EUROPA-
KOMMISSIONEN

Bruxelles, den 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed").

(EØS-relevant tekst)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Den Europæiske Union har truffet en række foranstaltninger for at øge sin modstandsdygtighed og styrke sit cybersikkerhedsberedskab. Den første strategi for cybersikkerhed[1], som blev vedtaget i 2013, fastlagde de strategiske målsætninger og konkrete foranstaltninger til at opnå modstandsdygtighed, mindske cyberkriminalitet, udvikle cyberforsvarspolitik og -kapacitet, udvikle industrielle og teknologiske ressourcer og udarbejde en sammenhængende international cyberspacepolitik for EU. Der er i denne forbindelse sket en væsentlig udvikling siden da, herunder navnlig det andet mandat for Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA)[2] og vedtagelsen af **direktivet om sikkerhed for net- og informationssystemer** ("NIS-direktivet")[3], som udgør grundlaget for det foreliggende forslag.

Herudover **vedtog Kommissionen i 2016 en meddelelse om styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri**[4], hvori der blev bebudet yderligere foranstaltninger til at øge samarbejde og informations- og videndeling, EU's modstandskraft og beredskab, også under hensyntagen til muligheden for væsentlige hændelser og en mulig paneuropæisk cybersikkerhedskrise. Kommissionen bebudede i denne sammenhæng, at den ville fremskynde **evalueringen** og **revisionen** af Europa-Parlamentets og Rådets forordning (EU) nr. 526/2013 om ENISA og om ophævelse af forordning (EF) nr. 460/2004 ("ENISA-forordningen") Evalueringsprocessen kunne give anledning til en reform af Agenturet og en styrkelse af dets kompetencer og kapacitet til at støtte medlemsstaterne på en bæredygtig måde. Forslaget ville give Agenturet en mere operationel og central rolle i gennemførelsen af bedre modstandsdygtighed på cybersikkerhedsområdet og ville i det nye mandat anerkende Agenturets nye ansvarsområder i henhold til NIS-direktivet.

NIS-direktivet er et første afgørende skridt med henblik på at fremme en risikostyringskultur ved at indføre sikkerhedskrav som retlige forpligtelser for de vigtigste økonomiske aktører, herunder navnlig operatører af væsentlige tjenester og udbydere af visse centrale digitale tjenester. Da sikkerhedskrav anses for væsentlige for at sikre fordelene ved digitaliseringen af samfundet og på baggrund af den hurtige udbredelse af forbundet udstyr (tingenes Internet – IoT), indgik der i meddelelsen fra 2016 ligeledes et forslag om at fastlægge en ramme for sikkerhedscertificering for IKT-produkter og -tjenester med sigte på at øge tilliden til og sikkerheden i det digitale indre marked. IKT-sikkerhedscertificering er navnlig relevant i lyset af den tiltagende brug af teknologier, som kræver et højt cybersikkerhedsniveau, f.eks. forbundne og selvkørende biler, e-sundhedssystemer eller industrielle automationsstyringssystemer (IACS).

---

1 Kommissionens og EU-Udenrigstjenestens fælles meddelelse: EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace – JOIN (2013).

2 Forordning (EU) nr. 526/2013 om Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og om ophævelse af forordning (EF) nr. 460/2004.

3 Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

4 Kommissionens meddelelse om styrkelse af Europas system for modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri, COM/2016/0410 final.

Disse politiske foranstaltninger og meddelelser blev yderligere styrket af **Rådets konklusioner** i 2016, som anerkendte, at "at cybertrusler og sårbarheder fortsat udvikler sig og tiltager, hvilket vil kræve vedvarende og tættere samarbejde, særlig ved håndteringen af store grænseoverskridende cybersikkerhedshændelser". Konklusionerne bekræftede, at "ENISA-forordningen er et af de centrale elementer i EU's ramme for modstandsdygtighed over for cyberangreb"[5] og opfordrede Kommissionen til at tage yderligere skridt til at håndtere certificeringsspørgsmålet på EU-niveau.

