil kunne berøre mindst to CSIRT'er, idet der tages behørigt hensyn til CSIRT-netværkets standardprocedurer.

(47) Med henblik på at øge Unionens beredskab til at reagere på cybersikkerhedshændelser bør ENISA regelmæssigt tilrettelægge cybersikkerhedsøvelser på EU-niveau og på deres anmodning støtte medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer i at tilrettelægge sådanne øvelser. Omfattende øvelser i stor skala, som omfatter tekniske, operationelle og strategiske elementer, bør afholdes mindst hvert andet år. ENISA bør desuden regelmæssigt kunne afholde mindre omfattende øvelser med samme mål om at øge Unionens beredskab til at reagere på hændelser.

(48) ENISA bør videreudvikle og opretholde sin ekspertise inden for cybersikkerhedscertificering med sigte på at understøtte Unionens politik på dette område. ENISA bør bygge videre på eksisterende bedste praksis og fremme udbredelsen af cybersikkerhedscertificering i Unionen, herunder ved at bidrage til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau (den europæiske ramme for cybersikkerhedscertificering), for at øge gennemsigtigheden af IKT-produkters, -tjenesters og -processers cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked og dets konkurrenceevne.

(49) Effektive cybersikkerhedsstrategier bør baseres på velgennemtænkte risikovurderingsmetoder, både i den offentlige og den private sektor. Risikovurderingsmetoder anvendes på forskellige niveauer og uden fælles praksis for, hvordan de anvendes effektivt. Ved at fremme og udvikle bedste praksis for risikovurdering og interoperable risikostyringsløsninger i den offentlige og den private sektors organisationer kan cybersikkerhedsniveauet i Unionen højnes. Til dette formål bør ENISA støtte samarbejdet mellem interessenter på EU-plan og lette deres bestræbelser på at etablere og indføre europæiske og internationale standarder for risikostyring og for målbar sikkerhed i elektroniske produkter, systemer, net og tjenester, som sammen med software udgør net- og informationssystemerne.

(50) ENISA bør tilskynde medlemsstaterne, producenter eller udbydere af IKT-produkter, -tjenester og -processer til at hæve deres generelle sikkerhedsstandarder, så alle internetbrugere kan tage de nødvendige skridt til at sikre deres egen personlige cybersikkerhed og bør give incitamenter til at gøre det. Navnlig bør producenter og udbydere af IKT-produkter, -tjenester og -processer udsende nødvendige opdateringer og tilbagekalde, tilbagetrække eller genbruge IKT-produkter, -tjenester eller -processer, som ikke overholder cybersikkerhedsstandarderne, mens importører og distributører bør sikre sig, at de IKT-produkter, -tjenester og -processer, som de bringer i omsætning på EU-markedet, opfylder de gældende krav og ikke udgør en risiko for Unionens forbrugere.

(51) I samarbejde med de kompetente myndigheder bør ENISA kunne formidle oplysninger om cybersikkerhedsniveauet for IKT-produkter, -tjenester og -processer, som udbydes i det indre marked, og det bør kunne udstede advarsler til producenter eller udbydere af IKT-produkter, -tjenester eller -processer og pålægge dem at forbedre sikkerheden af deres IKT-produkter, -tjenester og -processer, herunder cybersikkerheden.

(52) ENISA bør tage fuldt hensyn til igangværende forsknings-, udviklings- og teknologivurderingsaktiviteter, navnlig aktiviteter der gennemføres som led i de forskellige EU-forskningsinitiativer for at rådgive Unionens institutioner, organer, kontorer og agenturer og, hvor det er relevant, medlemsstaterne, hvis de anmoder herom, om forskningsbehov og -prioriteter inden for cybersikkerhed. Med henblik på at klarlægge forskningsbehov og -prioriteter bør ENISA også høre de relevante brugergrupper. Mere specifikt kunne der etableres et samarbejde med Det Europæiske Forskningsråd (EFR), Det Europæiske Institut for Innovation og Teknologi (EIT) og Den Europæiske Unions Institut for Sikkerhedsstudier (EUISS).

(53) ENISA bør regelmæssigt høre standardiseringsorganisationer, navnlig europæiske standardiseringsorganisationer, i forbindelse med udarbejdelsen af de europæiske cybersikkerhedscertificeringsordninger.

(54) Cybertrusler er af global karakter. Der er behov for et tættere internationalt samarbejde for at forbedre cybersikkerhedsstandarderne, herunder behov for definitioner af fælles adfærdsnormer, vedtagelse af adfærdskodekser, anvendelse af internationale standarder og informationsudveksling, fremme af hurtigere internationalt samarbejde som reaktion på net- og informationssikkerhedsspørgsmål og fremme af en global tilgang til sådanne spørgsmål. ENISA bør derfor støtte yderligere EU-engagement og -samarbejde med tredjelande og internationale organisationer, ved, hvor det er relevant, at yde den nødvendige ekspertise og analyse til Unionens relevante institutioner, organer, kontorer og agenturer.

(55) ENISA bør være i stand til at imødekomme ad hoc-anmodninger om rådgivning og bistand fra medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer i forhold til spørgsmål, som er omfattet af ENISA's mandat.

(56) Det er fornuftigt og anbefales at gennemføre visse principper om ENISA's forvaltning for at overholde den fælles erklæring og fælles tilgang, som Den Interinstitutionelle Arbejdsgruppe om Unionens Decentrale Agenturer nåede til enighed om i juli 2012, og som har til formål at strømline de decentrale agenturers aktiviteter og forbedre deres resultater. Anbefalingerne i den fælles erklæring og den fælles tilgang vedrørende ENISA's arbejdsprogrammer, evalueringer og rapporterings- og administrationspraksis bør også afspejles, når det er relevant.

(57) Bestyrelsen, som består af repræsentanter for medlemsstaterne og for Kommissionen, bør fastlægge de overordnede retningslinjer for ENISA's drift og sikre, at det udfører sine opgaver i overensstemmelse med denne forordning. Bestyrelsen bør have de beføjelser, der er nødvendige, til at fastlægge budgettet, kontrollere budgettets gennemførelse, vedtage passende finansielle bestemmelser, fastlægge transparente arbejdsprocedurer for ENISA's beslutningstagning, vedtage ENISA's samlede programmeringsdokument,

vedtage sin egen forretningsorden, udnævne den administrerende direktør og træffe afgørelse om at forlængelse og ophør af den administrerende direktørs mandatperiode.

(58) For at ENISA kan fungere korrekt og effektivt, bør Kommissionen og medlemsstaterne sikre, at personer, der udpeges til bestyrelsen, har passende faglig ekspertise og erfaring. Kommissionen og medlemsstaterne bør også gøre en indsats for at begrænse udskiftningen af deres respektive repræsentanter i bestyrelsen, så der sikres kontinuitet i bestyrelsens arbejde.

(59) Et velfungerende ENISA kræver, at den administrerende direktør udnævnes på grundlag af kvalifikationer og dokumenterede administrative og ledelsesmæssige færdigheder samt kvalifikationer og erfaring, der er relevante for cybersikkerhed. Den administrerende direktørs opgaver bør udføres i fuld uafhængighed. Den administrerende direktør bør efter forudgående høring af Kommissionen udarbejde et forslag til ENISA's årlige arbejdsprogram og træffe alle nødvendige foranstaltninger til at sikre, at dette arbejdsprogram gennemføres korrekt. Den administrerende direktør bør udarbejde en årsberetning, der skal forelægges bestyrelsen, og som omhandler gennemførelsen af ENISA's årlige arbejdsprogram, udfærdige et udkast til overslag over ENISA's indtægter og udgifter samt gennemføre budgettet. Den administrerende direktør bør endvidere kunne nedsætte ad hoc-arbejdsgrupper til at behandle specifikke spørgsmål, navnlig spørgsmål af videnskabelig, teknisk, retlig eller samfundsøkonomisk art.

Navnlig i forbindelse med udarbejdelsen af et forslag til en specifik europæisk cybersikkerhedscertificeringsordning anses det for nødvendigt at nedsætte en ad hoc-arbejdsgruppe. Den administrerende direktør bør sikre, at medlemmerne af ad hoc-arbejdsgrupperne udvælges på grundlag af den højeste ekspertisesstandard, og tage skridt til at sikre en jævn kønsfordeling og en passende balance, afhængigt af de specifikke spørgsmål, mellem medlemsstaternes offentlige forvaltninger, Unionens institutioner organer, kontorer og agenturer og den private sektor, herunder branchen, brugerne og akademiske eksperter i net- og informationssikkerhed.

(60) Forretningsudvalget bør bidrage til en velfungerende bestyrelse. Som led i det forberedende arbejde i forbindelse med bestyrelsens afgørelser bør forretningsudvalget nøje undersøge relevante oplysninger og gennemgå mulighederne og tilbyde rådgivning og løsninger til forberedelse af bestyrelsens afgørelser.

(61) ENISA bør have en ENISA-rådgivningsgruppe som et rådgivende organ, der kan sikre en løbende dialog med den private sektor, forbrugerorganisationer og andre relevante interessenter. ENISA-Rådgivningsgruppen, der nedsættes af bestyrelsen efter forslag af den administrerende direktør, bør koncentrere sig om spørgsmål, der er relevante for interessenter, og forelægge dem for ENISA. ENISA-Rådgivningsgruppen bør navnlig høres i forbindelse med udkastet til ENISA's årlige arbejdsprogram. Sammensætningen af ENISA-Rådgivningsgruppen og dens opgaver bør sikre en tilstrækkelig repræsentation af interessenter i ENISA's arbejde.

(62) Der bør nedsættes en cybersikkerhedscertificeringsgruppe for interessenter for at bistå ENISA og Kommissionen med at fremme høringen af relevante interessenter. Cybersikkerhedscertificeringsgruppen for Interessenter bør sammensættes af medlemmer, der i afbalanceret omfang repræsenterer branchen, både på efterspørgsels- og udbudssiden i forbindelse med IKT-produkter og -tjenester og herunder navnlig SMV'er, udbydere af digitale tjenester, europæiske og internationale standardiseringsorganer, nationale akkrediteringsorganer, databeskyttelsestilsynsmyndigheder og overensstemmelsesvurderingsorganer i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008⁽¹⁶⁾ samt akademiske kredse og forbrugerorganisationer.

(63) ENISA bør vedtage regler for forebyggelse og håndtering af interessekonflikter. ENISA bør også følge de relevante EU-bestemmelser om aktindsigt som fastlagt i Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001⁽¹⁷⁾. ENISA's behandling af personoplysninger bør være i overensstemmelse med

Europa-Parlamentets og Rådets forordning (EU) 2018/1725⁽¹⁸⁾. ENISA bør overholde de bestemmelser, der gælder for Unionens institutioner, organer, kontorer og agenturer, samt national lovgivning vedrørende behandling af oplysninger, navnlig følsomme ikkeklassificerede oplysninger og EU-klassificerede oplysninger (EUCI).

(64) For at ENISA kan sikres fuld selvstændighed og uafhængighed og for at sætte det i stand til at udføre supplerende og nye opgaver, herunder uforudsete hasteopgaver, bør ENISA råde over et tilstrækkeligt og selvstændigt budget, hvis indtægter hovedsageligt kommer fra et bidrag fra Unionen og bidrag fra tredjelande, der deltager i ENISA's arbejde. For at sikre, at ENISA har tilstrækkelig kapacitet til at klare alle sine voksende opgaver og opnå sine mål, er det af helt afgørende betydning, at det tildeles tilstrækkelige midler. Størstedelen af ENISA's ansatte bør være direkte involveret i den operationelle gennemførelse af ENISA's mandat. Værtsmedlemsstaten og enhver anden medlemsstat bør kunne yde frivillige bidrag til ENISA's budget. Unionens budgetprocedure bør finde anvendelse på ethvert bidrag, som kommer fra Unionens almindelige budget. Desuden bør revisionen af ENISA's regnskaber forestås af Revisionsretten for at sikre gennemsigtighed og ansvarlighed.

(65) Cybersikkerhedscertificering spiller en vigtig rolle for at øge tilliden til og sikkerheden af IKT-produkter, -tjenester og -processer. Det digitale indre marked og navnlig dataøkonomien og tingenes internet kan kun trives, hvis offentligheden generelt har tillid til, at sådanne produkter, tjenester og processer har et vist cybersikkerhedsniveau. Netforbundne og selvkørende biler, elektronisk medicinsk udstyr, industrielle automatiseringskontrollsystemer og intelligente forsyningsnet er blot nogle eksempler på sektorer, hvor certificering allerede bruges i vidt omfang eller sandsynligvis vil blive brugt i nærmeste fremtid. De sektorer, der reguleres af direktiv (EU) 2016/1148, er også sektorer, hvor cybersikkerhedscertificering er afgørende.

(66) I meddelelsen fra 2016 »Styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri«, beskrev Kommissionen nødvendigheden af cybersikkerhedsprodukter og -løsninger, som er af høj kvalitet, økonomisk overkommelige og interoperable. Udbuddet af IKT-produkter, -tjenester og -processer i det indre marked er fortsat meget fragmenteret geografisk. Det skyldes, at cybersikkerhedsindustrien i Europa hovedsageligt har udviklet sig på grundlag af national statslig efterspørgsel. Derudover mangler der også interoperable løsninger (tekniske standarder), praksis og EU-dækkende mekanismer for certificering, og det har en negativ virkning på det indre marked for cybersikkerhed. Dette gør det vanskeligt for europæiske virksomheder at konkurrere på nationalt plan, EU-plan og globalt plan. Det begrænser også udbuddet af levedygtige og brugbare cybersikkerhedsteknologier, som enkeltpersoner og virksomheder har adgang til. Ligeledes fremhævede Kommissionen i meddelelsen fra 2017 om midtvejsevalueringen om gennemførelsen af strategien for det digitale indre marked — Et forbundet digitalt indre marked for alle behovet for sikre netforbundne produkter og systemer og anførte, at indførelsen af en europæisk IKT-sikkerhedsramme, der fastsætter regler for tilrettelæggelse af IKT-sikkerhedscertificering i Unionen, både ville kunne bevare tilliden til internettet og gøre noget ved den nuværende fragmentering af det indre marked.

(67) I øjeblikket anvendes cybersikkerhedscertificering af IKT-produkter, -tjenester og -processer kun i begrænset omfang. Hvis den findes, er det som regel på medlemsstatsniveau eller inden for rammerne af en brancheordning. I den forbindelse anerkendes en attest udstedt af en national cybersikkerhedscertificeringsmyndighed i princippet ikke i andre medlemsstater. Virksomhederne kan således være nødt til at certificere deres IKT-produkter, -tjenester og -processer i flere medlemsstater, hvor de driver virksomhed, f.eks. hvis de vil deltage i nationale offentlige udbud, hvorved deres omkostninger øges. Desuden er der, selv om der laves nye ordninger, tilsyneladende ikke nogen sammenhængende og holistisk tilgang til horisontale cybersikkerhedsspørgsmål, f.eks. inden for tingenes internet. De eksisterende ordninger

har væsentlige mangler og forskelle med hensyn til produktdekning, tillidsniveau, materielle kriterier og faktisk anvendelse, hvilket vanskeliggør mekanismer til gensidig anerkendelse i Unionen.

(68) Der er tidligere taget tilløb til at sikre gensidig anerkendelse af attester i Unionen. De har dog kun været delvis vellykkede. Det vigtigste eksempel herpå er Gruppen af Højtstående Embedsmænd vedrørende Informationssystemers Sikkerheds (SOG-IS') aftale om gensidig anerkendelse (MRA). Selv om det er den vigtigste model for samarbejde og gensidig anerkendelse på sikkerhedscertificeringsområdet, omfatter SOG-IS kun visse af Unionens medlemsstater. I forhold til det indre marked gør dette forhold, at SOG-IS' MRA kun er begrænset effektiv.

(69) Derfor er det nødvendigt at vedtage en fælles tilgang og etablere en europæisk ramme for cybersikkerhedscertificering, som fastlægger de vigtigste horisontale krav til kommende europæiske cybersikkerhedscertificeringsordninger, og som giver mulighed for anerkendelse og brug af europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer for IKT-produkter, -tjenester og -processer i alle medlemsstater. I denne forbindelse er det afgørende at bygge videre på eksisterende nationale og internationale ordninger samt på systemer for gensidig anerkendelse, navnlig SOG-IS, og at give mulighed for en smidig overgang fra de eksisterende ordninger under sådanne systemer til ordninger under den nye europæiske ramme for cybersikkerhedscertificering. Den europæiske ramme for cybersikkerhedscertificering bør have et dobbelt formål. For det første bør den bidrage til at øge tilliden til IKT-produkter, -tjenester og -processer, der er certificeret i henhold til europæiske cybersikkerhedscertificeringsordninger. For det andet bør den hindre udbredelsen af modstridende eller overlappende nationale cybersikkerhedscertificeringsordninger og dermed mindske omkostningerne for virksomheder, der opererer på det digitale indre marked. De europæiske cybersikkerhedscertificeringsordninger bør være ikkediskriminerende og baseret på europæiske eller internationale standarder, medmindre sådanne standarder er ineffektive eller uhensigtsmæssige til at opfylde Unionens legitime mål i denne henseende.

(70) Den europæiske ramme for cybersikkerhedscertificering bør etableres på en ensartet måde i alle medlemsstater for at undgå »certificeringsshopping« som følge af forskellige krav i medlemsstaterne.

(71) De europæiske cybersikkerhedscertificeringsordninger bør bygge på det, der allerede eksisterer på internationalt og nationalt plan, og om nødvendigt på tekniske specifikationer fra fora og konsortier, idet der drages lære af nuværende stærke sider, og svagheder vurderes og korrigeres.

(72) Industrien har brug for fleksible cybersikkerhedsløsninger for at kunne foregribe cybertrusler, og det bør derfor sikres, at ingen certificeringsordning udformes på en måde, hvor den forældes for hurtigt.

(73) Kommissionen bør tillægges beføjelse til at vedtage europæiske cybersikkerhedscertificeringsordninger for specifikke grupper af IKT-produkter, -tjenester og -processer. Nationale cybersikkerhedscertificeringsmyndigheder bør gennemføre og føre tilsyn med disse ordninger, og attester udstedt i henhold til disse ordninger bør være gyldige og anerkendes i hele Unionen. Certificeringsordninger, som er branchedrevne eller drives af andre private organisationer, bør ikke være omfattet af denne forordnings anvendelsesområde. Organer, der driver sådanne ordninger, bør dog kunne foreslå Kommissionen at betragte ordningerne som grundlaget for at godkende dem som en europæisk cybersikkerhedscertificeringsordning.

(74) Bestemmelserne i denne forordning bør ikke berøre EU-ret om specifikke regler for certificering af IKT-produkter, -tjenester og -processer. Navnlig fastsætter forordning (EU) 2016/679 bestemmelser om til fastlæggelse af certificeringsmekanismer for databeskyttelse samt databeskyttelsesmærkninger og -mærker med henblik på at påvise, at dataansvarliges og databehandlers behandlingsaktiviteter overholder nævnte forordning. Sådanne certificeringsmekanismer og databeskyttelsesmærkninger bør give de registrerede mulighed for hurtigt at vurdere de relevante IKT-produkters, -tjenesters og -processers data-

beskyttelsesniveau. Nærværende forordning berører ikke certificeringen af databehandlingsoperationer i henhold til forordning (EU) 2016/679, herunder hvis sådanne operationer er indeholdt i IKT-produkter, -tjenester og -processer.

(75) Målet med europæiske cybersikkerhedscertificeringsordninger bør være at sikre, at de IKT-produkter, -tjenester og -processer, der er certificeret i henhold til sådanne ordninger, opfylder de fastsatte krav med henblik på at beskytte tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der lagres, overføres eller behandles, eller af de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, tjenester og processer i hele deres livscyklus. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-produkter, -tjenester og -processer i denne forordning. IKT-produkter, -tjenester og -processer og de til disse produkter, tjenester og processer hørende cybersikkerhedsbehov er så forskellige, at det er meget vanskeligt at udvikle generelle cybersikkerhedskrav, der gælder i alle situationer. Det er derfor nødvendigt at anlægge en bred og generel opfattelse af cybersikkerhed med henblik på certificering, som bør suppleres af en række specifikke cybersikkerhedsmål, som skal tages i betragtning ved udformningen af europæiske cybersikkerhedscertificeringsordninger. De ordninger, der skal anvendes til at nå disse mål i forhold til specifikke IKT-produkter, -tjenester og -processer, bør så præciseres yderligere i den enkelte certificeringsordning, der vedtages af Kommissionen, f.eks. i form af henvisninger til standarder eller tekniske specifikationer, hvis der ikke findes hensigtsmæssige standarder.

(76) De tekniske specifikationer, der skal anvendes i en europæisk cybersikkerhedscertificeringsordning, bør overholde kravene i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012⁽¹⁹⁾. Visse afvigelser fra disse krav kan dog anses for at være nødvendige i behørigt begrundede tilfælde, hvor de pågældende tekniske specifikationer skal anvendes i en europæisk cybersikkerhedscertificeringsordning, der henviser til tillidsniveauet »højt«. Årsagerne til sådanne afvigelser bør gøres offentligt tilgængelige.

(77) Certificeret overensstemmelsesvurdering er en procedure til at evaluere, om nærmere krav til et IKT-produkt, en IKT-tjeneste eller en IKT-proces er opfyldt. Denne procedure gennemføres af en uafhængig tredjepart, som ikke er producenten eller udbyderen af de IKT-produkter, -tjenester eller -processer, der vurderes. En europæisk cybersikkerhedsattest bør udstedes efter vellykket evaluering af et IKT-produkt, en IKT-tjeneste eller en IKT-proces. En europæisk cybersikkerhedsattest bør anses som en bekræftelse af, at evalueringen er foretaget korrekt. Afhængigt af tillidsniveauet bør den europæiske cybersikkerhedscertificeringsordning angive, om den europæiske cybersikkerhedsattest udstedes af et privat eller offentligt organ. Overensstemmelsesvurdering og certificering kan ikke i sig selv garantere, at certificerede IKT-produkter, -tjenester og -processer er cybersikre. Der er snarere tale om procedurer og tekniske metoder til at attestere, at IKT-produkter, -tjenester og -processer er blevet prøvet, og at de opfylder visse krav til cybersikkerhed, som er fastsat andetsteds, f.eks. i tekniske standarder.

(78) Det valg af passende certificering og tilhørende sikkerhedskrav, som brugerne af europæiske cybersikkerhedsattester træffer, bør bygge på en analyse af de risici, der er forbundet med anvendelse af de pågældende IKT-produkter, -tjenester eller -processer. Tillidsniveauet bør således afspejle det risikoniveau, der er forbundet med den tilsigtede anvendelse af et IKT-produkt eller en IKT-tjeneste eller -proces.

(79) En europæisk cybersikkerhedscertificeringsordning kan fastsætte, at en overensstemmelsesvurdering skal foretages under eneansvar af producenten eller udbyderen af IKT-produkter, -tjenester eller -processer (selvvurdering af overensstemmelse). I sådanne tilfælde bør det være tilstrækkeligt, at producenten eller udbyderen af IKT-produkter, -tjenester eller -processer selv foretager hele kontrollen med henblik på at sikre, at de pågældende IKT-produkter, -tjenester eller -processer stemmer overens med den europæiske cybersikkerhedscertificeringsordning. Selvvurdering af overensstemmelse bør betragtes som passende for

IKT-produkter, -tjenester og -processer med lav kompleksitet, som udgør en lav risiko for offentligheden (enkel udformnings- og produktionsmekanisme). Desuden bør selvvurdering af overensstemmelse kun tillades for IKT-produkter, -tjenester og -processer, hvis de svarer til tillidsniveauet »grundlæggende«.

(80) En europæisk cybersikkerhedscertificeringsordning kan give mulighed for både selvvurdering af overensstemmelse og certificering af IKT-produkter, -tjenester eller -processer. I så fald bør ordningen fastsætte klare og forståelige måder, hvorpå forbrugerne eller andre brugere kan skelne mellem IKT-produkter, -tjenester eller -processer, for hvilke producenten eller udbyderen af IKT-produkter, -tjenester eller -processer er ansvarlig for vurderingen, og IKT-produkter, -tjenester eller -processer, der er certificeret af en tredjepart.

(81) Producenter og udbydere af IKT-produkter, -tjenester eller -processer, som foretager selvvurdering af overensstemmelse, bør kunne udstede og undertegne en EU-overensstemmelseserklæring som led i overensstemmelsesvurderingsproceduren. En EU-overensstemmelseserklæring er et dokument, der angiver, at et bestemt IKT-produkt eller en bestemt IKT-tjeneste eller -proces opfylder kravene i den europæiske cybersikkerhedscertificeringsordning. Ved at udstede og undertegne en EU-overensstemmelseserklæring påtager producenten eller udbyderen af IKT-produkter, -tjenester eller -processer sig ansvaret for, at IKT-produktet, -tjenesten eller -processen opfylder de retlige krav i den europæiske cybersikkerhedscertificeringsordning. En kopi af EU-overensstemmelseserklæringen bør indgives til den nationale cybersikkerhedscertificeringsmyndighed og ENISA.

(82) Producenter eller udbydere af IKT-produkter, -tjenester eller -processer bør stille EU-overensstemmelseserklæringen, den tekniske dokumentation og alle øvrige relevante oplysninger vedrørende IKT-produkternes, -tjenesternes eller -processernes overensstemmelse med en europæisk cybersikkerhedscertificeringsordning til rådighed for den kompetente nationale cybersikkerhedscertificeringsmyndighed i en periode fastsat i den relevante europæiske cybersikkerhedscertificeringsordning. Den tekniske dokumentation bør præcisere de krav, der gælder i henhold til ordningen, og omfatte IKT-produktets, -tjenestens eller -processens udformning, fremstilling og drift, i det omfang dette er relevant for selvvurderingen af overensstemmelse. Den tekniske dokumentation bør være udarbejdet på en måde, der gør det muligt at vurdere, om et IKT-produkt eller en IKT-tjeneste overholder kravene i henhold til den pågældende ordning.

(83) I forvaltningen af den europæiske ramme for cybersikkerhedscertificering tages der højde for såvel inddragelse af medlemsstaterne som passende inddragelse af interessenter, og Kommissionens rolle i forbindelse med planlægning, fremsættelse af forslag, anmodninger, udarbejdelse, vedtagelse og revision af europæiske cybersikkerhedscertificeringsordninger fastlægges.

(84) Kommissionen bør med støtte fra Den Europæiske Cybersikkerhedscertificeringsgruppe (»ECCG«) og Cybersikkerhedscertificeringsgruppen for Interessenter og efter en åben og bred høring udarbejde Unionens rullende arbejdsprogram for europæiske cybersikkerhedscertificeringsordninger og offentliggøre det i form af et ikkebindende instrument. Unionens rullende arbejdsprogram bør være et strategisk dokument, der giver navnlig branchen, nationale myndigheder og standardiseringsorganer mulighed for på forhånd at forberede sig på fremtidige europæiske cybersikkerhedscertificeringsordninger. Unionens rullende arbejdsprogram bør omfatte en flerårig oversigt over de anmodninger om forslag til ordninger, som Kommissionen agter at forelægge for ENISA med henblik på udarbejdelse på grundlag af særlige forhold. Kommissionen bør tage hensyn til Unionens rullende arbejdsprogram, når den udarbejder den rullende plan for IKT-standardisering og standardiseringsanmodninger til europæiske standardiseringsorganisationer. I betragtning af den hurtige indførelse og udbredelse af nye teknologier, forekomsten af hidtil ukendte cybersikkerhedsrisici samt den lovgivningsmæssige udvikling og markedsudviklingen bør Kommissionen eller ECCG have ret til at anmode ENISA om at udarbejde forslag til ordninger, som

ikke er opført i Unionens rullende arbejdsprogram. I sådanne tilfælde bør Kommissionen og ECCG også vurdere nødvendigheden af en sådan anmodninger under hensyntagen til denne forordnings overordnede mål og formål og til behovet for at sikre kontinuitet med hensyn til ENISA's planlægning og brug af ressourcer.

ENISA bør efter en sådan anmodning udarbejde forslag til ordninger for specifikke IKT-produkter, -tjenester eller processer hurtigst muligt. Kommissionen bør evaluere sin anmodnings positive og negative indvirkninger på det specifikke marked, navnlig indvirkningerne på SMV'er, innovation, hindringer for adgang til dette marked og omkostningerne for slutbrugerne. Kommissionen bør tillægges beføjelse til på grundlag af det af ENISA udarbejdede forslag til ordning at vedtage den europæiske cybersikkerhedscertificeringsordning ved hjælp af gennemførelsesretsakter. Under hensyntagen til det generelle formål og de sikkerhedsmål, der er fastsat i denne forordning, bør europæiske cybersikkerhedscertificeringsordninger, der vedtages af Kommissionen, angive et minimumssæt af elementer vedrørende den enkelte ordnings genstand, omfang og funktion. Disse elementer bør bl.a. omfatte cybersikkerhedscertificeringens omfang og genstand, herunder de omfattede kategorier af IKT-produkter, -tjenester og -processer, nærmere specifikation af cybersikkerhedskravene, f.eks. ved henvisning til standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder og det påtænkte tillidsniveau (»grundlæggende«, »betydeligt« eller »højt«), og evalueringsniveauerne, hvor det er relevant. ENISA bør kunne afvise en anmodning fra ECCG. Sådanne afgørelser bør træffes af bestyrelsen og bør begrundes behørigt.

(85) ENISA bør føre et websted med oplysninger om og offentliggørelse af europæiske cybersikkerhedscertificeringsordninger, bl.a. bør indeholde anmodningerne om udarbejdelse af forslag til ordning samt den feedback, der modtages under den høringsproces, som ENISA gennemfører i udarbejdelsesfasen. Webstedet bør også indeholde oplysninger om de europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer, der er udstedt i henhold til denne forordning, herunder oplysninger om tilbagekaldelse eller udløb af sådanne europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer. Webstedet bør også angive de nationale cybersikkerhedscertificeringsordninger, som er blevet erstattet af en europæisk cybersikkerhedscertificeringsordning.

(86) Tillidsniveauet for en europæisk certificeringsordning udgør et grundlag for tillid til, at et IKT-produkt, en IKT-tjeneste eller en IKT-proces opfylder sikkerhedskravene i en bestemt europæisk cybersikkerhedscertificeringsordning. For at sikre sammenhæng i den europæiske ramme for cybersikkerhedscertificering bør en europæisk cybersikkerhedscertificeringsordning kunne præcisere tillidsniveauer for europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer, der udstedes i henhold til den pågældende ordning. Den enkelte europæiske cybersikkerhedsattest kan eventuelt henvise til et af tillidsniveauerne — »grundlæggende«, »betydeligt« eller »højt« — mens EU-overensstemmelseserklæringen eventuelt kun kan henvise til tillidsniveauet »grundlæggende«. Tillidsniveauerne vil indebære en tilsvarende grad af stringens og dybde i evalueringen af IKT-produktet, -tjenesten eller -processen og vil være karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at afbøde eller forhindre hændelser. Hvert tillidsniveau bør være ensartet på tværs af de forskellige sektorspecifikke områder, hvor der anvendes certificering.

(87) En europæisk cybersikkerhedscertificeringsordning kan fastsætte flere evalueringsniveauer, alt efter hvor stringent og dyb den anvendte evalueringsmetode er. Evalueringsniveauerne bør svare til et af tillidsniveauerne og være ledsaget af en passende kombination af tillidskomponenter. For samtlige tillidsniveauer bør IKT-produktet, -tjenesten eller -processen indeholde en række sikre funktioner som nærmere fastsat i ordningen, og som kan omfatte: sikker klar til brug-konfiguration, signeret kode, sikker opdatering og mekanismer til begrænsning af exploits og fuld stack- eller heap-hukommelsesbeskyttelse. Disse funktioner bør være udviklet og vedligeholdes ved hjælp af sikkerhedsorienterede udviklingstilgange

og tilknyttede værktøjer for at sikre, at effektive software- og hardwaremekanismer er indarbejdet på pålidelig vis.

(88) For tillidsniveauet »grundlæggende« bør evalueringen som minimum tage udgangspunkt i følgende tillidskomponenter: Evalueringen bør som minimum omfatte en gennemgang af den tekniske dokumentation for IKT-produktet, -tjenesten eller -processen foretaget af overensstemmelsesvurderingsorganet. Hvis certificeringen omfatter IKT- processer, bør den proces, der anvendes til at udforme, udvikle og vedligeholde et IKT-produkt eller en IKT- tjeneste, også være omfattet af den tekniske gennemgang. I tilfælde, hvor en europæisk cybersikkerhedscertificeringsordning giver mulighed for selv vurdering af overensstemmelsesniveauet, bør det være tilstrækkeligt, hvis producenten eller udbyderen af IKT-produkter, -tjenester eller -processer har udført en selv vurdering af IKT- produktets, -tjenestens eller -processens overensstemmelse med certificeringsordningen.

(89) For tillidsniveauet »betydeligt« bør evalueringen ud over kravene til tillidsniveauet »grundlæggende« som minimum tage udgangspunkt i kontrol af overensstemmelsen af IKT-produktets, -tjenestens eller -processens sikkerhedsfunktioner med den tilhørende tekniske dokumentation.

(90) For tillidsniveauet »højt« bør evalueringen ud over kravene til tillidsniveauet »betydeligt« som minimum tage udgangspunkt i en effektivitetstest, der vurderer modstandsdygtigheden af IKT-produktets, -tjenestens eller -processens sikkerhedsfunktioner over for overlagte cyberangreb udført af personer med betydelige færdigheder og ressourcer.

(91) Anvendelse af europæisk cybersikkerhedscertificering og EU-overensstemmelseserklæringer bør fortsat være frivillig, medmindre andet er fastsat i EU-retten eller medlemsstaternes ret vedtaget i overensstemmelse med EU-retten. I mangel af harmoniseret EU-ret kan medlemsstaterne vedtage nationale tekniske forskrifter, der fastsætter obligatorisk certificering i henhold til en europæisk cybersikkerhedscertificeringsordning i overensstemmelse med Europa- Parlamentets og Rådets direktiv (EU) 2015/1535⁽²⁰⁾. Medlemsstaterne anvender også europæisk cybersikkerhedscertificering i forbindelse med offentlige udbud og Europa-Parlamentets og Rådets direktiv 2014/24/EU⁽²¹⁾.

(92) På nogle områder kan det fremover være nødvendigt at pålægge specifikke krav til cybersikkerhed og at gøre certificering heraf obligatorisk for visse IKT-produkter, -processer eller -tjenester for at forbedre cybersikkerheden i Unionen. Kommissionen bør regelmæssigt overvåge, hvordan de vedtagne europæiske cybersikkerhedscertificeringsordninger påvirker tilgængeligheden af sikre IKT-produkter, -tjenester og -processer i det indre marked, og bør regelmæssigt vurdere, i hvor stor grad certificeringsordningerne anvendes af producenter eller udbydere af IKT- produkter, -tjenester og -processer i Unionen. Effektiviteten af de europæiske certificeringsordninger, og hvorvidt bestemte ordninger bør gøres obligatoriske, bør vurderes i lyset af EU-lovgivningen vedrørende cybersikkerhed, navnlig direktiv (EU) 2016/1148, under hensyntagen til sikkerheden i net- og informationssystemer, der anvendes af operatører af væsentlige tjenester.

(93) Europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer bør hjælpe slutbrugerne til at træffe informerede valg. IKT-produkter, -tjenester og -processer, der er certificeret, eller for hvilke der er udstedt en EU- overensstemmelsesvurdering, bør derfor ledsages af strukturerede oplysninger, der er tilpasset det forventede tekniske niveau hos den tilsigtede slutbruger. Alle sådanne oplysninger bør være tilgængelige online og, hvor det er hensigtsmæssigt, i et fysisk format. Slutbrugeren bør have adgang til oplysninger om certificeringsordningens referencenummer, tillidsniveauet, beskrivelsen af de cybersikkerhedsrisici, som er forbundet med IKT-produktet, -tjenesten eller -processen, samt den udstedende myndighed eller det udstedende organ, eller bør have mulighed for at rekvirere en kopi af den europæiske cybersikkerhedsattest. Desuden bør slutbrugeren informeres om den af producenten eller ud-

byderen af IKT-produkter, -tjenester eller -processer førte støttepolitik i forbindelse med cybersikkerhed, dvs. hvor længe slutbrugeren kan forvente at modtage cybersikkerhedsopdateringer eller -rettelser. Der bør, hvor det er relevant, vejledes om tiltag eller indstillinger, som slutbrugeren kan anvende for at opretholde eller øge IKT-produktets- eller -tjenestens cybersikkerhed, samt om kontaktoplysninger til et centralt kontaktpunkt til at indberette og modtage støtte i tilfælde af cyberangreb (i tillæg til automatisk indberetning). Disse oplysninger bør ajourføres regelmæssigt og gøres tilgængelige på et websted med oplysninger om europæiske cybersikkerhedscertificeringsordninger.

(94) Med sigte på at nå denne forordnings mål og undgå fragmentering af det indre marked bør de nationale cybersikkerhedscertificeringsordninger eller -procedurer for IKT-produkter, -tjenester og -processer, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, ophøre med at have virkning fra en dato, der fastsættes af Kommissionen ved hjælp af gennemførelsesretsakter. Medlemsstaterne bør desuden ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester eller -processer, der allerede er omfattet af en eksisterende europæisk cybersikkerhedscertificeringsordning. Medlemsstaterne bør dog ikke være forhindret i at vedtage eller opretholde nationale cybersikkerhedscertificeringsordninger af nationale sikkerhedshensyn. Medlemsstaterne bør underrette Kommissionen og ECCG om enhver hensigt om at udarbejde nye nationale cybersikkerhedscertificeringsordninger. Kommissionen og ECCG bør evaluere, hvordan de nye nationale cybersikkerhedscertificeringsordninger påvirker et velfungerende indre marked og i lyset af en eventuel strategisk interesse i stedet at anmode om en europæisk cybersikkerhedscertificeringsordning.

(95) Europæiske cybersikkerhedscertificeringsordninger har til formål at bidrage til at harmonisere cybersikkerhedspraksis i Unionen. De skal bidrage til at højne cybersikkerhedsniveauet i Unionen. Udformningen af de europæiske cybersikkerhedscertificeringsordninger bør tage hensyn til og tillade udvikling af innovative løsninger inden for cybersikkerhed.

(96) Europæiske cybersikkerhedscertificeringsordninger bør tage hensyn til eksisterende metoder til udvikling af software og hardware og navnlig til, hvordan hyppige opdateringer af software eller firmware påvirker de individuelle europæiske cybersikkerhedsattester. Europæiske cybersikkerhedscertificeringsordninger bør fastsætte betingelserne for, at en opdatering kan kræve, at et IKT-produkt, en IKT-tjeneste eller en IKT-proces recertificeres, eller at anvendelsesområdet for en specifik europæisk cybersikkerhedsattest indskrænkes, under hensyntagen til opdateringens eventuelt negative indvirkning på overholdelsen af attestens sikkerhedskrav.

(97) Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, bør producenter eller udbydere af IKT-produkter, -tjenester eller -processer kunne indgive ansøgninger om certificering af deres IKT-produkter eller -tjenester til et overensstemmelsesvurderingsorgan efter eget valg over alt i Unionen. Overensstemmelsesvurderingsorganerne bør akkrediteres af et nationalt akkrediteringsorgan, hvis de opfylder visse nærmere krav fastsat i denne forordning. Akkreditering bør udstedes for en periode på højst fem år og bør kunne fornys på samme betingelser, forudsat at overensstemmelsesvurderingsorganet fortsat opfylder kravene. 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 denne forordning.

(98) Henvisninger i national lovgivning til nationale standarder, der er ophørt med at have virkning som følge af ikrafttrædelsen af en europæisk cybersikkerhedscertificeringsordning, kan være en kilde til forvirring. Medlemsstaterne bør derfor afspejle vedtagelsen af en europæisk cybersikkerhedscertificeringsordning i deres nationale lovgivning.

(99) For at sikre ensartede standarder i hele Unionen, lette gensidig anerkendelse og fremme den generelle accept af europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer er det nødvendigt at indføre et peerreviewsystem mellem de nationale cybersikkerhedscertificeringsmyndigheder. Peerreviewet bør omfatte procedurer for tilsyn med IKT-produkters, -tjenesters og -processers overensstemmelse med europæiske cybersikkerhedsattester, for overvågning af de forpligtelser, som producenter eller udbydere af IKT-produkter, -tjenester eller -processer, der foretager selv vurdering, har og for overvågning af overensstemmelsesvurderingsorganer, samt relevansen af ekspertisen hos medarbejderne i organer, der udsteder attester for tillidsniveauet »højt«. Kommissionen bør ved hjælp af gennemførelsesretsakter kunne fastsætte mindst en femårig plan for peerreview samt fastlægge kriterier og metodologier for peerreviewsystemets drift.

(100) Uden at det berører det generelle peerreviewsystem, der skal indføres for alle nationale cybersikkerhedscertificeringsmyndigheder inden for den europæiske ramme for cybersikkerhedscertificering, kan visse certificeringsordninger omfatte en peervurderingsmekanisme for de organer, der udsteder europæiske cybersikkerhedsattester for IKT-produkter, -tjenester og -processer med tillidsniveauet »højt« under sådanne ordninger. ECCG bør støtte gennemførelsen af sådanne peervurderingsmekanismer. Peervurderingerne bør navnlig vurdere, om de pågældende organer udfører deres opgaver på en harmoniseret måde, og kan omfatte appelmekanismer. Resultaterne af peervurderingerne bør offentliggøres. De pågældende organer kan vedtage hensigtsmæssige foranstaltninger for at tilpasse deres praksis og ekspertise i overensstemmelse hermed.

(101) Medlemsstaterne bør udpege en eller flere nationale cybersikkerhedscertificeringsmyndigheder til at føre tilsyn med overholdelsen af de forpligtelser, der følger af denne forordning. En national cybersikkerhedscertificeringsmyndighed kan være en eksisterende eller ny myndighed. En medlemsstat bør også efter aftale med en anden medlemsstat kunne udpege en eller flere nationale cybersikkerhedscertificeringsmyndigheder på denne anden medlemsstats område.