Indførelse af en certificeringsordning forudsætter oprettelsen af et hensigtsmæssigt forvaltningssystem på EU-niveau, herunder en omfattende ekspertise leveret af et uafhængigt EU-agentur. I det foreliggende forslag identificeres ENISA som det naturlige organ på EU-plan, der er kompetent inden for cybersikkerhed, og som kunne overtage en sådan rolle med henblik på at samle og koordinere det arbejde, der udføres af kompetente nationale organer på certificeringsområdet.

I sin meddelelse om **midtvejsevalueringen af strategien for det digitale indre marked af maj 2017** angav Kommissionen endvidere, at den ville revidere ENISA's mandat senest i september 2017. Det skulle ske for at definere Agenturets rolle i det ændrede IT-sikkerhedsøkosystem og udvikle foranstaltninger vedrørende cybersikkerhedsstandarder, -certificering og -mærkning for at gøre IKT-baserede systemer, herunder netforbundne objekter, mere cybersikre[6]. **Det Europæiske Råds konklusioner** af juni 2017[7] ser positivt på Kommissionens intentioner om at revidere cybersikkerhedsstrategien i september og foreslå yderligere målrettede aktioner inden udgangen af 2017.

Den foreslåede forordning fastlægger et omfattende sæt foranstaltninger, som bygger på tidligere foranstaltninger og fremmer specifikke mål, som indbyrdes styrker hinanden:

- **Øgede kapaciteter og beredskab** i medlemsstaterne og virksomhederne
- Forbedret **samarbejde og samordning** mellem medlemsstaterne og EU's institutioner, agenturer og organer
- Øget **kapacitet på EU-niveau til at supplere medlemsstaternes indsats**, navnlig i tilfælde af grænseoverskridende cyberkriser
- Øget **oplysning** til borgere og virksomhederne om cybersikkerhed
- Øget overordnet **gennemsigtighed af cybersikkerhedstillidsniveauet**[8] for IKT-produkter og -tjenester med sigte på at styrke tilliden til det digitale indre marked og digital innovation og
- Undgåelse af **opsplitning af certificeringsordningerne** i EU og dermed forbundne sikkerhedskrav og evalueringskriterier på tværs af medlemsstater og sektorer.

---

5 Rådets konklusioner om styrkelse af Europas modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri – 15. november 2016.

6 Kommissionens meddelelse om midtvejsevalueringen af gennemførelsen af strategien for det digitale indre marked – COM(2017)228.

7 Det Europæiske Råds møde (den 22. og 23. juni 2017) – konklusioner EUCO 8/17.

8 Gennemsigtighed af sikringen af cybersikkerheden betyder, at brugerne får tilstrækkelige oplysninger om cybersikkerhedsegenskaber til objektivt at kunne bedømme sikkerhedsniveauet for et givet IKT-produkt, -tjeneste eller -proces.

I den følgende del af begrundelsen forklares baggrunden for initiativet med hensyn til de foreslåede foranstaltninger vedrørende ENISA og cybersikkerhedscertificering nærmere.

ENISA

ENISA fungerer som et ekspertisecenter, der har til opgave at forbedre net- og informationssikkerheden i EU og støtte kapacitetsopbygningen i medlemsstaterne.

ENISA blev oprettet i 2004[9] for at bidrage til det overordnede mål om at sikre et højt fælles niveau for net- og informationssikkerhed i EU. I 2013 blev Agenturets nye mandat fastsat for en periode på syv år frem til 2020 ved forordning (EU) nr. 526/2013. Agenturet har sit hjemsted i Grækenland, dvs. det administrative sæde i Heraklion (Kreta) og det centrale operationelle hovedsæde i Athen.

ENISA er et lille agentur med et lille budget og et lille antal ansatte i forhold til alle EU's andre agenturer. Det har en tidsbegrænset mandatperiode.

ENISA bistår EU-institutionerne, medlemsstaterne og erhvervslivet med at **behandle, tackle og navnlig forebygge net- og informationssikkerhedsproblemer**. Det foregår gennem en række aktiviteter på fem områder, som er udpeget i Agenturets strategi[10]:

- Ekspertise: tilrådighedsstillelse af oplysninger og ekspertviden om centrale net- og informationssikkerhedsspørgsmål
- Politik: støtte til politisk beslutningstagning og gennemførelse i Unionen
- Kapacitet: støtte til kapacitetsopbygning i hele EU (f.eks. gennem uddannelse, henstillinger, oplysningskampagner)
- Fællesskab: fremme net- og informationssikkerhedsfællesskabet (f.eks. støtte til IT-beredskabsenheder (CERT), koordinering af fælleseuropæiske cyberberedskabsøvelser)
- Facilitering (f.eks. ved at inddrage interesserede parter og internationale forbindelser).