(102) Den nationale cybersikkerhedscertificeringsmyndighed bør navnlig overvåge og håndhæve de forpligtelser, som producenter eller udbydere af IKT-produkter, -tjenester eller -processer, der er etableret på dens respektive område, er underlagt i henhold til EU-overensstemmelseserklæringen, bistå de nationale akkrediteringsorganer med overvågning af og tilsyn med overensstemmelsesvurderingsorganers aktiviteter ved at stille ekspertise og relevante oplysninger til rådighed for dem, bemyndige overensstemmelsesvurderingsorganer til at udføre deres opgaver, hvis sådanne organer opfylder yderligere krav, der er fastsat i en europæisk cybersikkerhedscertificeringsordning, og overvåge relevante udviklinger inden for cybersikkerhedscertificering. De nationale cybersikkerhedscertificeringsmyndigheder bør også behandle klager fra fysiske eller juridiske personer i forbindelse med europæiske cybersikkerhedsattester udstedt af disse myndigheder eller i forbindelse med europæiske cybersikkerhedsattester udstedt af overensstemmelsesvurderingsorganer, når sådanne attester henviser til tillidsniveauet »højt«, undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig

frist. Herudover bør nationale cybersikkerhedscertificeringsmyndigheder samarbejde med andre nationale cybersikkerhedscertificerings myndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters, -tjenesters og -processers manglende overholdelse af denne forordnings krav eller af specifikke cybersikkerhedscertificeringsordninger. Kommissionen bør lette denne udveksling af oplysninger ved at stille et understøttende generelt elektronisk informationssystem til rådighed, f.eks. informations- og kommunikationssystemet for markedsovervågning (ICSMS) og det hurtige varslingssystem for farlige nonfoodprodukter (RAPEX), som allerede anvendes af markedsovervågningsmyndighederne i medfør af forordning (EF) nr. 765/2008.

(103) Med henblik på at sikre en ensartet anvendelse af den europæiske ramme for cybersikkerhedscertificering bør der oprettes en ECCG, som består af repræsentanter for de nationale cybersikkerhedscertificeringsmyndigheder eller andre relevante nationale myndigheder. ECCG's vigtigste opgaver bør være at rådgive og bistå Kommissionens i dens arbejde med at sikre en ensartet gennemførelse og anvendelse af den europæiske ramme for cybersikkerhedscertificering, at bistå og arbejde tæt sammen med ENISA ved udarbejdelsen af forslag til cybersikkerhedscertificeringsordninger, i behørigt begrundede tilfælde at anmode ENISA om at udarbejde et forslag til ordning samt at vedtage udtalelser rettet til ENISA vedrørende forslag til ordninger og til Kommissionen vedrørende vedligeholdelse og revision af eksisterende europæiske cybersikkerhedscertificeringsordninger. ECCG bør lette udvekslingen af god praksis og ekspertise mellem de forskellige nationale cybersikkerhedscertificeringsmyndigheder, der er ansvarlige for bemyndigelse af overensstemmelsesvurderingsorganer og udstedelse af europæiske cybersikkerhedsattester.

(104) For at udbrede kendskabet til og lette accepten af fremtidige europæiske cybersikkerhedsordninger kan Kommissionen udstede generelle eller sektorspecifikke cybersikkerhedsretningslinjer om f.eks. god praksis inden for cybersikkerhed eller ansvarlig cybersikkerhedsadfærd, som fremhæver den positive virkning af certificerede IKT-produkter, -tjenester og -processer.

(105) For yderligere at lette handelen og i erkendelse af, at IKT-forsyningskæderne er globale, kan aftaler om gensidig anerkendelse vedrørende europæiske cybersikkerhedsattester indgås af Unionen i overensstemmelse med artikel 218 i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Kommissionen kan under hensyntagen til rådgivningen fra ENISA og ECCG anbefale, at der indledes relevante forhandlinger. Hver europæisk cybersikkerhedsordning bør fastsætte specifikke betingelser for sådan gensidig anerkendelse med tredjelande.

(106) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011⁽²²⁾.

(107) Undersøgellesproceduren bør anvendes til at vedtage gennemførelsesretsakter om europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester eller -processer, til at vedtage gennemførelsesretsakter om ordninger for ENISA's gennemførelse af undersøgelser, til at vedtage gennemførelsesretsakter om en plan om peerreview af de nationale cybersikkerhedscertificeringsmyndigheder samt til vedtagelse af gennemførelsesretsakter om vilkår, formater og procedurer for de nationale cybersikkerhedscertificerings myndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer til Kommissionen.

(108) Der bør foretages regelmæssig og uafhængig evaluering af ENISA's arbejde. Evalueringen bør tage hensyn til ENISA's mål, til dets arbejdsmetoder og til, om dets opgaver er relevante, navnlig dets opgaver vedrørende operationelt samarbejde på EU-plan. Evalueringen bør desuden vurdere virkningen og effektiviteten af den europæiske ramme for cybersikkerhedscertificering. I tilfælde af en revision bør Kommissionen evaluere, hvordan ENISA's rolle som referencepunkt for rådgivning og ekspertise kan styrkes, og bør desuden evaluere muligheden for, at ENISA får en rolle, som understøtter vurderingen af tredjelandes IKT-produkter, -tjenester og -processer, som ikke er i overensstemmelse med EU-reglerne, når sådanne produkter, tjenester og processer føres ind i Unionen.

(109) Målene for denne forordning kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne, men kan på grund af dens virkning og effekt bedre nås på EU-plan; Unionen kan derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union (TEU). I

overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke videre, end hvad der er nødvendigt for at nå disse mål.

(110) Forordning (EU) nr. 526/2013 bør ophæves —

VEDTAGET DENNE FORORDNING:

AFSNIT I

GENERELLE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

1. Med henblik på at sikre et velfungerende indre marked og opnå et højt niveau af cybersikkerhed, cyberrobusthed og tillid i Unionen fastlægges i denne forordning:

a) mål, opgaver og organisatoriske forhold vedrørende ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), og

b) en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, -tjenester og -processer i Unionen, samt at undgå fragmentering af det indre marked med hensyn til cybersikkerhedscertificeringsordninger i Unionen.

Rammen omhandlet i første afsnit, litra b), finder anvendelse, uden at det berører specifikke bestemmelser i andre EU- retsakter vedrørende frivillig eller obligatorisk certificering.

2. Denne forordning berører ikke medlemsstaternes beføjelser med hensyn til aktiviteter vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område.

Artikel 2

Definitioner

I denne forordning forstås ved:

1) »cybersikkerhed«: de aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, brugerne af sådanne systemer og andre personer berørt af cybertrusler

2) »net- og informationssystem«: et net- og informationssystem som defineret i artikel 4, nr. 1), i direktiv (EU) 2016/1148

3) »national strategi for sikkerheden i net- og informationssystemer«: en national strategi for sikkerheden i net- og informationssystemer som defineret i artikel 4, nr. 3), i direktiv (EU) 2016/1148

4) »operatør af væsentlige tjenester«: en operatør af væsentlige tjenester som defineret i artikel 4, nr. 4), i direktiv (EU) 2016/1148

5) »udbyder af digitale tjenester«: en udbyder af digitale tjenester som defineret i artikel 4, nr. 6), i direktiv (EU) 2016/1148

6) »hændelse«: en hændelse som defineret i artikel 4, nr. 7), i direktiv (EU) 2016/1148

- 7) »håndtering af hændelser«: håndtering af hændelser som defineret i artikel 4, nr. 8), i direktiv (EU) 2016/1148
- 8) »cybertrussel«: enhver potentiel omstændighed, begivenhed eller handling, som kan skade, forstyrre eller på anden måde have en negativ indvirkning på net- og informationssystemer, brugerne af sådanne systemer og andre personer
- 9) »europæisk cybersikkerhedscertificeringsordning«: et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er fastsat på EU-plan, og som finder anvendelse på certificeringen eller overensstemmelsesvurderingen af specifikke IKT-produkter, -tjenester og -processer
- 10) »national cybersikkerhedscertificeringsordning«: et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er udviklet og vedtaget af en national offentlig myndighed, og som finder anvendelse på certificeringen eller overensstemmelsesvurderingen af IKT-produkter, -tjenester og -processer, der er omfattet af den pågældende ordning
- 11) »europæisk cybersikkerhedsattest«: et dokument udstedt af et relevant organ, som attesterer, at et givet IKT-produkt, en given IKT-tjeneste eller en given IKT-proces er blevet evalueret med henblik på overensstemmelse med specifikke sikkerhedskrav fastsat i en europæisk cybersikkerhedscertificeringsordning
- 12) »IKT-produkt«: et element eller en gruppe af elementer i net- og informationssystemer
- 13) »IKT-tjeneste«: en tjeneste, der helt eller hovedsagelig består i overførsel, lagring, indhentning eller behandling af oplysninger ved hjælp af net- og informationssystemer
- 14) »IKT-proces«: et sæt aktiviteter, der udføres for at udforme, udvikle, levere eller vedligeholde et IKT-produkt eller en IKT-tjeneste
- 15) »akkreditering«: akkreditering som defineret i artikel 2, nr. 10), i forordning (EF) nr. 765/2008
- 16) »nationalt akkrediteringsorgan«: et nationalt akkrediteringsorgan som defineret i artikel 2, nr. 11), i forordning (EF) nr. 765/2008
- 17) »overensstemmelsesvurdering«: en overensstemmelsesvurdering som defineret i artikel 2, nr. 12), i forordning (EF) nr. 765/2008
- 18) »overensstemmelsesvurderingsorgan«: et overensstemmelsesvurderingsorgan som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008
- 19) »standard«: en standard som defineret i artikel 2, nr. 1), i forordning (EU) nr. 1025/2012
- 20) »teknisk specifikation«: et dokument, der fastsætter de tekniske krav, som et IKT-produkt, en IKT-tjeneste eller en IKT-proces skal opfylde, eller de dertil hørende overensstemmelsesvurderingsprocedurer
- 21) »tillidsniveau«: et grundlag for tillid til, at et IKT-produkt, en IKT-tjeneste eller en IKT-proces opfylder sikkerhedskravene i en bestemt europæisk cybersikkerhedscertificeringsordning, og en angivelse af, på hvilket niveau et IKT-produkt, en IKT-tjeneste eller en IKT-proces er blevet evalueret uden som sådan at måle IKT-produktets, IKT-tjenestens eller IKT-processens sikkerhed
- 22) »selvvurdering af overensstemmelse«: en handling foretaget af en producent eller udbyder af IKT-produkter, tjenester eller -processer, der evaluerer, hvorvidt IKT-produkterne, -tjenesterne eller -processerne opfylder kravene i en specifik europæisk cybersikkerhedscertificeringsordning.

AFSNIT II

ENISA (DEN EUROPÆISKE UNIONS AGENTUR FOR CYBERSIKKERHED)*KAPITEL I****Mandat og formål****Artikel 3***Mandat**

1. ENISA udfører de opgaver, det tillægges i henhold til denne forordning, med det formål at opnå et højt fælles cybersikkerhedsniveau i hele Unionen, herunder ved aktivt at støtte medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer i at forbedre cybersikkerheden. ENISA fungerer som et referencepunkt for rådgivning om og ekspertise i cybersikkerhed for Unionens institutioner, organer, kontorer og agenturer samt for andre relevante EU- interessenter.

ENISA bidrager til at mindske fragmenteringen af det indre marked ved at udføre de opgaver, det tillægges i henhold til denne forordning.

2. ENISA udfører de opgaver, det tillægges ved EU-retsakter, der fastsætter foranstaltninger med henblik på indbyrdes tilnærmelse af de af medlemsstaternes love og administrative bestemmelser, der vedrører cybersikkerhed.

3. ENISA handler uafhængigt ved udførelsen af sine opgaver, undgår overlap med medlemsstaternes aktiviteter og tager hensyn til medlemsstaternes allerede eksisterende ekspertise.

4. ENISA udvikler sine egne nødvendige ressourcer, herunder teknisk og menneskelig kapacitet og færdigheder, for at udføre de opgaver, det har fået tillagt i henhold til denne forordning.

*Artikel 4***Formål**

1. ENISA fungerer som et ekspertisecenter for cybersikkerhed i kraft af sin uafhængighed, den videnskabelige og tekniske kvalitet af den rådgivning og bistand, det yder, de oplysninger, det leverer, den gennemsigtighed, der er forbundet med dets procedurer, dets driftsmetoder og dets omhu ved udførelsen af sine opgaver.

2. ENISA bistår Unionens institutioner, organer, kontorer og agenturer samt medlemsstaterne med udvikling og gennemførelse af EU-politikker vedrørende cybersikkerhed, herunder sektorspecifikke politikker om cybersikkerhed.

3. ENISA støtter kapacitetsopbygning og beredskab i hele Unionen ved at bistå Unionens institutioner, organer, kontorer og agenturer samt medlemsstaterne og offentlige og private interessenter for at øge beskyttelsen af deres net- og informationssystemer, udvikle og forbedre cyberrobusthed og indsatskapaciteter og udvikle færdigheder og kompetencer inden for cybersikkerhed.

4. ENISA fremmer samarbejde, herunder informationsudveksling og koordinering på EU-plan, mellem medlemsstaterne, Unionens institutioner, organer, kontorer og agenturer og relevante private og offentlige interessenter for så vidt angår spørgsmål vedrørende cybersikkerhed.

5. ENISA bidrager til øget cybersikkerhedskapacitet på EU-plan for at støtte medlemsstaternes tiltag til at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser.

6. ENISA fremmer brugen af europæisk cybersikkerhedscertificering med henblik på at undgå fragmentering af det indre marked. ENISA bidrager til etablering og vedligeholdelse af en europæisk ramme for cybersikkerhedscertificering, jf. afsnit III, for at øge gennemsigtigheden af IKT-produkters, -tjenesters og -processers cybersikkerhedsniveau og dermed styrke tilliden til det digitale indre marked og dets konkurrenceevne.

7. ENISA fremmer et højt niveau af cybersikkerhedsoplysning, herunder cyberhygiejne og cyberfærdigheder blandt borgere, organisationer og virksomheder.

KAPITEL II

Opgaver

Artikel 5

Udvikling og gennemførelse af Unionens politikker og lovgivning

ENISA bidrager til udvikling og gennemførelse af Unionens politikker og lovgivning ved at:

1) bistå og rådgive ved udvikling og revision af Unionens politik og lovgivning inden for cybersikkerhed samt sektorspecifik politik og lovgivningsinitiativer, som involverer cybersikkerhedsanliggender, navnlig ved at levere uafhængige udtalelser og analyser samt udføre forberedende arbejde

2) bistå medlemsstaterne med en konsekvent gennemførelse af Unionens politikker og lovgivning om cybersikkerhed, navnlig i forbindelse med direktiv (EU) 2016/1148, herunder ved hjælp af udstedelse af udtalelser, retningslinjer, levering af rådgivning og bedste praksis om emner som risikostyring, indberetning af hændelser og informationsudveksling, samt ved at lette udvekslingen af bedste praksis mellem de kompetente myndigheder i denne henseende

3) bistå medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer med at udvikle og fremme cybersikkerhedspolitikker, der er forbundet med at understøtte den generelle tilgængelighed eller integritet af den offentligt tilgængelige kerne af det åbne internet

4) bidrage til arbejdet i samarbejdsgruppen, jf. artikel 11 i direktiv (EU) 2016/1148, ved at stille sin ekspertise og bistand til rådighed

5) støtte:

a) udvikling og gennemførelse af Unionens politikker inden for elektroniske identifikations- og tillidstjenester, navnlig gennem rådgivning og udstedelse af tekniske retningslinjer, samt ved at fremme udvekslingen af bedste praksis mellem de kompetente myndigheder

b) fremme af et højere sikkerhedsniveau i elektronisk kommunikation, herunder ved at levere rådgivning og ekspertise, samt ved at fremme udvekslingen af bedste praksis mellem de kompetente myndigheder

c) medlemsstaterne i forhold til at gennemføre specifikke cybersikkerhedsaspekter af Unionens politik og lovgivning vedrørende databaseskyttelse og privatlivets fred, herunder ved efter anmodning at levere rådgivning til Det Europæiske Databaseskyttelsesråd.

6) understøtte en jævnlig gennemgang af Unionens politiske aktiviteter ved at udarbejde en årsrapport om status for gennemførelsen af de respektive retlige rammer vedrørende:

a) oplysninger om medlemsstaternes underretninger om hændelser til samarbejdsgruppen via de centrale kontaktpunkter i henhold til artikel 10, stk. 3, i direktiv (EU) 2016/1148

b) sammenfatninger af de indberetninger om brud på sikkerheden eller tab af integritet, som er modtaget fra tillidstjenesteudbydere, og som forelægges ENISA af tilsynsorganerne i henhold til artikel 19, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014⁽²³⁾

c) indberetninger af sikkerhedshændelser fra udbydere af offentlige elektroniske kommunikationsnet eller af offentligt tilgængelige elektroniske kommunikationstjenester, som forelægges ENISA af de kompetente myndigheder i henhold til artikel 40 i direktiv (EU) 2018/1972.

Artikel 6

Kapacitetsopbygning

1. ENISA bistår:

a) medlemsstaterne i deres bestræbelser på at forbedre forebyggelse, opdagelse og analyse af og kapaciteten til at reagere på cybertrusler og -hændelser ved at stille viden og ekspertise til rådighed for dem

b) medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer med at etablere og gennemføre politikker for offentliggørelse af sårbarheder på frivillig basis

c) Unionens institutioner, organer, kontorer og agenturer i deres bestræbelser på at forbedre forebyggelse, opdagelse og analyse af cybertrusler og -hændelser, og til at forbedre deres kapacitet til at reagere på sådanne cybertrusler og -hændelser, navnlig gennem passende støtte til CERT-EU)

d) medlemsstaterne med udviklingen af nationale CSIRT'er, når der anmodes herom i henhold til artikel 9, stk. 5, i direktiv (EU) 2016/1148

e) medlemsstaterne med udviklingen af nationale strategier for sikkerhed i net- og informationssystemer, når der anmodes herom i henhold til artikel 7, stk. 2, i direktiv (EU) 2016/1148; ENISA skal også fremme udbredelsen af og notere fremskridtene med hensyn til gennemførelsen af disse strategier i hele Unionen med henblik på at fremme bedste praksis

f) Unionens institutioner med udviklingen og revisionen af Unionens strategier vedrørende cybersikkerhed og fremmer deres udbredelse og følger fremskridtene med hensyn til deres gennemførelse

g) de nationale CSIRT'er og Unionens CSIRT'er i deres kapacitetsudbygning, herunder ved at fremme dialog og udveksling af oplysninger for at sikre, at hver CSIRT har et fælles sæt af minimumskapaciteter med hensyn til det aktuelle tekniske niveau og opererer i overensstemmelse med bedste praksis

h) medlemsstaterne ved regelmæssigt og mindst hvert andet år at tilrettelægge cybersikkerhedsøvelserne på EU-plan som omhandlet i artikel 7, stk. 5, og ved at fremsætte politikanbefalinger baseret på vurderingen af øvelserne og de indhøstede erfaringer fra dem

i) relevante offentlige organer ved at tilbyde kurser om cybersikkerhed, hvor det er relevant i samarbejde med interessenter

j) samarbejdsgruppen i forbindelse med udveksling af bedste praksis, navnlig med hensyn til medlemsstaternes identificering af operatører af væsentlige tjenester, herunder i forbindelse med en grænseoverskri-

dende afhængighed vedrørende risici og hændelser, i henhold til artikel 11, stk. 3, litra l), i direktiv (EU) 2016/1148.

2. ENISA støtter informationsudveksling i og mellem sektorer, navnlig i de sektorer, der er opført i bilag II til direktiv (EU) 2016/1148, ved at stille bedste praksis og vejledning om tilgængelige værktøjer og procedurer samt om håndtering af reguleringsmæssige spørgsmål relateret til informationsudveksling til rådighed.

Artikel 7

Operationelt samarbejde på EU-plan

1. ENISA understøtter operationelt samarbejde mellem medlemsstaterne, Unionens institutioner, organer, kontorer og agenturer og mellem interessenter.

2. ENISA samarbejder på det operationelle plan og etablerer synergier med Unionens institutioner, organer, kontorer og agenturer, herunder CERT-EU, med de tjenestegrene, der beskæftiger sig med cyberkriminalitet, og med tilsynsmyndigheder med ansvar for beskyttelse af privatlivets fred og personoplysninger, med henblik på at behandle spørgsmål af fælles interesse, herunder ved at:

- a) udveksle knowhow og bedste praksis
- b) levere rådgivning og udstede retningslinjer om relevante cybersikkerhedsspørgsmål
- c) indføre praktiske ordninger for udførelse af bestemte opgaver efter høring af Kommissionen.

3. ENISA varetager sekretariatsfunktionen for CSIRT-netværket, jf. artikel 12, stk. 2, i direktiv (EU) 2016/1148, og støtter i denne egenskab aktivt informationsudveksling og samarbejdet mellem dets medlemmer.

4. ENISA støtter medlemsstaterne med hensyn til det operationelle samarbejde i CSIRT-netværket ved at:

- a) rådgive om, hvordan de forbedrer deres kapacitet til at forebygge, opdage og reagere på hændelser, og efter anmodning fra en eller flere medlemsstater yde rådgivning i forhold til en specifik cybertrussel
- b) efter anmodning fra en eller flere medlemsstater at bistå i vurderingen af hændelser, der har betydelige eller væsentlige konsekvenser, ved at yde ekspertise og lette den tekniske håndtering af sådanne hændelser, herunder navnlig ved at støtte frivillig udveksling af relevante oplysninger og tekniske løsninger mellem medlemsstaterne
- c) analysere sårbarheder og hændelser på grundlag af offentligt tilgængelige oplysninger eller oplysninger, som medlemsstaterne frivilligt har stillet til rådighed til dette formål, og
- d) efter anmodning fra en eller flere medlemsstater yde støtte i forbindelse med efterfølgende tekniske undersøgelser af hændelser, der har betydelige eller væsentlige konsekvenser som omhandlet i direktiv (EU) 2016/1148.

Ved udøvelsen af disse opgaver indgår ENISA og CERT-EU i et struktureret samarbejde med henblik på at udnytte synergier og undgå overlap af aktiviteter.

5. ENISA tilrettelægger regelmæssigt cybersikkerhedsøvelser på EU-plan og støtter medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer i at tilrettelægge cybersikkerhedsøvelser på deres anmodning. Sådanne cybersikkerhedsøvelser på EU-plan kan omfatte tekniske, operationelle eller strategiske elementer. ENISA tilrettelægger hvert andet år en omfattende samlet øvelse.

Hvor det er relevant, bidrager ENISA også til og hjælper med at tilrettelægge sektorspecifikke cybersikkerhedsøvelser sammen med relevante organisationer, der også deltager i cybersikkerhedsøvelser på EU-plan.

6. ENISA udarbejder i tæt samarbejde med medlemsstaterne regelmæssigt en tilbundsående teknisk EU-cybersikkerhedsrapport om hændelser og cybertrusler, der er baseret på offentligt tilgængelige oplysninger, ENISA's egen analyse og rapporter, som deles af bl.a. medlemsstaternes CSIRT'er eller de ved direktivet (EU) 2016/1148 oprettede centrale kontaktpunkter, begge på frivillig basis, EC3 og CERT-EU.

7. ENISA bidrager til at udvikle en samarbejdsorienteret reaktion på EU- og medlemsstatsplan på væsentlige grænseoverskridende hændelser eller -kriser relateret til cybersikkerhed ved navnlig at:

- a) samle og analysere rapporter fra nationale kilder, der er offentligt tilgængelige eller delt på frivillig basis, med henblik på at bidrage til skabelsen af en fælles situationsforståelse
- b) sikre en effektiv informationsstrøm og sørge for, at der er eskaleringsmekanismer på plads til brug mellem CSIRT-netværket og de tekniske og politiske beslutningstagere på EU-niveau
- c) efter anmodning lette den tekniske håndtering af sådanne hændelser eller kriser, herunder navnlig ved at støtte frivillig udveksling af tekniske løsninger mellem medlemsstaterne
- d) støtte Unionens institutioner, organer, kontorer og agenturer og efter anmodning medlemsstaterne i kommunikation til offentligheden om sådanne hændelser eller kriser
- e) afprøve samarbejdsplaner for reaktionen på sådanne hændelser eller kriser på EU-plan og efter anmodning støtte medlemsstaterne i afprøvningen af sådanne planer på nationalt plan.

Artikel 8

Marked, cybersikkerhedscertificering og standardisering

1. ENISA støtter og fremmer udviklingen og gennemførelsen af Unionens politik vedrørende cybersikkerhedscertificering af IKT-produkter, -tjenester og -processer som fastsat i denne forordnings afsnit III ved:

- a) løbende at overvåge udviklingen på beslægtede standardiseringsområder og anbefale passende tekniske specifikationer til brug for udvikling af europæiske cybersikkerhedscertificeringsordninger i henhold til artikel 54, stk. 1, litra c), i tilfælde, hvor der ikke findes standarder
- b) forberede forslag til europæiske cybersikkerhedscertificeringsordninger (»forslag til ordninger«) for IKT-produkter, -tjenester og -processer i overensstemmelse med artikel 49
- c) evaluere vedtagne europæiske cybersikkerhedscertificeringsordninger i overensstemmelse med artikel 49, stk. 8
- d) deltage i peerreviews i henhold til artikel 59, stk. 4
- e) bistå Kommissionen med at varetage sekretariatsfunktionen for ECCG i henhold til artikel 62, stk. 5.

2. ENISA varetager sekretariatsfunktionen for Cybersikkerhedscertificeringsgruppen for Interessenter i henhold til artikel 22, stk. 4.

3. ENISA samler og offentliggør retningslinjer og udvikler god praksis vedrørende cybersikkerhedskrav til IKT-produkter, -tjenester og -processer i samarbejde med nationale cybersikkerhedscertificeringsmyndigheder og branchen på en formaliseret, struktureret og gennemsigtig måde.

4. ENISA bidrager til kapacitetsopbygning i forbindelse med evaluerings- og certificeringsprocesser ved at samle og udstede retningslinjer og yde støtte til medlemsstaterne på deres anmodning.
5. ENISA fremmer indførelse og udbredelse af europæiske og internationale standarder for risikostyring og for IKT- produkters, -tjenesters og processers sikkerhed.
6. ENISA udarbejder i samarbejde med medlemsstaterne og branchen vejledning og retningslinjer om de tekniske områder vedrørende sikkerhedskrav for operatører af væsentlige tjenester og udbydere af digitale tjenester samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, i henhold til artikel 19, stk. 2, i direktiv (EU) 2016/1148.
7. ENISA udfører og formidler regelmæssige analyser af de vigtigste tendenser på markedet for cybersikkerhed, både på efterspørgsels- og udbudssiden, med henblik på at fremme cybersikkerhedsmarkedet i Unionen.

Artikel 9

Viden og information

ENISA skal:

- a) udføre analyser af nye teknologier og tilvejebringe emnespecifikke vurderinger af de forventede sociale, retlige, økonomiske og reguleringsmæssige konsekvenser af teknologiske innovationer inden for cybersikkerhed
- b) udføre langsigtede strategiske analyser af cybertrusler og -hændelser for at identificere nye tendenser og bidrage til at forebygge hændelser
- c) i samarbejde med eksperter fra medlemsstaternes myndigheder og relevante interessenter levere rådgivning, vejledning og bedste praksis for sikkerheden af net- og informationssystemer, navnlig for sikkerheden af de infrastrukturer, der understøtter sektorerne opført i bilag II til direktiv (EU) 2016/1148, og dem, der anvendes af udbydere af de digitale tjenester, der er opført i bilag III til nævnte direktiv
- d) via en særlig webportal samle, organisere og offentliggøre oplysninger om cybersikkerhed, der leveres af Unionens institutioner, organer, kontorer og agenturer, og oplysninger om cybersikkerhed, der leveres på frivillig basis af medlemsstaterne og private og offentlige interessenter
- e) indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og sammenstille rapporter med henblik på at yde vejledning til borgere, organisationer og virksomheder i hele Unionen.

Artikel 10

Bevidstgørelse og uddannelse

ENISA skal:

- a) øge offentlighedens bevidsthed om risiciene i forbindelse med cybersikkerhed og yde vejledning om god praksis for individuelle brugere, der er målrettet mod borgere, organisationer og virksomheder, herunder cyberhygiejne og cyberfærdigheder
- b) i samarbejde med medlemsstaterne, Unionens institutioner, organer, kontorer og agenturer og branchen tilrettelægge jævnlige informations- og oplysningskampagner for at øge cybersikkerheden og dens synlighed i Unionen og tilskynde til en bred offentlig debat

- c) bistå medlemsstaterne i deres bestræbelser på at øge bevidstheden om cybersikkerhed og fremme uddannelse i cybersikkerhed
- d) støtte tættere koordinering og udveksling af bedste praksis mellem medlemsstaterne om bevidstgørelse om og uddannelse i cybersikkerhed.

Artikel 11

Forskning og innovation

I forbindelse med forskning og innovation skal ENISA:

- a) rådgive Unionens institutioner, organer, kontorer og agenturer og medlemsstaterne om forskningsbehov og -prioriteter inden for cybersikkerhed med henblik på at gøre det muligt effektivt at imødegå nuværende og kommende risici og cybertrusler, herunder hvad angår nye og kommende informations- og kommunikationsteknologier, og med henblik på effektivt at bruge risikoforebyggende teknologier
- b) i tilfælde, hvor Kommissionen har tillagt det de relevante beføjelser, deltage i gennemførelsesfasen af programmer til finansiering af forskning og innovation eller som støttemodtager
- c) bidrage til den strategiske forsknings- og innovationsdagsorden på EU-plan inden for cybersikkerhed.

Artikel 12

Internationalt samarbejde

ENISA skal bidrage til Unionens indsats for at samarbejde med tredjelande og internationale organisationer samt inden for relevante internationale samarbejdsrammer med henblik på at fremme internationalt samarbejde om cybersikkerhed ved:

- a) hvor det er relevant, at deltage som observatør i tilrettelæggelsen af internationale øvelser og analysere og rapportere om resultatet af sådanne øvelser til bestyrelsen
- b) på Kommissionens anmodning at fremme udveksling af bedste praksis
- c) på Kommissionens anmodning at stille ekspertise til rådighed for Kommissionen
- d) at rådgive og støtte Kommissionen i spørgsmål vedrørende aftaler om gensidig anerkendelse af cybersikkerhedsattester med tredjelande i samarbejde med ECCG, der er nedsat i henhold til artikel 62.

KAPITEL III

ENISA's organisation

Artikel 13

ENISA's struktur

ENISA's administrative og ledelsesmæssige struktur består af:

- a) en bestyrelse
- b) et forretningsudvalg
- c) en administrerende direktør

- d) en ENISA-rådgivningsgruppe
- e) et netværk af nationale forbindelsesofficerer.

A f d e l i n g 1

B e s t y r e l s e n

Artikel 14

Bestyrelsens sammensætning

1. Bestyrelsen består af et medlem, der udnævnes af hver medlemsstat, og to medlemmer, der udnævnes af Kommissionen. Alle medlemmer har stemmeret.
2. Hvert medlem af bestyrelsen skal have en suppleant. Denne suppleant repræsenterer medlemmet, når medlemmet ikke er til stede.
3. Bestyrelsesmedlemmerne og deres suppleanter udpeges på grundlag af deres viden inden for cybersikkerhed og under hensyntagen til deres relevante ledelsesmæssige, administrative og budgetmæssige kompetencer. Kommissionen og medlemsstaterne bestræber sig på at begrænse udskiftningen af deres repræsentanter i bestyrelsen med henblik på at sikre kontinuiteten i bestyrelsens arbejde. Kommissionen og medlemsstaterne tilstræber at opnå ligevægt mellem kønnene i bestyrelsen.
4. Mandatperioden for bestyrelsesmedlemmerne og deres suppleanter er fire år. Perioden kan fornyes.

Artikel 15

Bestyrelsens opgaver

1. Bestyrelsen skal:
 - a) fastlægge de overordnede retningslinjer for ENISA's drift og sikre, at ENISA udfører sine opgaver i overensstemmelse med de regler og principper, der er fastsat i denne forordning. Den sikrer endvidere, at der er sammenhæng mellem ENISA's arbejde og aktiviteter, der udføres af medlemsstaterne og på EU-plan
 - b) vedtage ENISA's udkast til det samlede programmeringsdokument, der er omhandlet i artikel 24, før det forelægges for Kommissionen med henblik på en udtalelse
 - c) vedtage ENISA's samlede programmeringsdokument under hensyntagen til Kommissionens udtalelse
 - d) føre tilsyn med gennemførelsen af det flerårige og det årlige arbejdsprogram, der er omfattet af det samlede programmeringsdokument
 - e) vedtage ENISA's årsbudget og varetage andre funktioner i relation til ENISA's budget i overensstemmelse med kapitel IV
 - f) evaluere og vedtage den konsoliderede årsberetning om ENISA's virksomhed, herunder regnskaberne og en beskrivelse af, hvorledes ENISA har opfyldt sine resultatindikatorer, sende både årsberetningen og evalueringen heraf til Europa- Parlamentet, Rådet, Kommissionen og Revisionsretten senest den 1. juli i det følgende år og offentliggøre årsberetningen
 - g) vedtage de finansielle bestemmelser for ENISA, jf. artikel 32

- h) vedtage en strategi for bekæmpelse af svig, som står i forhold til risikoen for svig, under hensyn til en cost-benefit- analyse af de foranstaltninger, der skal gennemføres
- i) vedtage regler for forebyggelse og håndtering af interessekonflikter i forhold til medlemmerne
- j) sikre passende opfølgning på resultater og henstillinger som følge af undersøgelser foretaget af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og forskellige interne eller eksterne auditrapporter og evalueringer
- k) vedtage sin forretningsorden, herunder regler for foreløbige afgørelser om delegation af specifikke opgaver, i henhold til artikel 19, stk. 7
- l) over for ENISA's personale udøve de beføjelser, som ved vedtægten for tjenestemænd og ansættelsesvilkårene for Unionens øvrige ansatte (»tjenestemandsvedtægten« og »ansættelsesvilkårene for øvrige ansatte«) som fastlagt i Rådets forordning (EØF, Euratom, EKSF) nr. 259/68⁽²⁴⁾ er tillagt ansættelsesmyndigheden og den myndighed, der har beføjelse til at indgå ansættelseskontrakter (»ansættelsesmyndighederne«), i overensstemmelse med denne artikels stk. 2
- m) vedtage gennemførelsesbestemmelser til tjenestemandsvedtægten og ansættelsesvilkårene for øvrige ansatte i overensstemmelse med proceduren i tjenestemandsvedtægtens artikel 110
- n) udnævne den administrerende direktør og, hvis det er relevant, forlænge den administrerende direktørs mandatperiode eller afskedige vedkommende i overensstemmelse med artikel 36
- o) udnævne en regnskabsfører, som kan være Kommissionens regnskabsfører, som er fuldstændig uafhængig i udøvelsen af sit hverv
- p) træffe alle afgørelser vedrørende etablering af ENISA's interne strukturer og om nødvendigt ændring heraf under hensyntagen til ENISA's aktivitetsbehov og til forsvarlig budgetforvaltning
- q) bemyndige etablering af samarbejdsordninger med henblik på artikel 7
- r) bemyndige etablering eller indgåelse af samarbejdsordninger i overensstemmelse med artikel 42.

2. Bestyrelsen vedtager i overensstemmelse med tjenestemandsvedtægtens artikel 110 en afgørelse baseret på tjenestemandsvedtægtens artikel 2, stk. 1, og artikel 6 i ansættelsesvilkårene for øvrige ansatte om delegation af de relevante beføjelser som ansættelsesmyndighed til den administrerende direktør og fastlæggelse af betingelserne for at suspendere denne delegation af beføjelser. Den administrerende direktør kan videredelegere disse beføjelser.

3. Under helt særlige omstændigheder kan bestyrelsen vedtage en afgørelse om midlertidigt at suspendere de beføjelser som ansættelsesmyndighed, der er delegeret til den administrerende direktør, og eventuelle beføjelser som ansættelsesmyndighed, som den administrerende direktør måtte have videredelegeret, og i stedet selv udøve dem eller delegerer dem til et af sine medlemmer eller til en anden ansat end den administrerende direktør.

Artikel 16

Bestyrelsens formand

Bestyrelsen vælger med to tredjedeles flertal en formand og en næstformand blandt sine medlemmer. Deres mandatperiode er fire år, der kan fornyes én gang. Hvis en formand eller næstformand ophører med at være medlem af bestyrelsen under sin mandatperiode, ophører mandatperioden dog automatisk

samtidig. Næstformanden træder uden videre i stedet for formanden, hvis formanden er forhindret i at udøve sit hverv.

Artikel 17

Bestyrelsens møder

1. Det påhviler bestyrelsens formand at indkalde til dens møder.
2. Bestyrelsen afholder mindst to ordinære møder om året. Den afholder endvidere ekstraordinære møder efter anmodning fra formanden, på Kommissionens anmodning eller på anmodning af mindst en tredjedel af dens medlemmer.
3. Den administrerende direktør deltager i bestyrelsens møder, men har ikke stemmeret.
4. Medlemmerne af ENISA-Rådgivningsgruppen kan deltage i bestyrelsens møder efter invitation fra formanden, men har ikke stemmeret.
5. Bestyrelsesmedlemmerne og deres stedfortrædere kan under bestyrelsesmøderne bistås af rådgivere eller eksperter, såfremt forretningsordenen tillader det.
6. ENISA varetager bestyrelsens sekretariatsfunktion.

Artikel 18

Bestyrelsens afstemningsregler

1. Bestyrelsen træffer sine afgørelser med flertal blandt medlemmerne.
2. Der kræves et flertal på to tredjedele af bestyrelsens medlemmer for at vedtage det samlede programmeringsdokument og årsbudgettet og for at udnævne eller afskedige den administrerende direktør eller forlænge dennes mandatperiode.
3. Hvert medlem har én stemme. Hvis et medlem ikke er til stede, har medlemmets suppleant medlemmets stemmeret.
4. Bestyrelsens formand deltager i afstemningen.
5. Den administrerende direktør deltager ikke i afstemningen.
6. I bestyrelsens forretningsorden fastsættes mere detaljerede afstemningsregler, navnlig regler om, hvornår et medlem kan handle på et andet medlems vegne.

A f d e l i n g 2

F o r r e t n i n g s u d v a l g e t

Artikel 19

Forretningsudvalget

1. Bestyrelsen bistås af et forretningsudvalg.
2. Forretningsudvalget skal:

- a) forberede de afgørelser, der skal vedtages af bestyrelsen
 - b) i samarbejde med bestyrelsen sikre passende opfølgning på de resultater og henstillinger, der hidrører fra undersøgelser foretaget af OLAF og fra forskellige interne eller eksterne auditrapporter og evalueringer
 - c) uden at det berører den administrerende direktørs ansvarsområder, jf. artikel 20, bistå og rådgive den administrerende direktør i gennemførelsen af bestyrelsens afgørelser vedrørende administrative og budgetmæssige spørgsmål i henhold til artikel 20.
3. Forretningsudvalget består af fem medlemmer. Medlemmerne af forretningsudvalget udpeges blandt bestyrelsesmedlemmerne. Et af medlemmerne er formanden for bestyrelsen, der også kan være formand for forretningsudvalget, og et andet medlem er en af repræsentanterne for Kommissionen. Ved udpegelserne af medlemmerne af forretningsudvalget tilstræbes det at sikre en ligevægt mellem kønnene i forretningsudvalget. Den administrerende direktør deltager i bestyrelsens møder, men har ikke stemmeret.
4. Forretningsudvalgsmedlemmerne har en mandatperiode på fire år. Perioden kan fornyes.
5. Forretningsudvalget mødes mindst én gang hver tredje måned. Formanden for forretningsudvalget indkalder til yderligere møder på anmodning af forretningsudvalgets medlemmer.
6. Bestyrelsen vedtager forretningsudvalgets forretningsorden.
7. Hvis det er nødvendigt i hastende tilfælde, kan forretningsudvalget træffe visse foreløbige afgørelser på bestyrelsens vegne, navnlig vedrørende den administrative forvaltning, herunder suspendering af delegationen af beføjelser som ansættelsesmyndighed, og budgetanliggender. En sådan foreløbig afgørelse meddeles bestyrelsen hurtigst muligt. Bestyrelsen afgør derefter, om den foreløbige afgørelse skal godkendes eller afvises, senest tre måneder efter, at afgørelsen blev truffet. Forretningsudvalget træffer ikke afgørelser på bestyrelsens vegne, som kræver godkendelse af et flertal på to tredjedele af bestyrelsens medlemmer.

A f d e l i n g 3

D e n a d m i n i s t r e r e n d e d i r e k t ø r

Artikel 20

Den administrerende direktørs opgaver

1. ENISA ledes af den administrerende direktør, som udfører sit hverv i uafhængighed. Den administrerende direktør står til ansvar over for bestyrelsen.
2. Den administrerende direktør aflægger rapport til Europa-Parlamentet om udførelsen af sit hverv, når denne anmodes herom. Rådet kan anmode den administrerende direktør om at aflægge rapport om udførelsen af dennes hverv.
3. Den administrerende direktør er ansvarlig for:
 - a) den daglige administration af ENISA
 - b) at gennemføre de afgørelser, der træffes af bestyrelsen
 - c) at udarbejde det samlede programmeringsdokument og forelægge det for bestyrelsen til godkendelse før dets fremsendelse til Kommissionen

- d) at gennemføre det samlede programmeringsdokument og aflægge rapport til bestyrelsen herom
- e) at udarbejde den konsoliderede årsberetning om ENISA's aktiviteter, bl.a. om gennemførelsen af ENISA's årlige arbejdsprogram, og forelægge denne for bestyrelsen til vurdering og godkendelse
- f) at udarbejde en handlingsplan til opfølgning på konklusionerne fra retrospektive evalueringer og aflægge en statusrapport til Kommissionen hvert andet år
- g) at udarbejde en handlingsplan til opfølgning på konklusionerne fra interne eller eksterne auditrapporter samt undersøgelser fra OLAF og aflægge en statusrapport hvert andet år til Kommissionen og regelmæssigt til bestyrelsen
- h) at udarbejde udkast til de i artikel 32 omhandlede finansielle bestemmelser for ENISA
- i) at udarbejde ENISA's udkast til overslag over indtægter og udgifter og gennemføre dets budget
- j) at beskytte Unionens finansielle interesser gennem forholdsregler til forebyggelse af svig, korruption og enhver anden ulovlig aktivitet, gennem effektiv kontrol og, hvis der konstateres uregelmæssigheder, gennem inddrivelse af uretmæssigt udbetalte beløb og om nødvendigt gennem administrative og finansielle sanktioner, der er effektive og forholdsmæssige og har en afskrækkende virkning
- k) at udarbejde ENISA's strategi for bekæmpelse af svig og forelægge denne for bestyrelsen til godkendelse
- l) at etablere og opretholde kontakt med erhvervslivet og forbrugerorganisationer med henblik på at sikre en løbende dialog med relevante interessenter
- m) regelmæssig udveksling af synspunkter og oplysninger med Unionens institutioner, organer, kontorer og agenturer om deres cybersikkerhedsrelaterede aktiviteter for at sikre sammenhæng i udviklingen og gennemførelsen af Unionens politik
- n) at udføre andre opgaver, som den administrerende direktør pålægges ved denne forordning.