I løbet af forhandlingerne om NIS-direktivet besluttede EU-medlovgiverne at give ENISA en fremtrædende rolle ved gennemførelsen af dette direktiv. Agenturet varetager navnlig sekretariatsfunktionen for CSIRT-netværket (oprettet for at fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne om specifikke cybersikkerhedshændelser og informationsudveksling om risici) og det bistår også samarbejdsgruppen med udførelsen af dens opgaver. Herudover pålægger direktivet ENISA at bistå medlemsstaterne og Kommissionen med ekspertise og rådgivning og at lette udveksling af bedste praksis.

I overensstemmelse med ENISA-forordningen har Kommissionen gennemført en evaluering af Agenturet, som omfatter en uafhængig undersøgelse og en offentlig høring. Evalueringen vurderede Agenturets relevans, virkning, effektivitet, omkostningseffektivitet, sammenhæng og EU-merværdi med hensyn til dets præstationer, styring, intern organisatorisk struktur og arbejdsmetoder i perioden 2013-2016.

---

9 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).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

ENISA's præstationer blev samlet set bedømt positivt af et flertal af respondenterne[11] (74%) i den offentlige høring. Et flertal af respondenterne mente endvidere, at ENISA når sine forskellige mål (mindst 63 % for hvert enkelt mål). ENISA's tjenester og produkter bruges regelmæssigt (en gang om måneden eller hyppigere) af næsten halvdelen af respondenterne (46 %), og de værdsættes for den omstændighed, at de stammer fra et EU-organ (83 %) og kvaliteten (62 %).

Et stort flertal (88 %) af respondenterne mente dog, at de aktuelle instrumenter og mekanismer, der er til rådighed på EU-plan, er utilstrækkelige eller kun delvis fyldestgørende til at håndtere de nuværende udfordringer på cybersikkerhedsområdet. Et stort flertal af respondenterne (98 %) mente, at der var behov for et EU-organ til at tackle udfordringerne, og 99 % anså ENISA for at være den rette organisation hertil. Herudover udtrykte 67,5 % den mening, at ENISA kan spille en rolle ved fastlæggelse af en harmoniseret ramme for sikkerhedscertificering af IT-produkter og -tjenester.

Den overordnede evaluering (ikke kun baseret på den offentlige høring, men også en række individuelle interviews, yderligere målrettede undersøgelser og workshopper) nåede til følgende konklusioner:

- ENISA's målsætninger er stadig relevante i dag. I en kontekst med hurtig teknologisk udvikling og skiftende trusler og i lyset af de tiltagende globale cybersikkerhedsrisici er der et klart behov i EU for fremme og yderligere styrkelse af teknisk ekspertise på højt plan, når det gælder cybersikkerhed. Der må opbygges kapacitet i medlemsstaterne til at forstå og imødegå trusler, og interessenterne må samarbejde på tværs af temaområder og institutioner.
- Til trods for sit begrænsede budget er Agenturet drevet omkostningseffektivt med hensyn til ressourceforbrug og gennemførelsen af dets opgaver. Opdelingen mellem Athen og Heraklion har imidlertid også medført ekstra administrative omkostninger.
- For så vidt angår omkostningseffektivitet, opfyldte ENISA delvis sine mål. Agenturet har med succes bidraget til at forbedre net- og informationssikkerheden i EU ved at tilbyde kapacitetsopbygning i 28 medlemsstater[12], ved at forbedre samarbejdet mellem medlemsstater og interessenter på net- og informationssikkerhedsområdet og ved at stille ekspertise til rådighed, opbygge fællesskaber og støtte udvikling af politikker. Overordnet set fokuserede ENISA omhyggeligt på gennemførelsen af sit arbejdsprogram og fungerede som en pålidelig partner for sine interessenter inden for et område, hvis grænseoverskridende dimension først for nylig er blevet anerkendt.