4. Er det nødvendigt og inden for rammerne af ENISA's formål og opgaver, kan den administrerende direktør nedsætte ad hoc-arbejdsgrupper bestående af eksperter, herunder eksperter fra medlemsstaternes kompetente myndigheder. Den administrerende direktør underretter bestyrelsen herom på forhånd. Procedurene vedrørende navnlig sammensætningen af arbejdsgrupperne, den administrerende direktørs udnævnelse af eksperterne til arbejdsgrupperne og arbejdsgruppernes virke fastsættes i ENISA's interne forretningsgange.

5. Hvis det er nødvendigt med henblik på at udføre ENISA's opgaver på en effektiv og virkningsfuld måde og på grundlag af en hensigtsmæssig cost-benefit-analyse, kan den administrerende direktør beslutte at etablere et eller flere lokale kontorer i en eller flere medlemsstater. Inden det beslutes at oprette et lokalt kontor, anmoder den administrerende direktør om en udtalelse fra den eller de berørte medlemsstater, herunder den medlemsstat, hvor ENISA's hovedsæde er beliggende, og indhenter forudgående samtykke fra Kommissionen og bestyrelsen. I tilfælde af uenighed under høringsprocessen mellem den administrerende direktør og de berørte medlemsstater, forelægges spørgsmålet Rådet til drøftelse. Det samlede antal ansatte på alle lokale kontorer skal begrænses til et minimum og må ikke udgøre mere end 40 % af ENISA's antal ansatte i den medlemsstat, hvor ENISA's hovedsæde er beliggende. Antallet af ansatte på det enkelte lokale kontor må ikke udgøre mere end 10 % af ENISA's samlede antal ansatte i den medlemsstat, hvor ENISA's hovedsæde er beliggende.

I afgørelsen om oprettelse af et lokalt kontor fastsættes omfanget af de aktiviteter, der skal udføres af det lokale kontor, således at der undgås unødige omkostninger og overlap af ENISA's administrative funktioner.

Afdeling 4

ENISA-rådgivningsgruppen, cybersikkerhedscertificeringsgruppen for interessenter og netværket af nationale forbindelsesofficerer

Artikel 21

ENISA-Rådgivningsgruppen

1. På forslag af den administrerende direktør nedsætter bestyrelsen på gennemsigtig vis en ENISA-rådgivningsgruppe bestående af anerkendte eksperter, der repræsenterer de relevante interessenter såsom IKT-industrien, udbydere af elektroniske kommunikationsnet eller -tjenester til offentligheden, SMV'er, operatører af væsentlige tjenester, forbrugergrupper, akademiske eksperter inden for cybersikkerhed og repræsentanter for de kompetente myndigheder, der er givet meddelelse om i overensstemmelse med direktiv (EU) 2018/1972, europæiske standardiseringsorganisationer, samt af retshåndhævende myndigheder og databeskyttelsestilsynsmyndigheder. Bestyrelsen bestræber sig på at sikre en passende kønsmæssig og geografisk balance samt balance mellem de forskellige interessentgrupper.
2. Procedurerne for ENISA-Rådgivningsgruppen, vedrørende navnlig gruppens sammensætning, den administrerende direktørs forslag som omhandlet i stk. 1, antal og udpegelse af dens medlemmer og ENISA-Rådgivningsgruppens virke, fastlægges i ENISA's interne forretningsgange og offentliggøres.
3. ENISA-Rådgivningsgruppen ledes af den administrerende direktør eller af en person udpeget af den administrerende direktør fra sag til sag.
4. Mandatperioden for medlemmerne af ENISA-Rådgivningsgruppen er to et halvt år. Medlemmer af bestyrelsen kan ikke være medlemmer af ENISA-Rådgivningsgruppen. eksperter fra Kommissionen og medlemsstaterne har ret til at være til stede på møderne og deltage i arbejdet i ENISA-Rådgivningsgruppen. Repræsentanter for andre organer, som den administrerende direktør skønner er relevante, og som ikke er medlemmer af ENISA-Rådgivningsgruppen, kan indbydes til at være til stede på ENISA-Rådgivningsgruppens møder og deltage i dens arbejde.
5. ENISA-Rådgivningsgruppen rådgiver ENISA med hensyn til udførelsen af dets opgaver, bortset fra anvendelsen af bestemmelserne i denne forordnings afsnit III. Den rådgiver navnlig den administrerende direktør om udarbejdelsen af forslag til ENISA's årlige arbejdsprogram samt om varetagelse af kommunikation med de relevante interessenter om spørgsmål, der vedrører det årlige arbejdsprogram.
6. ENISA-Rådgivningsgruppen underretter regelmæssigt bestyrelsen om sine aktiviteter.

Artikel 22

Cybersikkerhedscertificeringsgruppen for Interessenter

1. Der nedsættes en cybersikkerhedscertificeringsgruppe for interessenter.
2. Cybersikkerhedscertificeringsgruppen for Interessenter sammensættes af medlemmer, der udvælges blandt anerkendte eksperter, som repræsenterer de relevante interessenter. Kommissionen udvælger medlemmer af Cybersikkerhedscertificeringsgruppen for Interessenter efter en gennemsigtig og åben indkal-

delse på forslag af ENISA, idet der sikres balance mellem de forskellige interessentgrupper samt en passende kønsmæssig og geografisk balance.

3. Cybersikkerhedscertificeringsgruppen for Interessenter:

a) rådgiver Kommissionen om strategiske spørgsmål vedrørende den europæiske ramme for cybersikkerhedscertificering

b) rådgiver på anmodning ENISA om generelle og strategiske spørgsmål vedrørende ENISA's opgaver i relation til markedet, cybersikkerhedscertificering og standardisering

c) bistår Kommissionen med udarbejdelsen af EU's rullende arbejdsprogram som omhandlet i artikel 47

d) afgiver udtalelse om Unionens rullende arbejdsprogram i henhold til artikel 47, stk. 4, og

e) rådgiver i hastende tilfælde Kommissionen og ECCG om behovet for yderligere certificeringsordninger, der ikke er omfattet af Unionens rullende arbejdsprogram, jf. artikel 47 og 48.

4. Cybersikkerhedscertificeringsgruppen for Interessenter ledes i fællesskab af repræsentanter for Kommissionen og ENISA, og dens sekretariatsfunktion varetages af ENISA.

Artikel 23

Netværk af nationale forbindelsesofficerer

1. På forslag fra den administrerende direktør opretter bestyrelsen et netværk af nationale forbindelsesofficerer bestående af repræsentanter fra alle medlemsstaterne (»nationale forbindelsesofficerer«). Hver medlemsstat udpeger én repræsentant til netværket af nationale forbindelsesofficerer. Møderne i netværket af nationale forbindelsesofficerer kan afholdes i forskellige ekspertsammensætninger.

2. Netværket af nationale forbindelsesofficerer skal navnlig fremme udvekslingen af oplysninger mellem ENISA og medlemsstaterne og støtte ENISA i formidlingen af dets aktiviteter, resultater og henstillinger til de relevante interessenter i hele Unionen.

3. Nationale forbindelsesofficerer fungerer som et kontaktpunkt på nationalt plan for at lette samarbejdet mellem ENISA og nationale eksperter som led i gennemførelsen af ENISA's årlige arbejdsprogram.

4. Mens nationale forbindelsesofficerer skal arbejde tæt sammen med deres respektive medlemsstaters repræsentanter i bestyrelsen, må det arbejde, som netværket af nationale forbindelsesofficerer selv udfører, ikke overlappe hverken bestyrelsens eller andre EU-foras arbejde.

5. Funktionerne og procedurerne for netværket af nationale forbindelsesofficerer fastlægges i ENISA's interne forretningsgange og offentliggøres.

A f d e l i n g 5

D r i f t

Artikel 24

Samlet programmeringsdokument

1. ENISA skal virke i overensstemmelse med det samlede programmeringsdokument, som omfatter dets årlige og flerårige arbejdsprogram, og som skal indeholde alle planlagte aktiviteter.

2. Hvert år udarbejder den administrerende direktør under hensyntagen til Kommissionens retningslinjer det samlede programmeringsdokument, som omfatter det årlige og flerårige arbejdsprogram med de mod-

svarende planer for økonomiske og menneskelige ressourcer, jf. artikel 32 i Kommissionens delegerede forordning (EU) nr. 1271/2013⁽²⁵⁾.

3. Senest den 30. november hvert år vedtager bestyrelsen det samlede programmeringsdokument omhandlet i stk. 1 og sender det til Europa-Parlamentet, Rådet og Kommissionen senest den 31. januar det følgende år sammen med eventuelle efterfølgende ajourførte udgaver af dokumentet.

4. Det samlede programmeringsdokument bliver endeligt efter den endelige vedtagelse af Unionens almindelige budget og justeres om nødvendigt.

5. Det årlige arbejdsprogram skal indeholde detaljerede mål og forventede resultater, herunder resultatindikatorer. Det skal også indeholde en beskrivelse af de foranstaltninger, der skal finansieres, og oplysninger om de økonomiske og menneskelige ressourcer, der afsættes til hver foranstaltning, i overensstemmelse med principperne om aktivitetsbaseret budgetlægning og -forvaltning. Det årlige arbejdsprogram skal være i overensstemmelse med det i stk. 7 omhandlede flerårige arbejdsprogram. Det skal klart anføres i programmet, hvilke opgaver der er blevet tilføjet, ændret eller slettet i forhold til det foregående regnskabsår.

6. Bestyrelsen ændrer det vedtagne årlige arbejdsprogram, hvis ENISA tillægges nye opgaver. Væsentlige ændringer af det årlige arbejdsprogram vedtages efter samme procedure som det oprindelige årlige arbejdsprogram. Bestyrelsen kan delegere beføjelsen til at foretage ikkevæsentlige ændringer i det årlige arbejdsprogram til den administrerende direktør.

7. Det flerårige arbejdsprogram skal angive den overordnede strategiske programmering, herunder mål, forventede resultater og resultatindikatorer. Det skal også indeholde ressourceplanen, herunder det flerårige budget og personale.

8. Ressourceplanen ajourføres hvert år. Den strategiske programmering ajourføres efter behov, navnlig med henblik på at tage højde for resultatet af den evaluering, der er omhandlet i artikel 67.

Artikel 25

Interesseerklæring

1. Bestyrelsesmedlemmerne, den administrerende direktør samt embedsmænd, der midlertidigt er stillet til rådighed af medlemsstaterne, afgiver hver især en loyalitetserklæring og en erklæring, hvori de anfører, hvorvidt der foreligger direkte eller indirekte interesser, der kan anses for at berøre deres uafhængighed. Erklæringerne skal være præcise og fuldstændige og afgives skriftligt hvert år og ajourføres, når det er nødvendigt.

2. Bestyrelsesmedlemmerne, den administrerende direktør og eksterne eksperter, der deltager i ad hoc-arbejdsgrupper, gør hver især på præcis og fyldestgørende vis senest ved hvert mødes start opmærksom på eventuelle interesser, som kan anses for at berøre deres uafhængighed med hensyn til de punkter, der er på dagsordenen, og afholder sig fra at deltage i drøftelserne af og afstemningen om sådanne punkter.

3. ENISA fastsætter i sine interne forretningsgange bestemmelser om, hvordan de i stk. 1 og 2 omhandlede regler om interesseerklæringer gennemføres i praksis.

*Artikel 26***Gennemsigtighed**

1. ENISA sikrer, at der er en høj grad af gennemsigtighed i dets aktiviteter i overensstemmelse med artikel 28.
2. ENISA sikrer, at offentligheden og eventuelle interesserede parter får passende, objektive, pålidelige og let tilgængelige oplysninger, især vedrørende resultaterne af dets arbejde. Det offentliggør også interesseerklæringer afgivet i overensstemmelse med artikel 25.
3. Bestyrelsen kan på forslag af den administrerende direktør give interesserede parter tilladelse til at følge procedurerne i forbindelse med nogle af ENISA's aktiviteter.
4. ENISA fastsætter i sine interne forretningsgange bestemmelser om, hvordan de i stk. 1 og 2 omhandlede regler om gennemsigtighed gennemføres i praksis.

*Artikel 27***Fortrolighed**

1. Uden at det berører artikel 28, må ENISA ikke videregive oplysninger, som det behandler eller modtager, og for hvilke der foreligger en begrundet begæring om, at de holdes fortrolige, til tredjemand.
2. Bestyrelsesmedlemmerne, den administrerende direktør, medlemmerne af ENISA-Rådgivningsgruppen, eksterne eksperter, der deltager i ad hoc-arbejdsgrupperne, samt ENISA's personale, herunder embedsmænd, der midlertidigt er udstationeret fra medlemsstaterne, skal, selv efter at deres hverv er ophørt, overholde forpligtelsen til fortrolighed som fastsat i artikel 339 i TEUF.
3. ENISA fastsætter i sine interne forretningsgange bestemmelser om, hvordan de i stk. 1 og 2 omhandlede regler om fortrolighed gennemføres i praksis.
4. Bestyrelsen beslutter, såfremt det er nødvendigt for udførelsen af ENISA's opgaver, at tillade ENISA at behandle klassificerede oplysninger. I så fald vedtager ENISA efter aftale med Kommissionens tjenestegrene sikkerhedsregler, der bygger på sikkerhedsprincipperne i Kommissionens afgørelse (EU, Euratom) 2015/443⁽²⁶⁾ og 2015/444⁽²⁷⁾. Disse sikkerhedsregler skal omfatte bestemmelser om udveksling, behandling og lagring af klassificerede oplysninger.

*Artikel 28***Aktindsigt**

1. Forordning (EF) nr. 1049/2001 finder anvendelse på ENISA's dokumenter.
2. Bestyrelsen vedtager de praktiske bestemmelser til gennemførelse af forordning (EF) nr. 1049/2001 senest den 28. december 2019.
3. De beslutninger, som ENISA træffer efter artikel 8 i forordning (EF) nr. 1049/2001, kan gøres til genstand for en klage til Den Europæiske Ombudsmand i henhold til artikel 228 i TEUF eller en klage indbragt for Den Europæiske Unions Domstol i henhold til artikel 263 i TEUF.

KAPITEL IV

Opstilling og struktur for ENISA's budget*Artikel 29***Opstilling af ENISA's budget**

1. Hvert år udarbejder den administrerende direktør et udkast til overslag over ENISA's indtægter og udgifter for det følgende regnskabsår og forelægger det for bestyrelsen ledsaget af et udkast til stillingsfortegnelse. Der skal være balance mellem indtægter og udgifter.
2. Hvert år vedtager bestyrelsen på grundlag af udkastet til overslag et overslag over ENISA's indtægter og udgifter for det følgende regnskabsår.
3. Bestyrelsen fremsender senest den 31. januar hvert år overslaget, der skal være en del af udkastet til det samlede programmeringsdokument, til Kommissionen og de tredjelande, som Unionen har indgået aftaler med som omhandlet i artikel 42, stk. 2.
4. På grundlag af dette overslag opfører Kommissionen i forslaget til Unionens almindelige budget de overslag, den skønner nødvendige for stillingsfortegnelsen, og de bidrag, der skal ydes over Unionens almindelige budget, og fremsender overslaget til Europa-Parlamentet og Rådet i overensstemmelse med artikel 314 i TEUF.
5. Europa-Parlamentet og Rådet godkender bevillingen af bidraget fra Unionen til ENISA.
6. Europa-Parlamentet og Rådet vedtager ENISA's stillingsfortegnelse.
7. Bestyrelsen vedtager ENISA's budget sammen med det samlede programmeringsdokument. ENISA's budget bliver endeligt efter den endelige vedtagelse af Unionens almindelige budget. Om nødvendigt tilpasser bestyrelsen ENISA's budget og dets samlede programmeringsdokument i overensstemmelse med Unionens almindelige budget.

*Artikel 30***Struktur for ENISA's budget**

1. Uden at det berører andre ressourcer, udgøres ENISA's indtægter af:
 - a) et bidrag fra Unionens almindelige budget
 - b) formålsbestemte indtægter med henblik på specifikke udgiftsposter i overensstemmelse med de finansielle bestemmelser omhandlet i artikel 32
 - c) EU-finansiering i form af delegationsaftaler eller ad hoc-tilskud i overensstemmelse med de finansielle bestemmelser omhandlet i artikel 32 og med bestemmelserne i de relevante instrumenter til gennemførelse af Unionens politikker
 - d) bidrag fra tredjelande, der deltager i ENISA's arbejde, som omhandlet i artikel 42
 - e) eventuelle frivillige bidrag fra medlemsstaterne i form af pengebeløb eller naturalier.
- Medlemsstater, der yder frivillige bidrag i henhold til første afsnit litra e), kan ikke påberåbe sig nogen specifikke rettigheder eller tjenester som følge heraf.

2. ENISA's udgifter omfatter udgifter til personale, administrativ og teknisk bistand, infrastruktur og driftsudgifter samt udgifter som følge af kontrakter med tredjemand.

Artikel 31

Gennemførelse af ENISA's budget

1. Den administrerende direktør er ansvarlig for gennemførelsen af ENISA's budget.
2. Kommissionens interne revisor varetager i forhold til ENISA de samme funktioner, som er tildelt denne i forhold til Kommissionens tjenestegrene.
3. ENISA's regnskabsfører sender det foreløbige årsregnskab (år N) til Kommissionens regnskabsfører og Revisionsretten senest den 1. marts i det følgende regnskabsår (år N+1).
4. Ved modtagelsen af Revisionsrettens bemærkninger om ENISA's foreløbige årsregnskab i henhold til artikel 246 i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046⁽²⁸⁾ opstiller ENISA's regnskabsfører på eget ansvar ENISA's endelige årsregnskab og forelægger det for bestyrelsen til udtalelse.
5. Bestyrelsen afgiver en udtalelse om ENISA's endelige årsregnskab.
6. Den administrerende direktør sender senest den 31. marts i år N + 1 beretningen om budgetforvaltningen og den økonomiske forvaltning til Europa-Parlamentet, Rådet, Kommissionen og Revisionsretten.
7. ENISA's regnskabsfører sender senest den 1. juli i år N+1 ENISA's endelige årsregnskab ledsaget af bestyrelsens udtalelse til Europa-Parlamentet, Rådet, Kommissionens regnskabsfører og Revisionsretten.
8. ENISA's regnskabsfører sender på samme dato som fremsendelsen af ENISA's endelige årsregnskaber ligeledes en forvaltningserklæring, der dækker disse endelige årsregnskaber, til Revisionsretten, med kopi til Kommissionens regnskabsfører.
9. Den administrerende direktør offentliggør ENISA's endelige regnskab i Den Europæiske Unions Tidende senest den 15. november i år N+1.
10. Den administrerende direktør sender senest den 30. september i år N + 1 Revisionsretten et svar på dens bemærkninger og sender ligeledes en kopi af svaret til bestyrelsen og Kommissionen.
11. Hvis Europa-Parlamentet anmoder derom, forelægger den administrerende direktør alle de oplysninger, der er nødvendige for, at dechargeproceduren for det pågældende regnskabsår kan forløbe tilfredsstillende, for Europa-Parlamentet, jf. artikel 261, stk. 3, i Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046.
12. Efter henstilling fra Rådet meddeler Europa-Parlamentet inden den 15. maj i år N + 2 den administrerende direktør decharge for gennemførelsen af budgettet for år N.

Artikel 32

Finansielle bestemmelser

De finansielle bestemmelser for ENISA vedtages af bestyrelsen efter høring af Kommissionen. Disse finansielle bestemmelser må kun afvige fra delegeret forordning (EU) nr. 1271/2013, hvis dette er særligt nødvendigt for ENISA's drift, og Kommissionen på forhånd har givet sit samtykke.

*Artikel 33***Bekæmpelse af svig**

1. For at lette bekæmpelsen af svig, korruption og andre retsstridige handlinger i henhold til Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013⁽²⁹⁾ tiltræder ENISA senest den 28. december 2019 den interinstitutionelle aftale af 25. maj 1999 mellem Europa-Parlamentet, Rådet for Den Europæiske Union og Kommissionen for De Europæiske Fællesskaber om de interne undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF)⁽³⁰⁾. ENISA vedtager passende bestemmelser, som skal finde anvendelse på ENISA's medarbejdere, under anvendelse af den model, der findes i bilaget til nævnte aftale.
2. Revisionsretten har beføjelse til gennem bilagskontrol og kontrol på stedet at kontrollere alle tilskudsmødtager, kontrahenter og underkontrahenter, som har modtaget EU-midler gennem ENISA.
3. OLAF kan foretage undersøgelser, herunder kontrol og inspektion på stedet, i overensstemmelse med de bestemmelser og procedurer, der er fastsat i forordning (EU, Euratom) nr. 883/2013 og Rådets forordning (Euratom, EF) nr. 2185/96⁽³¹⁾ for at fastslå, om der har været svig, korruption eller andre ulovlige aktiviteter til skade for Unionens finansielle interesser i forbindelse med tilskud eller en kontrakt, der finansieres af ENISA.
4. Uden at det berører stk. 1, 2 og 3, skal ENISA's samarbejdsaftaler med tredjelande eller internationale organisationer, kontrakter, tilskudsftaler og afgørelser om ydelse af tilskud indeholde bestemmelser, der udtrykkeligt giver Revisionsretten og OLAF beføjelse til at foretage denne kontrol og disse undersøgelser i overensstemmelse med deres respektive beføjelser.