---

[11] 90 interessenter fra 19 medlemsstater svarede under høringen (88 besvarelser og 2 holdningsdokumenter), herunder nationale myndigheder fra 15 medlemsstater og 8 paraplyorganisationer, som repræsenterer et betydeligt antal europæiske virksomheder.

[12] Respondenterne i den offentlige høring blev bedt om at kommentere, hvad de opfattede som ENISA's vigtigste resultater i perioden 2013-2016. Respondenter fra alle grupper (55 i alt, herunder 13 fra nationale myndigheder, 20 fra den private sektor og 22 fra "andre") anså følgende for at være ENISA's vigtigste resultater: 1) Koordineringen af Cyber Europe-øvelser, 2) støtte til CERT/CSIRT-enheder gennem uddannelseskurser og workshopper for at fremme koordinering og udveksling, 3) ENISA's publikationer (retningslinjer og henstillinger, cybertrusselrapporter, strategier for indberetning af hændelser og krisestyring osv.), som blev anset for nyttige til at oprette og ajourføre nationale sikkerhedsrammer samt som referencer for politiske beslutningstagere og cybereksperter, 4) bistand med at fremme af NIS-direktivet, 5) indsatsen for at øge bevidstheden om cybersikkerhed gennem afholdelse af cybersikkerhedsmåneden (Cyber Security Month).

- ENISA har gjort en forskel, i hvert fald i et vist omfang, inden for det omfattende net- og informationssikkerhedsområde, men har ikke fuldt ud formået at udvikle et stærkt "brand" og opnå tilstrækkelig synlighed til at blive anerkendt som "det" europæiske ekspertisecenter. Årsagen hertil ligger i ENISA's brede mandat, idet der ikke blev tildelt tilsvarende tilstrækkelige ressourcer. Derudover er ENISA stadig det eneste EU-agentur med et tidsbegrænset mandat, hvilket begrænser dets evne til at udvikle en langsigtet vision og støtte sine interessenter på en bæredygtig måde. Dette er også i modstrid med bestemmelserne i NIS-direktivet, som overdrager opgaver til ENISA, som ikke har nogen slutdato. Endelig konstateres det i vurderingen, at denne manglende effektivitet delvis kan forklares med den høje afhængighed af ekstern i forhold til intern ekspertise og med vanskeligheder med at rekruttere og holde på specialiseret personale.
- Sidst men ikke mindst konkluderes det i evalueringen, at ENISA's merværdi primært ligger i Agenturets evne til at forbedre samarbejdet, hovedsageligt mellem medlemsstaterne og navnlig med beslægtede net- og informationssikkerhedsfælleskaber (navnlig mellem CSIRT). Der findes ingen anden aktør på EU-plan, der støtter et så bredt udsnit af interessenter på området net- og informationssikkerhed. På grund af behovet for nøje at prioritere sine aktiviteter er ENISA's arbejdsprogram for det meste styret af medlemsstaternes behov. Som følge heraf er det ikke tilstrækkeligt rettet mod andre interessenters behov, herunder navnlig erhvervslivets. Det gjorde også Agenturet mere tilbøjelig til at opfylde sine vigtigste interessenters behov, hvilket forhindrede det i at opnå en større virkning. Agenturets merværdi har således været varierende, alt efter de forskellige interessenters behov og det omfang, i hvilket Agenturet var i stand til at opfylde dem (f.eks. store over for små medlemsstater, medlemsstaterne over for erhvervslivet).

Sammenfattende kan det siges, at høringerne af interessenter og evalueringen tydede på, at ENISA's ressourcer og mandat må tilpasses, så det i tilstrækkelig grad kan reagere på nuværende og fremtidige udfordringer.