*KAPITEL V**Personale**Artikel 34***Generelle bestemmelser**

Tjenestemandsvedtægten og ansættelsesvilkårene for øvrige ansatte samt de regler, som EU-institutionerne i fællesskab har vedtaget for anvendelsen af tjenestemandsvedtægten og ansættelsesvilkårene for øvrige ansatte, gælder for ENISA's personale.

*Artikel 35***Privilegier og immuniteter**

Protokol nr. 7 vedrørende Den Europæiske Unions privilegier og immuniteter, der er knyttet som bilag til TEU og til TEUF, finder anvendelse på ENISA og dets personale.

*Artikel 36***Den administrerende direktør**

1. Den administrerende direktør ansættes i en stilling som midlertidigt ansat ved ENISA i henhold til artikel 2, litra a), i ansættelsesvilkårene for øvrige ansatte.

2. Den administrerende direktør udnævnes af bestyrelsen på grundlag af en liste over kandidater, som Kommissionen foreslår, efter en åben og gennemsigtig udvælgelsesprocedure.
3. Med henblik på indgåelsen af ansættelseskontrakten med den administrerende direktør repræsenteres ENISA af formanden for bestyrelsen.
4. Før udnævnelsen indbydes den ansøger, bestyrelsen har valgt, til at afgive en redegørelse for Europa-Parlamentets relevante udvalg og besvare spørgsmål fra medlemmerne.
5. Den administrerende direktørs mandatperiode er fem år. Ved udløbet af denne periode foretager Kommissionen en vurdering af den administrerende direktørs resultater og ENISA's fremtidige opgaver og udfordringer i betragtning.
6. Afgørelser om udnævnelse og afskedigelse af den administrerende direktør og om forlængelse af dennes mandatperiode træffes af bestyrelsen i overensstemmelse med artikel 18, stk. 2.
7. Bestyrelsen kan på grundlag af et forslag fra Kommissionen, der tager hensyn til den i stk. 5 omhandlede vurdering, forlænge den administrerende direktørs mandatperiode én gang for en periode på fem år.
8. Bestyrelsen underretter Europa-Parlamentet, hvis den har til hensigt at forlænge den administrerende direktørs mandatperiode. Inden for tre måneder inden forlængelsen af mandatperioden afgiver den administrerende direktør, såfremt denne indbydes hertil, en redegørelse for Europa-Parlamentets relevante udvalg og besvarer medlemmernes spørgsmål.
9. En administrerende direktør, hvis mandatperiode er blevet forlænget, kan ikke deltage i endnu en udvælgelsesprocedure til den samme stilling.
10. Den administrerende direktør kan kun afskediges ved en afgørelse truffet af bestyrelsen efter forslag fra Kommissionen.

Artikel 37

Udstationerede nationale eksperter og andet personale

1. ENISA kan gøre brug af udstationerede nationale eksperter og andet personale, der ikke er ansat af ENISA. Tjenestemandsvedtægten og ansættelsesvilkårene for øvrige ansatte gælder ikke for sådanne ansatte.
2. Bestyrelsen vedtager en afgørelse, der fastlægger regler for udstationering af nationale eksperter til ENISA.

KAPITEL VI

Generelle bestemmelser vedrørende ENISA

Artikel 38

ENISA's retlige status

1. ENISA er et EU-organ og har status som juridisk person.
2. ENISA har i hver medlemsstat den videstgående rets- og handleevne, som vedkommende stats lovgivning tillægger juridiske personer. Det kan navnlig erhverve og afhænde fast ejendom og løse og optræde som part i retssager.

3. ENISA repræsenteres af den administrerende direktør.

Artikel 39

ENISA's ansvar

1. ENISA's ansvar i kontraktforhold reguleres af den lovgivning, der finder anvendelse på den pågældende kontrakt.
2. Den Europæiske Unions Domstol har kompetence til at træffe afgørelse i henhold til en voldgiftsbestemmelse i en kontrakt, som ENISA har indgået.
3. For så vidt angår ansvar uden for kontraktforhold skal ENISA erstatte skader, der er forvoldt af ENISA eller af dets ansatte under udøvelsen af deres hverv, i overensstemmelse med de almindelige retsgrundsætninger, der er fælles for medlemsstaternes retssystemer.
4. Den Europæiske Unions Domstol har kompetence til at træffe afgørelse i tvister vedrørende skadeserstatninger som omhandlet i stk. 3.
5. Det personlige ansvar for ENISA's ansatte over for ENISA reguleres i de ansættelsesvilkår, der gælder for ENISA's personale.

Artikel 40

Sprogordning

1. Rådets forordning nr. 1 finder anvendelse på ENISA⁽³²⁾. Medlemsstaterne og andre organer, der er udpeget af medlemsstaterne, kan henvende sig til ENISA og modtage svar på det af EU-institutionernes officielle sprog, de ønsker.
2. De oversættelsesopgaver, der er påkrævet i forbindelse med ENISA's virksomhed, udføres af Oversættelsescentret for Den Europæiske Unions Organer.

Artikel 41

Beskyttelse af personoplysninger

1. ENISA's behandling af personoplysninger er omfattet af forordning (EU) 2018/1725.
2. Bestyrelsen vedtager gennemførelsesbestemmelser som omhandlet i artikel 45, stk. 3, i forordning (EU) 2018/1725. Bestyrelsen kan vedtage yderligere foranstaltninger, der er nødvendige med henblik på ENISA's anvendelse af forordning (EU) 2018/1725.

Artikel 42

Samarbejde med tredjelande og internationale organisationer

1. I det omfang det er nødvendigt for at nå de i denne forordning fastsatte mål, kan ENISA samarbejde med kompetente myndigheder i tredjelande og/eller med internationale organisationer. I det øjemed kan ENISA etablere samarbejdsordninger med myndigheder i tredjelande og internationale organisationer på betingelse af Kommissionens forudgående godkendelse. Disse samarbejdsordninger må ikke skabe retlige forpligtelser for Unionen og dens medlemsstater.

2. Tredjelande, som har indgået aftaler med Unionen herom, kan deltage i ENISA's arbejde. Der fastlægges i henhold til de relevante bestemmelser i disse aftaler samarbejdsordninger, hvori navnlig arten og omfanget af disse landes deltagelse i ENISA's arbejde fastsættes, samt på hvilken måde deltagelsen i ENISA's arbejde skal ske, og der fastsættes bestemmelser om deltagelse i initiativer iværksat af ENISA, om økonomiske bidrag og om personale. Hvad angår personaleanliggende, skal disse samarbejdsordninger under alle omstændigheder overholde tjenstemandsvedtægten og ansættelsesvilkårene for øvrige ansatte.

3. Bestyrelsen vedtager en strategi for forbindelser med tredjelande og internationale organisationer for så vidt angår spørgsmål, der hører under ENISA's kompetenceområde. Kommissionen sikrer, at ENISA arbejder inden for sit mandat og den eksisterende institutionelle ramme, ved at indgå en passende samarbejdsordning med den administrerende direktør.

Artikel 43

Sikkerhedsregler for beskyttelse af følsomme ikkeklassificerede oplysninger og klassificerede oplysninger

Efter høring af Kommissionen vedtager ENISA sikkerhedsregler, der bygger på sikkerhedsprincipperne i Kommissionens sikkerhedsforskrifter til beskyttelse af følsomme ikkeklassificerede oplysninger og EUCI som fastsat i Kommissionens afgørelse (EU, Euratom) 2015/443 og (EU, Euratom) 2015/444. ENISA's sikkerhedsforskrifter skal omfatte bestemmelser om udveksling, behandling og lagring af sådanne oplysninger.

Artikel 44

Hjemstedsaftale og driftsvilkår

1. De nødvendige bestemmelser vedrørende de lokaler, der skal stilles til rådighed for ENISA i værtsmedlemsstaten, og de faciliteter, der skal stilles til rådighed af værtsmedlemsstaten, samt de særlige regler i værtsmedlemsstaten, der finder anvendelse på ENISA's administrerende direktør, bestyrelsesmedlemmerne, ENISA's personale og deres familiemedlemmer, fastsættes i en hjemstedsaftale mellem ENISA og værtsmedlemsstaten, der indgås, efter at bestyrelsen har godkendt den.

2. ENISA's værtsmedlemsstat sikrer de bedst mulige betingelser for, at ENISA kan fungere efter hensigten, idet der tages hensyn til stedets tilgængelighed, tilbud om tilstrækkelige uddannelsesfaciliteter for personalets børn, tilstrækkelig adgang til arbejdsmarkedet, social sikring og lægebehandling for personalets børn og ægtefæller.

Artikel 45

Administrativ kontrol

ENISA's virke er underlagt Den Europæiske Ombudsmands tilsyn i overensstemmelse med artikel 228 i TEUF.

AFSNIT III

RAMMEBESTEMMELSER FOR CYBERSIKKERHEDSCERTIFICERING*Artikel 46***Europæisk ramme for cybersikkerhedscertificering**

1. Den europæiske ramme for cybersikkerhedscertificering etableres for at forbedre betingelserne for det indre markeds funktion ved at øge cybersikkerhedsniveauet i Unionen og muliggøre en harmoniseret tilgang på EU-plan til europæiske cybersikkerhedscertificeringsordninger for at skabe et digitalt indre marked for IKT-produkter, -tjenester og -processer.
2. Den europæiske ramme for cybersikkerhedscertificering definerer en mekanisme til fastlæggelse af europæiske cybersikkerhedscertificeringsordninger og til attestering af, at IKT-produkter, -tjenester og -processer, der er evalueret i overensstemmelse med sådanne ordninger, opfylder de fastlagte sikkerhedskrav med henblik på at beskytte tilgængeligheden, autenticiteten, integriteten eller fortroligheden af data, der lagres, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, tjenester og processer, i hele deres livscyklus.

*Artikel 47***Unionens rullende arbejdsprogram for europæisk cybersikkerhedscertificering**

1. Kommissionen offentliggør et rullende arbejdsprogram for europæisk cybersikkerhedscertificering (»Unionens rullende arbejdsprogram«), som opstiller strategiske prioriteter for fremtidige europæiske cybersikkerhedscertificeringsordninger.
2. Unionens rullende arbejdsprogram skal navnlig omfatte en liste over IKT-produkter, -tjenester og -processer eller kategorier heraf, der vil kunne drage fordel af at være omfattet af en europæisk cybersikkerhedscertificeringsordning.
3. Tilføjelse af bestemte IKT-produkter, -tjenester og -processer eller -kategorier heraf i Unionens rullende arbejdsprogram skal være begrundet på baggrund af et eller flere af følgende forhold:
 - a) tilgængeligheden og udviklingen af nationale cybersikkerhedscertificeringsordninger, der omfatter en bestemt kategori af IKT-produkter, -tjenester eller -processer, og navnlig for så vidt angår risikoen for fragmentering
 - b) relevant EU- eller national ret eller politik
 - c) efterspørgslen på markedet
 - d) udviklingen i cybertrusselsbilledet
 - e) anmodning om udarbejdelse af et specifikt forslag til ordning fra ECCG.
4. Kommissionen tager behørigt hensyn til udtalelserne om udkastet til Unionens rullende arbejdsprogram fra ECCG og Cybersikkerhedscertificeringsgruppen for Interessenter.
5. Det første af Unionens rullende arbejdsprogrammer offentliggøres senest den 28. juni 2020. Unionens rullende arbejdsprogram ajourføres mindst en gang hvert tredje år eller oftere, om nødvendigt.

*Artikel 48***Anmodning om en europæisk cybersikkerhedscertificeringsordning**

1. Kommissionen kan anmode ENISA om at udarbejde et forslag til ordning eller om revision af en eksisterende cybersikkerhedscertificeringsordning på grundlag af Unionens rullende arbejdsprogram.
2. I behørigt begrundede tilfælde kan Kommissionen eller ECCG anmode ENISA om at udarbejde et forslag til ordning eller om revision af en eksisterende ordning, som ikke er omfattet af Unionens rullende arbejdsprogram. Unionens rullende arbejdsprogram ajourføres i overensstemmelse hermed.

*Artikel 49***Udarbejdelse, vedtagelse og revision af en europæisk cybersikkerhedscertificeringsordning**

1. Efter anmodning fra Kommissionen i henhold til artikel 48 udarbejder ENISA et forslag til ordning, som opfylder kravene i artikel 51, 52 og 54.
2. Efter anmodning fra ECCG i henhold til artikel 48, stk. 2, kan ENISA udarbejde et forslag til ordning, som opfylder kravene i artikel 51, 52 og 54. Afviser ENISA en sådan anmodning, begrundes det afvisningen. Enhver afgørelse om afvisning af en sådan anmodning træffes af bestyrelsen.
3. Under udarbejdelsen af forslaget til ordning hører ENISA alle relevante interessenter ved hjælp af en formel, åben, gennemsigtig og inklusiv høringsproces.
4. For hvert forslag til ordning nedsætter ENISA en ad hoc-arbejdsgruppe i overensstemmelse med artikel 20, stk. 4, med henblik på at stille specifik rådgivning og ekspertise til rådighed for ENISA.
5. ENISA arbejder tæt sammen med ECCG. ECCG yder ENISA bistand og ekspertrådgivning i forbindelse med udarbejdelsen af forslaget til ordning og vedtager en udtalelse om forslaget til ordning.
6. ENISA tager størst muligt hensyn til ECCG's udtalelse, før det fremsender forslaget til ordning udarbejdet i overensstemmelse med stk. 3, 4 og 5 til Kommissionen. ECCG's udtalelse er ikke bindende for ENISA, og en manglende udtalelse forhindrer heller ikke ENISA i at fremsende forslaget til ordning til Kommissionen.
7. Kommissionen kan på grundlag af det af ENISA udarbejdede forslag til ordning vedtage gennemførelsesretsakter vedrørende europæiske cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester og -processer, der opfylder kravene i artikel 51, 52 og 54. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 66, stk. 2,
8. ENISA evaluerer mindst hvert femte år hver vedtagen europæisk cybersikkerhedscertificeringsordning under hensyntagen til tilbagemeldinger fra interesserede parter. Om nødvendigt kan Kommissionen eller ECCG anmode ENISA om at påbegynde processen med at udvikle et revideret forslag til ordning i overensstemmelse med artikel 48 og nærværende artikel.

*Artikel 50***Websted om europæiske cybersikkerhedscertificeringsordninger**

1. ENISA vedligeholder et dedikeret websted, der oplyser om og reklamerer for de europæiske cybersikkerhedscertificeringsordninger, europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer, herunder oplysninger med hensyn til europæiske cybersikkerhedscertificeringsordninger, som ikke

længere er gyldige, og med hensyn til europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer, der er trukket tilbage eller udløbet, og med hensyn til registeret over links til cybersikkerhedsoplysninger, der er stillet til rådighed i overensstemmelse med artikel 55.

2. I givet fald skal webstedet omhandlet i stk. 1 også angive de nationale cybersikkerhedscertificeringsordninger, som er blevet erstattet af en europæisk cybersikkerhedscertificeringsordning.

Artikel 51

Sikkerhedsmål for europæiske cybersikkerhedscertificeringsordninger

En europæisk cybersikkerhedscertificeringsordning skal være udformet til, alt efter relevans, som minimum at opfylde følgende sikkerhedsmål:

- a) beskyttelse af data, som lagres, overføres eller på anden måde behandles, mod utilsigtet eller uautoriseret lagring, behandling, adgang eller offentliggørelse i hele IKT-produktets, -tjenestens eller -processens livscyklus
- b) beskyttelse af data, som lagres, overføres eller på anden måde behandles, mod utilsigtet eller uautoriseret ødelæggelse, tab eller ændring eller manglende tilgængelighed i hele IKT-produktets, -tjenestens eller -processens livscyklus
- c) autoriserede personer, programmer eller maskiner kan udelukkende tilgå de data, tjenester eller funktioner, som de har adgangsret til
- d) identifikation af og dokumentation for kendt afhængighed og kendte sårbarheder
- e) registrering af, hvilke data, funktioner eller tjenester der er tilgået, anvendt eller på anden måde behandlet, på hvilket tidspunkt og af hvem
- f) det er muligt at kontrollere, hvilke data, tjenester og funktioner der er tilgået, anvendt eller på anden måde behandlet, på hvilket tidspunkt og af hvem
- g) verifikation af, at IKT-produkter, -tjenester og -processer ikke indeholder kendte sårbarheder
- h) hurtig genetablering af tilgængelighed af og adgang til data, tjenester og funktioner i tilfælde af en fysisk eller teknisk hændelse
- i) at IKT-processer, -tjenester og -processer er sikre som følge af standardindstillinger og indbygget sikkerhed
- j) IKT-produkter, -tjenester og -processer er forsynet med ajourført software og hardware, der ikke indeholder offentligt kendte sårbarheder, og som har mekanismer til sikker opdatering.

Artikel 52

Tillidsniveauer for europæiske cybersikkerhedscertificeringsordninger

1. En europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende tillidsniveauer for IKT- produkter, -tjenester og -processer: »grundlæggende«, »betydeligt« eller »højt«. Tillidsniveauet skal afspejle det risikoniveau, der er forbundet med den tilsigtede anvendelse af IKT-produktet, -tjenesten eller -processen, hvad angår sandsynligheden for og virkningen af en hændelse.

2. Europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer skal henvise til et tillidsniveau, der er angivet i den europæiske cybersikkerhedscertificeringsordning, i henhold til hvilken den europæiske cybersikkerhedsattest eller EU-overensstemmelseserklæringen er udstedt.
3. De sikkerhedskrav, som svarer til tillidsniveauet, skal fremgå af den relevante europæiske cybersikkerhedscertificeringsordning, herunder de tilsvarende sikkerhedsfunktioner og den tilsvarende grad af stringens og dybde i den evaluering, som IKT-produktet, -tjenesten eller processen skal undergå.
4. Attesten eller EU-overensstemmelseserklæringen skal henvise til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for eller forhindre cybersikkerhedshændelser.
5. En europæisk cybersikkerhedsattest eller EU-overensstemmelseserklæring, der henviser til tillidsniveauet »grundlæggende«, skal give sikkerhed for, at de IKT-produkter, -tjenester og -processer, som attesten eller EU-overensstemmelseserklæringen er udstedt for, opfylder de tilsvarende sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret på et niveau, der har til formål at minimere de kendte grundlæggende risici for hændelser og cyberangreb. Evalueringsaktiviteterne skal som minimum omfatte en gennemgang af den tekniske dokumentation. Hvis en sådangennemgang ikke er hensigtsmæssig, anvendes andre evalueringsaktiviteter med tilsvarende virkning.
6. En europæisk cybersikkerhedsattest, der henviser til tillidsniveauet »betydeligt«, skal give sikkerhed for, at de IKT-produkter, -tjenester og -processer, som attesten er udstedt for, opfylder de tilsvarende sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret på et niveau, der har til formål at minimere kendte cybersikkerhedsrisici og risikoen for hændelser og cyberangreb udført af aktører med begrænsede færdigheder og ressourcer. Evalueringsaktiviteterne skal som minimum omfatte følgende: en gennemgang med henblik på at påvise, at der ikke er offentligt kendte sårbarheder, og afprøvning med henblik på at påvise, at IKT-produkterne, tjenesterne eller -processerne udfører de nødvendige sikkerhedsfunktioner korrekt. Hvis sådanne evalueringsaktiviteter ikke er hensigtsmæssige, anvendes andre evalueringsaktiviteter med tilsvarende virkning.
7. En europæisk cybersikkerhedsattest, der henviser til tillidsniveauet »højt«, skal give sikkerhed for, at de IKT-produkter, -tjenester og -processer, som attesten er udstedt for, opfylder de tilsvarende sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret på et niveau, der har til formål at minimere risikoen for avancerede cyberangreb udført af aktører med betydelige færdigheder og ressourcer. Evalueringsaktiviteterne skal som minimum omfatte følgende: en gennemgang med henblik på at påvise, at der ikke er offentligt kendte sårbarheder, afprøvning med henblik på at påvise, at IKT-produkterne, -tjenesterne eller -processerne udfører de nødvendige sikkerhedsfunktioner korrekt med den mest avancerede teknologi, samt en vurdering af deres modstandsdygtighed over for drevne angribere ved hjælp af penetrationstest. Hvis sådanne evalueringsaktiviteter ikke er hensigtsmæssige, anvendes andre aktiviteter med tilsvarende virkning.
8. En europæisk cybersikkerhedscertificeringsordning kan fastsætte flere evalueringsniveauer, alt efter hvor stringent og omfattende den anvendte evalueringsmetodologi er. Hvert enkelt evalueringsniveau skal svare til et af tillidsniveauerne og være defineret ved en passende kombination af tillidskomponenter.

Artikel 53

Selvurdering af overensstemmelse

1. En europæisk cybersikkerhedscertificeringsordning kan tillade, at der foretages selvurdering af overensstemmelse, som producenter eller udbydere af IKT-produkter, -tjenester og -processer har det fulde

ansvar for. Selvvurdering af overensstemmelse er kun tilladt i forhold til IKT-produkter, -tjenester og -processer med lav risiko svarende til tillidsniveauet »grundlæggende«.

2. Producenter og udbydere af IKT-produkter, -tjenester eller -processer kan udstede en EU-overensstemmelseserklæring, hvoraf det fremgår, at det er blevet påvist, at de krav, som er fastsat i ordningen, er opfyldt. Ved at udstede en sådan erklæring står producenter og udbydere af IKT-produkter, -tjenester og -processer inde for, at IKT-produktet, -tjenesten eller -processen stemmer overens med den pågældende ordnings krav.

3. Producenter og udbydere af IKT-produkter, -tjenester eller -processer stiller EU-overensstemmelseserklæringen, den tekniske dokumentation og alle øvrige relevante oplysninger vedrørende IKT-produkternes eller -tjenesternes overensstemmelse med ordningen til rådighed for den nationale cybersikkerhedscertificeringsmyndighed som omhandlet i artikel 58, stk. 1, i den periode, der er fastsat i den tilsvarende europæiske cybersikkerhedscertificeringsordning. En kopi af EU-overensstemmelseserklæringen indgives til den nationale cybersikkerhedscertificeringsmyndighed og til ENISA.

4. Udstedelse af en EU-overensstemmelseserklæring er frivillig, medmindre andet er fastsat i EU-retten eller i medlemsstaternes ret.

5. EU-overensstemmelseserklæringer skal anerkendes i alle medlemsstater.

Artikel 54

Elementer i europæiske cybersikkerhedscertificeringsordninger

1. En europæisk cybersikkerhedscertificeringsordning skal som minimum omfatte følgende elementer:

a) certificeringsordningens genstand og omfang, herunder typer eller kategorier af IKT-produkter, -tjenester og -processer, der er omfattet

b) en klar beskrivelse af formålet med ordningen, og af hvordan de valgte standarder, evalueringsmetoder og tillidsniveauer svarer til behovene hos de tilsigtede brugere af ordningen

c) henvisninger til de internationale, europæiske eller nationale standarder, der anvendes ved evalueringen, eller, hvis der ikke foreligger sådanne standarder, eller de ikke er hensigtsmæssige, henvisninger til tekniske specifikationer, som opfylder kravene i bilag II til forordning (EU) nr. 1025/2012, eller, hvis sådanne specifikationer ikke foreligger, til tekniske specifikationer eller andre cybersikkerhedskrav, der er defineret i den europæiske cybersikkerhedscertificeringsordning

d) et eller flere tillidsniveauer, hvor det er relevant

e) en angivelse af, om selvvurdering af overensstemmelse er tilladt i henhold til ordningen

f) hvor det er relevant, specifikke eller yderligere krav, der gælder for overensstemmelsesvurderingsorganerne for at sikre deres tekniske kompetence til at evaluere cybersikkerhedskravene

g) de specifikke evalueringskriterier og -metoder, der skal anvendes, herunder typen af evaluering, for at påvise, at de sikkerhedsmål omhandlet i artikel 51 er nået

h) hvor det er relevant, de til certificering nødvendige oplysninger, som en ansøger skal videreføre eller på anden måde stille til rådighed for overensstemmelsesvurderingsorganerne

i) hvis ordningen fastsætter mærker eller etiketter, omstændighederne under hvilke sådanne mærker eller etiketter kan anvendes

- j) regler for overvågning af IKT-produkters, -tjenesters- og -processers overensstemmelse med de europæiske cybersikkerhedsattesters eller EU-overensstemmelseserklæringernes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav
 - k) hvor det er relevant, betingelserne for udstedelse, opretholdelse, forlængelse og fornyelse af den europæiske cybersikkerhedsattest samt betingelserne for udvidelse eller indskrænkning af certificeringens omfang
 - l) regler om følgerne for IKT-produkter, -tjenester og -processer, som er blevet certificeret, eller for hvilke en EU-overensstemmelseserklæring er udstedt, men som ikke overholder kravene i ordningen
 - m) regler om, hvordan hidtil uopdagede cybersikkerhedssårbarheder i IKT-produkter, -tjenester og -processer skal indberettes og håndteres
 - n) hvor det er relevant, regler om overensstemmelsesvurderingsorganers opbevaring af optegnelser
 - o) angivelse af nationale eller internationale cybersikkerhedscertificeringsordninger, som dækker samme type eller kategorier af IKT-processer, -produkter og -tjenester, sikkerhedskrav, evalueringskriterier og -metoder samt tillidsniveauer
 - p) indholdet af og formatet for de europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringerne, der skal udstedes
 - q) tilgængelighedsperioden af den EU-overensstemmelseserklæring, den tekniske dokumentation og alle de øvrige relevante oplysninger, der skal stilles til rådighed af producenter eller udbydere af IKT-produkter, -tjenester og -processer
 - r) den maksimale gyldighedsperiode for europæiske cybersikkerhedsattester udstedt i henhold til ordningen
 - s) politikken for offentliggørelse af europæiske cybersikkerhedsattester, der er udstedt, ændret eller tilbagetrukket i henhold til ordningen
 - t) betingelserne for gensidig anerkendelse af certificeringsordninger med tredjelande
 - u) hvor det er relevant, reglerne for en eventuel peervurderingsmekanisme, der ved ordningen er oprettet for de myndigheder eller organer, der udsteder europæiske cybersikkerhedsattester for tillidsniveauet »højt« i henhold til artikel 56, stk. 6. En sådan mekanisme berører ikke det peerreview, der er fastsat i artikel 59
 - v) format og procedurer, der skal følges af producenter eller udbydere af IKT-produkter, -tjenester eller -processer, når de giver og ajourfører de supplerende cybersikkerhedsoplysninger i overensstemmelse med artikel 55.
2. De krav, der er anført i den europæiske cybersikkerhedscertificeringsordning, skal være i overensstemmelse med eventuelle relevante retlige krav, navnlig krav som følge af harmoniseret EU-ret.
3. Hvis det er fastsat i en bestemt EU-retsakt, kan en attest eller en EU-overensstemmelseserklæring udstedt i henhold til en europæisk cybersikkerhedscertificeringsordning anvendes til at påvise en formodning om overensstemmelse med kravene i den pågældende retsakt.
4. I mangel af harmoniseret EU-ret kan medlemsstaternes ret også fastsætte, at en europæisk cybersikkerhedscertificeringsordning kan anvendes til at skabe en formodning om overensstemmelse med retlige krav.

*Artikel 55***Supplerende cybersikkerhedsoplysninger for certificerede IKT-produkter, -tjenester og -processer**

1. Producenter og udbydere af certificerede IKT-produkter, -tjenester eller -processer eller af IKT-produkter, -tjenester eller -processer, for hvilke en EU-overensstemmelseserklæring er udstedt, gør følgende supplerende cybersikkerhedsoplysninger offentligt tilgængelige:

- a) vejledning og anbefalinger for at bistå slutbrugere med sikker konfiguration, installation, ibrugtagning, drift og vedligeholdelse af IKT-produkterne eller -tjenesterne
- b) den periode, hvor slutbrugere tilbydes sikkerhedsstøtte, navnlig for så vidt angår tilgængelighed af cybersikkerhedsrelaterede opdateringer
- c) producentens eller udbyderens kontaktoplysninger og accepterede metoder til modtagelse af sårbarhedsoplysninger fra slutbrugere og sikkerhedsforskere
- d) en henvisning til onlineregistre over offentliggjorte sårbarheder vedrørende det pågældende IKT-produkt eller den pågældende IKT-tjeneste eller -proces og til eventuel relevant cybersikkerhedsrådgivning.

2. De oplysninger, der er omhandlet i stk. 1, skal være tilgængelige i elektronisk form og forblive tilgængelige og opdateres om nødvendigt mindst indtil udløbet af den tilsvarende europæiske cybersikkerhedsattest eller EU-overensstemmelseserklæring.

*Artikel 56***Cybersikkerhedscertificering**

1. IKT-produkter, -tjenester og -processer, der er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 49, formodes at overholde kravene i en sådan ordning.

2. Cybersikkerhedscertificeringen skal være frivillig, medmindre andet er fastsat i EU-retten eller i medlemsstaternes ret.

3. Kommissionen vurderer regelmæssigt effektiviteten og anvendelsen af de vedtagne europæiske cybersikkerhedscertificeringsordninger, og hvorvidt en bestemt europæisk cybersikkerhedscertificeringsordning skal gøres obligatoriske ved hjælp af relevant EU-ret for at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter, -tjenester og -processer i Unionen og forbedre det indre markeds funktion. Den første sådanne vurdering skal foretages senest den 31. december 2023 og efterfølgende vurderinger mindst hvert andet år derefter. Kommissionen identificerer på grundlag af resultatet af disse vurderinger de IKT-produkter, -tjenester og -processer, der er omfattet af en eksisterende certificeringsordning, og som skal omfattes af en obligatorisk certificeringsordning. Som en prioritet fokuserer Kommissionen på de sektorer i bilag II til direktiv (EU) 2016/1148, som skal vurderes senest to år efter vedtagelsen af den første europæiske cybersikkerhedscertificeringsordning.

Ved udarbejdelsen af vurderingen skal Kommissionen:

- a) tage hensyn til foranstaltningernes indvirkning på producenter og udbydere af sådanne IKT-produkter, -tjenester og -processer og på brugerne i form af omkostninger ved disse foranstaltninger samt de samfundsmæssige eller økonomiske fordele som følge af det forventede øgede sikkerhedsniveau for de pågældende IKT-produkter, -tjenester og -processer

- b) tage hensyn til eksistensen og gennemførelsen af relevant ret i medlemsstaterne eller tredjelande
- c) gennemføre en åben, gennemsigtig og inklusiv høringsproces med alle relevante interessenter og medlemsstater
- d) tage hensyn til eventuelle gennemførelsesfrister og overgangsforanstaltninger eller -perioder under hensyntagen til navnlig foranstaltningens mulige indvirkning på producenter eller udbydere af IKT-produkter, -tjenester og -processer, herunder SMV'er
- e) foreslå den hurtigste og mest effektive måde, hvorpå overgangen fra frivillige til obligatoriske certificeringsordninger skal gennemføres.

4. De overensstemmelsesvurderingsorganer, der er omhandlet i artikel 60, udsteder europæiske cybersikkerhedsattester i henhold til nærværende artikel på grundlag af de kriterier, der fremgår af den europæiske cybersikkerhedscertificeringsordning, som Kommissionen har vedtaget i medfør af artikel 49, idet de henviser til tillidsniveauet »grundlæggende« eller »betydeligt«.

5. Uanset stk. 4 kan det i behørigt begrundede tilfælde fastsættes i en specifik europæisk cybersikkerhedscertificeringsordning, at en europæisk cybersikkerhedsattest i medfør af denne ordning kun må udstedes af et offentligt organ. Et sådant organ skal være en af følgende:

- a) en national cybersikkerhedscertificeringsmyndighed som omhandlet i artikel 58, stk. 1, eller
- b) et offentligt organ, der er akkrediteret som overensstemmelsesvurderingsorgan i medfør af artikel 60, stk. 1.

6. I tilfælde, hvor en europæisk cybersikkerhedscertificeringsordning vedtaget i medfør af artikel 49 indeholder krav om tillidsniveau »højt«, kan den europæiske cybersikkerhedsattest i henhold til den pågældende ordning kun udstedes af en national cybersikkerhedscertificeringsmyndighed eller i følgende tilfælde af et overensstemmelsesvurderingsorgan:

- a) efter at 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.

7. Den fysiske eller juridiske person, der indgiver IKT-produkter, -tjenester eller -processer til certificering, stiller alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, til rådighed for den i artikel 58 omhandlede nationale cybersikkerhedscertificeringsmyndighed, hvis denne myndighed er det organ, der udsteder den europæiske cybersikkerhedsattest, eller for det i artikel 60 omhandlede overensstemmelsesvurderingsorgan.

8. Indehaveren af en europæisk cybersikkerhedsattest underretter den myndighed eller det organ, der er omhandlet i stk. 7, om eventuelle efterfølgende opdagede sårbarheder eller uregelmæssigheder i forbindelse med det certificerede IKT-produkt, den certificerede IKT-proces eller den certificerede IKT-tjenestes sikkerhed, som kan have en indvirkning på overholdelsen af de med certificeringen forbundne krav. Vedkommende organ eller myndighed sender hurtigst muligt disse oplysninger til den pågældende nationale cybersikkerhedscertificeringsmyndighed.

9. En europæisk cybersikkerhedsattest udstedes for den periode, som er fastsat i den pågældende europæiske cybersikkerhedscertificeringsordning, og kan fornyes, såfremt de relevante krav fortsat er opfyldt.

10. En europæisk cybersikkerhedsattest udstedt i henhold til denne artikel skal anerkendes i alle medlemsstater.

Artikel 57

Nationale cybersikkerhedscertificeringsordninger og -attester

1. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter, -tjenester og -processer, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, ophører med at have virkning fra det tidspunkt, der fastsættes i den gennemførelsesretsakt, som vedtages i medfør af artikel 49, stk. 7, uden at dette dog berører nærværende artikels stk. 3. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter, -tjenester og -processer, der ikke er omfattet af en europæisk cybersikkerhedscertificeringsordning, består fortsat.
2. Medlemsstaterne må ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter, -tjenester og -processer, som allerede er omfattet af en gældende europæisk cybersikkerhedscertificeringsordning.
3. Eksisterende attester, som blev udstedt i henhold til nationale cybersikkerhedscertificeringsordninger og omfattes af en europæisk cybersikkerhedscertificeringsordning, forbliver gyldige indtil deres udløbsdato.
4. Med henblik på at undgå fragmentering af det indre marked meddeler medlemsstaterne initiativer vedrørende udarbejdelse af nye nationale cybersikkerhedscertificeringsordninger til Kommissionen og ECCG.

Artikel 58

Nationale cybersikkerhedscertificeringsmyndigheder

1. 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 udpegede medlemsstat.
2. 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.
3. Uden at det berører artikel 56, stk. 5, litra a), og artikel 56, stk. 6, skal hver national cybersikkerhedscertificeringsmyndighed med hensyn til dens organisation, finansieringsbeslutninger, retlige struktur og beslutningstagning være uafhængig af de enheder, som den fører tilsyn med.
4. Medlemsstaterne sikrer, 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 nærværende artikel, og at disse aktiviteter udføres uafhængigt af hinanden.
5. Medlemsstaterne sikrer, at de nationale cybersikkerhedscertificeringsmyndigheder har tilstrækkelige ressourcer til at udøve deres beføjelser og udføre deres opgaver på en virkningsfuld og effektiv måde.

6. Med henblik på en effektiv gennemførelse af denne forordning er det hensigtsmæssigt, at nationale cybersikkerhedscertificeringsmyndigheder deltager i ECCG på en aktiv, effektiv, virkningsfuld og sikker måde.

7. Nationale cybersikkerhedscertificeringsmyndigheder skal:

a) føre tilsyn med og håndhæve regler, der indgår i de europæiske cybersikkerhedscertificeringsordninger i henhold til artikel 54, stk. 1, litra j), til overvågning af, at IKT-produkter, -tjenester og -processer opfylder kravene i de europæiske cybersikkerhedsattester, der er udstedt på deres respektive område, i samarbejde med andre relevante markedsovervågningsmyndigheder

b) overvåge og håndhæve de forpligtelser, som påhviler producenter eller udbydere af IKT-produkter, -tjenester og -processer, der er etableret på deres respektive område, og som foretager selv vurdering af overensstemmelse, navnlig forpligtelserne fastsat i artikel 53, stk. 2 og 3, og i den tilsvarende europæiske cybersikkerhedscertificeringsordning

c) aktivt bistå og støtte de nationale akkrediteringsorganer med overvågning af og tilsyn med overensstemmelsesvurderingsorganers aktiviteter med henblik på denne forordning, uden at det berører artikel 60, stk. 3

d) overvåge og føre tilsyn med de aktiviteter, der udføres af de i artikel 56, stk. 5, omhandlede offentlige organer

e) hvis det er relevant, bemyndige overensstemmelsesvurderingsorganer i henhold til artikel 60, stk. 3, og begrænse, suspendere eller inddrage eksisterende bemyndigelse i tilfælde af, at overensstemmelsesvurderingsorganer overtræder kravene i denne forordning

f) 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 samt undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist

g) forelægge en årlig sammenfattende rapport om de aktiviteter, der er udført i henhold til litra b), c) og d) eller stk. 8, for ENISA og ECCG

h) samarbejde med andre nationale cybersikkerhedscertificeringsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-processers, -produkters og -tjenesters manglende overholdelse af denne forordnings eller specifikke europæiske cybersikkerhedscertificeringsordningers krav, og

i) overvåge den relevante udvikling inden for cybersikkerhedscertificering.

8. Hver national cybersikkerhedscertificeringsmyndighed skal mindst have følgende beføjelser:

a) at 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

b) at 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 dette afsnit

c) i overensstemmelse med national ret at 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

d) at 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

e) i overensstemmelse med national ret at kunne tilbagekalde europæiske cybersikkerhedsattester, der er udstedt af de nationale cybersikkerhedscertificeringsmyndigheder 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

f) at kunne 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 denne forordning.

9. De nationale cybersikkerhedscertificeringsmyndigheder skal samarbejde med hinanden og Kommissionen ved navnlig at udveksle oplysninger, erfaringer og god praksis med hensyn til cybersikkerhedscertificering og tekniske spørgsmål vedrørende IKT-produkters, -tjenesters og -processers cybersikkerhed.

Artikel 59

Peerreview

1. For at opnå ensartede standarder i hele Unionen for så vidt angår europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer underkastes nationale cybersikkerhedscertificeringsmyndigheder peerreview.

2. Peerreviews skal foregå på grundlag af fornuftige og gennemsigtige evalueringskriterier og -procedurer, navnlig med hensyn til strukturelle krav, krav til menneskelige ressourcer og proceskrav samt fortrolighed og klager.

3. Ved peerreviews vurderes:

a) hvis det er relevant, hvorvidt 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, og hvorvidt disse aktiviteter udføres uafhængigt af hinanden

b) procedurerne for tilsyn med og håndhævelse af reglerne for overvågning af, at IKT-produkter, -tjenester og -processer overholder europæiske cybersikkerhedsattester i henhold til artikel 58, stk. 7, litra a)

c) procedurerne for overvågning og håndhævelse af forpligtelserne for producenter eller udbydere af IKT-produkter, -tjenester eller -processer i henhold til artikel 58, stk. 7, litra b)

d) procedurerne for overvågning og bemyndigelse af og tilsyn med overensstemmelsesvurderingsorganernes aktiviteter

e) hvis det er relevant, hvorvidt personalet i myndigheder eller organer, der udsteder attester for tillidsniveauet »højt« i henhold til artikel 56, stk. 6, har den fornødne ekspertise.

4. Peerreviews foretages af mindst to nationale cybersikkerhedscertificeringsmyndigheder fra andre medlemsstater og af Kommissionen og mindst hvert femte år. ENISA kan deltage i peerreviews.
5. Kommissionen kan vedtage gennemførelsesretsakter, der fastlægger en plan for peerreviews, 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. I forbindelse med vedtagelsen af disse gennemførelsesretsakter tager Kommissionen behørigt hensyn til ECCG's betragtninger. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 66, stk. 2.
6. Resultaterne af peerreviews gennemgås af ECCG, som udarbejder sammenfatninger, der kan offentliggøres, og som om nødvendigt udsteder retningslinjer eller henstillinger om tiltag eller foranstaltninger, der skal træffes af de berørte enheder.

Artikel 60

Overensstemmelsesvurderingsorganer

1. Overensstemmelsesvurderingsorganerne akkrediteres af nationale akkrediteringsorganer, der er udpeget i henhold til forordning (EF) nr. 765/2008. Sådant akkreditering udstedes kun, hvis overensstemmelsesvurderingsorganet opfylder kravene i bilaget til nærværende forordning.
2. 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 nærværende artikels stk. 1.
3. Hvis europæiske cybersikkerhedscertificeringsordninger fastsætter specifikke eller yderligere krav i henhold til artikel 54, stk. 1, litra f), må kun overensstemmelsesvurderingsorganer, der opfylder disse krav, bemyndiges af den nationale cybersikkerhedscertificeringsmyndighed til at udføre opgaver i henhold til sådanne ordninger.
4. Akkreditering som omhandlet i stk. 1 udstedes til overensstemmelsesvurderingsorganerne for en periode på højst fem år og kan fornys på samme betingelser, såfremt overensstemmelsesvurderingsorganet stadig opfylder de i denne artikel fastsatte krav. Nationale akkrediteringsorganer træffer inden for en rimelig tidsfrist alle passende foranstaltninger med henblik på at begrænse, suspendere eller tilbagekalde akkrediteringen af et overensstemmelsesvurderingsorgan udstedt i henhold til stk. 1, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis overensstemmelsesvurderingsorganet overtræder denne forordning.

Artikel 61

Anmeldelse

1. For hver europæisk cybersikkerhedscertificeringsordning underretter de nationale cybersikkerhedscertificeringsmyndigheder Kommissionen om de overensstemmelsesvurderingsorganer, der er akkrediteret og, hvor det er relevant, bemyndiget i henhold til artikel 60, stk. 3, til at udstede europæiske cybersikkerhedsattester på specifikke tillidsniveauer, jf. artikel 52. De nationale cybersikkerhedscertificeringsmyndigheder underretter Kommissionen om eventuelle senere ændringer heraf hurtigst muligt.
2. Et år efter ikrafttrædelsen af en europæisk cybersikkerhedscertificeringsordning offentliggør Kommissionen en liste over de overensstemmelsesvurderingsorganer, som er anmeldt under den pågældende ordning, i Den Europæiske Unions Tidende.

3. Modtager Kommissionen en anmeldelse efter udløbet af den periode, der er omhandlet i stk. 2, offentliggør den ændringerne af listen over anmeldte overensstemmelsesvurderingsorganer i Den Europæiske Unions Tidende inden for to måneder fra datoen for modtagelsen af denne anmeldelse.

4. En national cybersikkerhedscertificeringsmyndighed kan anmode Kommissionen om at fjerne et overensstemmelsesvurderingsorgan, der er anmeldt af den pågældende myndighed, fra den i stk. 2 omhandlede liste over anmeldte overensstemmelsesvurderingsorganer. Kommissionen offentliggør de dertil svarende ændringer af listen i Den Europæiske Unions Tidende inden for en måned fra datoen for modtagelsen af den nationale cybersikkerhedscertificeringsmyndigheds anmodning.

5. Kommissionen kan vedtage gennemførelsesretsakter, der fastlægger vilkår, formater og procedurer for anmeldelserne omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren, jf. artikel 66, stk. 2.

Artikel 62

Den Europæiske Cybersikkerhedscertificeringsgruppe

1. Den Europæiske Cybersikkerhedscertificeringsgruppe (»ECCG«) oprettes.
2. ECCG sammensættes af repræsentanter for nationale cybersikkerhedscertificeringsmyndigheder eller repræsentanter for andre relevante nationale myndigheder. Et medlem af ECCG kan ikke repræsentere mere end to medlemsstater.
3. Interessenter og relevante tredjeparter kan indbydes til at deltage i ECCG's møder og til at deltage i dens arbejde.
4. Gruppen har følgende opgaver:
 - a) at rådgive og bistå Kommissionen i dens arbejde med at sikre en konsekvent gennemførelse og anvendelse af dette afsnit, herunder navnlig hvad angår Unionens rullende arbejdsprogram, cybersikkerhedscertificeringspolitik, koordinering af politiske tiltag og udarbejdelse af europæiske cybersikkerhedscertificeringsordninger
 - b) at bistå, rådgive og samarbejde med ENISA i forbindelse med udarbejdelse af forslag til ordninger i henhold til artikel 49
 - c) at vedtage en udtalelse om forslag til ordning udarbejdet af ENISA i henhold til artikel 49
 - d) at anmode ENISA om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning i henhold til artikel 48, stk. 2
 - e) at vedtage udtalelser til Kommissionen vedrørende vedligeholdelse og revision af eksisterende europæiske cybersikkerhedscertificeringsordninger
 - f) at undersøge relevante udviklinger inden for cybersikkerhedscertificering og udveksle oplysninger og god praksis om cybersikkerhedscertificeringsordninger
 - g) at fremme samarbejdet mellem nationale cybersikkerhedscertificeringsmyndigheder i henhold til dette afsnit gennem kapacitetsopbygning og udveksling af oplysninger, herunder navnlig ved at indføre metoder til effektiv udveksling af oplysninger vedrørende cybersikkerhedscertificeringsanliggender
 - h) at støtte gennemførelsen af peervurderingsmekanismer i overensstemmelse med de regler, som er fastsat i en europæisk cybersikkerhedscertificeringsordning i henhold til artikel 54, stk. 1, litra u)

i) at lette europæiske cybersikkerhedscertificeringsordningers tilpasning til internationalt anerkendte standarder, herunder ved at gennemgå eksisterende europæiske cybersikkerhedscertificeringsordninger og, hvis det er relevant, fremsætte henstillinger til ENISA om at indlede dialog med relevante internationale standardiseringsorganisationer for at afhjælpe utilstrækkeligheder eller mangler i de tilgængelige internationalt anerkendte standarder.

5. Med bistand fra ENISA varetager Kommissionen ECCG's formandskab, og Kommissionen varetager en sekretariatsfunktion for ECCG i overensstemmelse med artikel 8, stk. 1, litra e).

Artikel 63

Ret til at indgive klage

1. Fysiske og juridiske personer har ret til at indgive klage til udstederen af en europæisk cybersikkerhedsattest eller, når klagen vedrører en europæisk cybersikkerhedsattest udstedt af et overensstemmelsesvurderingsorgan i overensstemmelse med artikel 56, stk. 6, til den relevante nationale cybersikkerhedscertificeringsmyndighed.

2. Den myndighed eller det organ, som klage er indgivet til, underretter klageren om forløbet af sagen og om den trufne afgørelse samt om retten til effektive retsmidler, jf. artikel 64.

Artikel 64

Ret til effektive retsmidler

1. Uanset eventuelle administrative eller andre udenretslige midler har fysiske og juridiske personer ret til effektive retsmidler med hensyn til:

a) afgørelser truffet af den myndighed eller det organ, der er omhandlet i artikel 63, stk. 1, herunder, hvis det er relevant, vedrørende uretmæssig udstedelse, manglende udstedelse eller anerkendelse af en europæisk cybersikkerhedsattest, som de pågældende fysiske eller juridiske personer er indehaver af

b) en undladelse af at reagere på en klage, der er indgivet til den myndighed eller det organ, der er omhandlet i artikel 63, stk. 1.

2. En sag i medfør af denne artikel anlægges ved domstolene i den medlemsstat, hvor den myndighed eller det organ, mod hvem retsmidlet søges, er beliggende.

Artikel 65

Sanktioner

Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelse af bestemmelserne i dette afsnit og i tilfælde af overtrædelser af europæiske cybersikkerhedscertificeringsordninger, og træffer alle nødvendige foranstaltninger for at sikre, at de anvendes. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver straks Kommissionen meddelelse om disse regler og foranstaltninger og underretter den om alle senere ændringer, der berører dem.

AFSNIT IV

AFSLUTTENDE BESTEMMELSER*Artikel 66***Udvalgsprocedure**

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.
2. Når der henvises til dette stykke, finder artikel 5, stk. 4, litra b), i forordning (EU) nr. 182/2011 anvendelse.

*Artikel 67***Evaluering og revision**

1. Senest den 28. juni 2024 og hvert femte år derefter vurderer Kommissionen virkningen og effektiviteten af ENISA's arbejde og af dets arbejdsmetoder, et eventuelt behov for at ændre ENISA's mandat og de finansielle virkninger af en sådan eventuel ændring. Evalueringen skal tage hensyn til enhver tilbagemelding til ENISA som reaktion på dets aktiviteter. Hvis Kommissionen finder, at der ikke længere er grund til at videreføre driften af ENISA i lyset af de mål, det mandat og de opgaver, som ENISA er tillagt, kan Kommissionen foreslå, at denne forordning ændres med hensyn til de bestemmelser, der vedrører ENISA.
2. Evalueringen skal også vurdere virkningen og effektiviteten af bestemmelserne i afsnit III med hensyn til målene om at sikre et tilstrækkeligt niveau for IKT-produkters, -tjenesters og -processers cybersikkerhed i Unionen og forbedre det indre markeds funktion.
3. I evalueringen skal det også vurderes, om væsentlige cybersikkerhedskrav for adgang til det indre marked er nødvendige for at undgå, at IKT-produkter, -tjenester og -processer, der ikke opfylder grundlæggende cybersikkerhedskrav, kommer ind på EU-markedet.
4. Senest den 28. juni 2024 og hvert femte år derefter sender Kommissionen en rapport om evalueringen og dens konklusioner til Europa-Parlamentet, Rådet og bestyrelsen. Resultaterne i denne rapport offentliggøres.

*Artikel 68***Ophævelse og succession**

1. Forordning (EU) nr. 526/2013 ophæves med virkning fra den 27. juni 2019.
2. Henvisninger til forordning (EU) nr. 526/2013 og til ENISA som oprettet ved nævnte forordning fortolkes som henvisninger til nærværende forordning og til ENISA som oprettet ved nærværende forordning.
3. ENISA som oprettet ved denne forordning succederer ENISA som oprettet ved forordning (EU) nr. 526/2013 med hensyn til ethvert ejendomsforhold, enhver aftale, enhver retlig forpligtelse, enhver ansættelseskontrakt, enhver økonomisk forpligtelse og ethvert økonomisk ansvar. Alle afgørelser vedtaget af bestyrelsen og forretningsudvalget i overensstemmelse med forordning (EU) nr. 526/2013 forbliver gyldige, forudsat at de er i overensstemmelse med nærværende forordning.

4. ENISA oprettes for en ubegrænset periode fra den 27. juni 2019.

5. Den administrerende direktør, der er udpeget i henhold til artikel 24, stk. 4, i forordning (EU) nr. 526/2013, fortsætter som og udøver sine opgaver som ENISA's administrerende direktør, jf. nærværende forordnings artikel 20, for den resterende del af den administrerende direktørs mandatperiode. De øvrige vilkår i vedkommendes kontrakt fortsætter uændret.

6. Bestyrelsens medlemmer og deres stedfortrædere, der er udpeget i henhold til artikel 6 i forordning (EU) nr. 526/2013, fortsætter som og udøver deres funktioner som bestyrelse, jf. nærværende forordnings artikel 15, for den resterende del af deres mandatperiode.

Artikel 69

Ikrafttræden

1. Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i Den Europæiske Unions Tidende.

2. Artikel 58, 60, 61, 63, 64 og 65 finder anvendelse fra den 28. juni 2021.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Strasbourg, den 17. april 2019.

På Europa-Parlamentets vegne

A. TAJANI

Formand

På Rådets vegne

G. CIAMBA

Formand

-
- (1) EUT C 227 af 28.6.2018, s. 86.
 - (2) EUT C 176 af 23.5.2018, s. 29.
 - (3) Europa-Parlamentets holdning af 12.3.2019 (endnu ikke offentliggjort i EUT) og Rådets afgørelse af 9.4.2019.
 - (4) Kommissionens henstilling af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).
 - (5) Europa-Parlamentets og Rådets forordning (EU) nr. 526/2013 af 21. maj 2013 om Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og om ophævelse af forordning (EF) nr. 460/2004 (EUT L 165 af 18.6.2013, s. 41).
 - (6) Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed (EUT L 77 af 13.3.2004, s. 1).
 - (7) Europa-Parlamentets og Rådets forordning (EF) nr. 1007/2008 af 24. september 2008 om ændring af forordning (EF) nr. 460/2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed for så vidt angår agenturets mandatperiode (EUT L 293 af 31.10.2008, s. 1).
 - (8) Europa-Parlamentets og Rådets forordning (EU) nr. 580/2011 af 8. juni 2011 om ændring af forordning (EF) nr. 460/2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed for så vidt angår agenturets mandatperiode (EUT L 165 af 24.6.2011, s. 3).
 - (9) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).
 - (10) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).
 - (11) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).
 - (12) Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).
 - (13) Afgørelse 2004/97/EF, Euratom truffet ved fælles aftale mellem repræsentanterne for medlemsstaterne, forsamlet på stats- og regeringschefniveau, den 13. december 2003 om fastlæggelse af hjemstedet for visse af Den Europæiske Unions kontorer og agenturer (EUT L 29 af 3.2.2004, s. 15).
 - (14) EUT C 12 af 13.1.2018, s. 1.
 - (15) Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).
 - (16) Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30).
 - (17) Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter (EFT L 145 af 31.5.2001, s. 43).
 - (18) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39).
 - (19) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).
 - (20) Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).
 - (21) Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).
 - (22) Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).
 - (23) Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).
 - (24) EFT L 56 af 4.3.1968, s. 1.
 - (25) Kommissionens delegerede forordning (EU) nr. 1271/2013 af 30. september 2013 om rammefinansforordningen for de organer, der er omhandlet i artikel 208 i Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 966/2012 (EUT L 328 af 7.12.2013, s. 42).
 - (26) Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen (EUT L 72 af 17.3.2015, s. 41).
 - (27) Kommissionens afgørelse (EU, Euratom) 2015/444 af 13. marts 2015 om reglerne for sikkerhedsbeskyttelse af EU's klassificerede informationer (EUT L 72 af 17.3.2015, s. 53).
 - (28) Europa-Parlamentets og Rådets forordning (EU, Euratom) 2018/1046 af 18. juli 2018 om de finansielle regler vedrørende Unionens almindelige budget, om ændring af forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og afgørelse nr. 541/2014/EU og om ophævelse af forordning (EU, Euratom) nr. 966/2012 (EUT L 193 af 30.7.2018, s. 1).
 - (29) Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 af 11. september 2013 om undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og om ophævelse af Europa-Parlamentets og Rådets forordning (EF) nr. 1073/1999 og Rådets forordning (Euratom) nr. 1074/1999 (EUT L 248 af 18.9.2013, s. 1).
 - (30) EFT L 136 af 31.5.1999, s. 15.
 - (31) Rådets forordning (Euratom, EF) nr. 2185/96 af 11. november 1996 om Kommissionens kontrol og inspektion på stedet med henblik på beskyttelse af De Europæiske Fællesskabers finansielle interesser mod svig og andre uregelmæssigheder (EFT L 292 af 15.11.1996, s. 2).
 - (32) Forordning nr. 1 om den ordning, der skal gælde for Det Europæiske Økonomiske Fællesskab på det sproglige område (EFT 17 af 6.10.1958, s. 385/58).

Bilag 2**»Bilag 2****KRAV, DER SKAL OPFYLDES AF OVERENSSTEMMELSESVALGORGANER**

Overensstemmelsesvurderingsorganer, som ønsker at blive akkrediteret, skal opfylde følgende krav:

1. Et overensstemmelsesvurderingsorgan skal oprettes i henhold til national lovgivning og være en juridisk person.
2. Et overensstemmelsesvurderingsorgan skal være et tredjepartsorgan, der er uafhængigt af den organisation eller de IKT-produkter, -tjenester eller -processer, som det vurderer.
3. Et organ, der er medlem af en erhvervsorganisation og/eller brancheforening, som repræsenterer virksomheder, der er involveret i udformning, fremstilling, levering, sammenbygning, brug eller vedligeholdelse af IKT-produkter, -tjenester eller -processer, som det vurderer, kan anses for at være et overensstemmelsesvurderingsorgan, forudsat at det er påvist, at det er uafhængigt, og at der ikke foreligger nogen interessekonflikt.
4. Overensstemmelsesvurderingsorganerne, deres øverste ledelse og de personer, der er ansvarlige for udførelsen af overensstemmelsesvurderingsopgaverne, må ikke være konstruktør, producent, leverandør, installatør, køber, ejer, bruger eller vedligeholder af det IKT-produkt, den IKT-tjeneste eller den IKT-proces, der vurderes, eller repræsentere nogen af disse parter. Dette forbud udelukker ikke, at overensstemmelsesvurderingsorganet bruger de IKT-produkter, der er vurderet og nødvendige for, at det kan udføre sit arbejde, eller brug af sådanne IKT-produkter til personlige formål.
5. Overensstemmelsesvurderingsorganerne, deres øverste ledelse og de personer, der er ansvarlige for at udføre overensstemmelsesvurderingsopgaverne, må ikke være direkte involveret i udformning, fremstilling eller konstruktion, markedsføring, installation, anvendelse eller vedligeholdelse af de IKT-produkter, -tjenester eller -processer, der vurderes, eller repræsentere parter, der er involveret i disse aktiviteter. Overensstemmelsesvurderingsorganerne, deres øverste ledelse og de personer, der er ansvarlige for at udføre overensstemmelsesvurderingsopgaverne, må ikke deltage i aktiviteter, som kan være i strid med deres objektivitet og integritet i forbindelse med deres overensstemmelsesvurderingsaktiviteter. Dette forbud gælder navnlig rådgivningstjenester.
6. Hvis et overensstemmelsesvurderingsorgan ejes eller drives af en offentlig enhed eller institution, skal der sikres uafhængighed og fravær af interessekonflikter mellem den nationale cybersikkerhedscertificeringsmyndighed og overensstemmelsesvurderingsorganet, og dette skal dokumenteres.
7. Overensstemmelsesvurderingsorganet skal sikre, at dets dattervirksomheders og underentreprenørers aktiviteter ikke påvirker fortroligheden, objektiviteten og uvildigheden af dets overensstemmelsesvurderingsaktiviteter.
8. Overensstemmelsesvurderingsorganet og dets personale skal udføre overensstemmelsesvurderingsaktiviteter med den størst mulige faglige integritet og den nødvendige tekniske kompetence på det specifikke område og ikke påvirkes af nogen form for pression og incitament, som kan have indflydelse på deres afgørelser eller resultaterne af deres overensstemmelsesvurderingsaktiviteter, herunder pression og incitament af økonomisk art, særlig fra personer eller grupper af personer, som har en interesse i resultaterne af disse aktiviteter.

9. Et overensstemmelsesvurderingsorgan skal kunne gennemføre alle de overensstemmelsesvurderingsopgaver, som det pålægges i henhold til denne forordning, uanset om disse opgaver udføres af overensstemmelsesvurderingsorganet selv eller på dets vegne og på dets ansvar. Enhver underentreprise eller høring af eksternt personale skal dokumenteres behørigt, må ikke omfatte mellemmand og skal være genstand for en skriftlig aftale, som blandt andet dækker fortrolighed og interessekonflikter. Det pågældende overensstemmelsesvurderingsorgan skal påtage sig det fulde ansvar for de opgaver, der udføres.

10. Et overensstemmelsesvurderingsorgan skal til enhver tid og for hver overensstemmelsesvurderingsprocedure og hver type, kategori eller underkategori af IKT-produkter, -tjenester eller -processer have følgende til rådighed i nødvendigt omfang:

- a) personale med teknisk viden og tilstrækkelig og relevant erfaring til at udføre overensstemmelsesvurderingsopgaverne
- b) beskrivelser af de procedurer, i overensstemmelse med hvilke overensstemmelsesvurdering skal foretages, for at sikre gennemsigtighed i og mulighed for at reproducere disse procedurer. Det skal have indført hensigtsmæssige politikker og procedurer, som skelner mellem de opgaver, som det udfører i sin egenskab af organ anmeldt i henhold til artikel 61, og dets andre aktiviteter
- c) procedurer, der sætter det i stand til at udføre sine aktiviteter under behørig hensyntagen til en virksomheds størrelse, den sektor, som den opererer inden for, og dens struktur, til graden af kompleksitet af det pågældende IKT-produkts, den pågældende IKT-tjenestes eller den pågældende IKT-proces teknologi og til fremstillingsprocessens karakter af masse- eller serieproduktion.

11. Et overensstemmelsesvurderingsorgan skal have de fornødne midler til at udføre de tekniske og administrative opgaver i forbindelse med overensstemmelsesvurderingsaktiviteterne på en egnet måde og skal have adgang til alt nødvendigt udstyr og alle nødvendige faciliteter.

12. De personer, som skal udføre overensstemmelsesvurderingsaktiviteterne, skal have:

- a) en solid teknisk og faglig uddannelse omfattende alle overensstemmelsesvurderingsaktiviteter
- b) et tilstrækkeligt kendskab til kravene vedrørende de overensstemmelsesvurderinger, de foretager, og den nødvendige bekræftelse til at udføre sådanne vurderinger
- c) et tilstrækkeligt kendskab til og en tilstrækkelig forståelse af de gældende krav og prøvningsstandarder
- d) den nødvendige færdighed i at udarbejde de attester, redegørelser og rapporter, som dokumenterer, at overensstemmelsesvurderingerne er blevet foretaget.

13. Der skal være garanti for uvildigheden af overensstemmelsesvurderingsorganerne, deres øverste ledelse, de personer, der er ansvarlige for at udføre overensstemmelsesvurderingsaktiviteterne, og eventuelle underleverandører.

14. Aflønningen af et overensstemmelsesvurderingsorgans øverste ledelse og af de personer, der er ansvarlige for at udføre overensstemmelsesvurderingsaktiviteterne, må ikke afhænge af, hvor mange overensstemmelsesvurderinger det udfører, eller hvordan vurderingerne falder ud.

15. Overensstemmelsesvurderingsorganer skal tegne en ansvarsforsikring, medmindre medlemsstaten er ansvarlig i henhold til sin nationale ret, eller medlemsstaten selv er direkte ansvarlig for overensstemmelsesvurderingen.

16. Et overensstemmelsesvurderingsorgan og dets personale, udvalg, dattervirksomheder, underentreprenører og eventuelle tilknyttede organer eller personalet i et overensstemmelsesvurderingsorgans eksterne organer skal opretholde fortrolighed og har tavshedspligt med hensyn til alle oplysninger, de kommer i besiddelse af ved udførelsen af deres overensstemmelsesvurderingsopgaver i henhold til denne forordning eller enhver bestemmelse i national ret, som gennemfører denne forordning, undtagen hvis offentliggørelse kræves i henhold til EU-retten eller en medlemsstats ret, som sådanne personer er omfattet af, og undtagen over for de kompetente myndigheder i den medlemsstat, hvor aktiviteterne udføres. Intellektuelle ejendomsrettigheder skal beskyttes. Overensstemmelsesvurderingsorganet skal have indført dokumenterede procedurer for så vidt angår kravene i dette punkt.

17. Med undtagelse af punkt 16 forhindrer kravene i dette bilag, at der udveksles tekniske oplysninger og reguleringsmæssig vejledning mellem et overensstemmelsesvurderingsorgan og en person, der ansøger om certificering, eller der overvejer at ansøge om certificering.

18. Overensstemmelsesvurderingsorganer skal fungere i henhold til et sæt konsekvente, retfærdige og rimelige vilkår og betingelser under hensyntagen til interesserne for SMV'er for så vidt angår gebyrer.

19. Overensstemmelsesvurderingsorganer skal opfylde kravene i den relevante standard, som er blevet harmoniseret i henhold til forordning (EF) nr. 765/2008 med henblik på akkrediteringen af overensstemmelsesvurderingsorganer, der foretager certificering af IKT-produkter, -tjenester eller -processer.

20. Overensstemmelsesvurderingsorganer skal sikre, at prøvningslaboratorier, der anvendes til overensstemmelsesvurdering, opfylder kravene i den relevante standard, som er blevet harmoniseret i henhold til forordning (EF) nr. 765/2008 med henblik på akkrediteringen af laboratorier, der gennemfører prøvning.