På baggrund af disse konstateringer gennemgår nærværende forslag ENISA's mandat og fastsætter et nyt sæt opgaver og funktioner med sigte på effektiv og omkostningseffektiv støtte til medlemsstaternes, EU-institutionernes og andre interessenters indsats for et sikkert cyberspace i Den Europæiske Union. Det nye foreslåede mandat søger at give Agenturet en stærkere og mere central rolle, navnlig ved også at støtte medlemsstaternes gennemførelse af NIS-direktivet og for at modvirke særlige trusler på en mere aktiv måde (operationel kapacitet) og ved at blive et ekspertisecenter, som støtter medlemsstaterne og Kommissionen i forbindelse med cybersikkerhedscertificering. I henhold til forslaget:

- Får ENISA et permanent mandat og således et stabilt grundlag for fremtiden. Mandatet, målene og opgaverne bør fortsat være genstand for regelmæssig revision.
- Det foreslåede mandat præciserer ENISA's mandat yderligere som EU' Agentur for cybersikkerhed og referencepunkt i EU's cybersikkerhedsøkosystem, der agerer i tæt samarbejde med alle andre relevante organer i et sådant økosystem.
- Agenturets organisation og styring, som fik en positiv vurdering under evalueringen, vil blive moderat revideret, navnlig for at tage højde for, at behovene i det bredere interessentfællesskab afspejles bedre i Agenturets arbejde.
- Det foreslåede omfang af mandatet opridses, idet de områder styrkes, hvor Agenturet har vist en klar merværdi, og der tilføjes de nye områder, hvor der er brug for støtte på grund af de nye politiske prioriteter og instrumenter, navnlig NIS-direktivet,

revisionen af EU's strategi for cybersikkerhed, den kommende plan for EU's cybersikkerhedssamarbejde i krisesituationer og IKT-sikkerhedscertificering:

- **Udvikling og gennemførelse af EU-politikker:** ENISA får til opgave at bidrage proaktivt til udviklingen af politikken på området net- og informationssikkerhed samt andre politiske initiativer med cybersikkerhedselementer inden for forskellige sektorer (f.eks. energi, transport, finans). Agenturet får i denne forbindelse en stærk rådgivende rolle, som det kan udfylde ved at levere uafhængige vurderinger og forberedende arbejde til udvikling og ajourføring af politikker og lovgivning. ENISA vil også understøtte EU's politikker og lovgivning inden for området elektronisk kommunikation og elektroniske identifikations- og tillidstjenester med sigte på at fremme et højere cybersikkerhedsniveau. I gennemførelsesfasen, herunder navnlig i forbindelse med NIS-samarbejdsgruppen, vil ENISA bistå medlemsstaterne med at opnå en konsekvent tilgang for så vidt angår gennemførelsen af NIS-direktivet på tværs af grænser og sektorer samt i forbindelse med andre relevante politikker og lovgivning. Med sigte på at understøtte den regelmæssige revision af politikker og lovgivning på cybersikkerhedsområdet vil ENISA også foretage regelmæssige indberetninger om status for gennemførelsen af EU's retlige rammer.

- **Kapacitetsopbygning:** ENISA vil bidrage til at forbedre EU's og de nationale offentlige myndigheders kapacitet og ekspertise, herunder når det gælder håndtering af hændelser og overvågning af cybersikkerhedsrelaterede lovgivningsmæssige foranstaltninger. Agenturet vil også skulle bidrage til etableringen af centre for informationsudveksling og analyse (ISAC'er) inden for en række sektorer ved at stille bedste praksis og vejledning om tilgængelige værktøjer og procedurer til rådighed samt ved på passende vis at håndtere lovgivningsmæssige spørgsmål relateret til informationsudveksling.

- **Viden og information samt oplysning:** ENISA vil blive EU's informationsknudepunkt. Det indebærer fremme og udveksling af bedste praksis og initiativer på tværs af EU ved at samle oplysninger om cybersikkerhed, der kommer fra EU og nationale institutioner, agenturer og organer. Agenturet vil også stille rådgivning, vedledning og bedste praksis vedrørende sikkerheden af kritiske infrastrukturer til rådighed. I kølvandet på væsentlige grænseoverskridende cybersikkerhedshændelser vil ENISA desuden udarbejde rapporter med henblik på at give vejledning til virksomheder og borgere i hele EU. Denne arbejdsstrøm vil også omfatte tilrettelæggelse af oplysningskampagner i samarbejde med medlemsstaternes myndigheder.

- **Markedsrelaterede opgaver (standardisering, cybersikkerhedscertificering):** ENISA vil udføre en række funktioner, herunder navnlig understøttelse af det indre marked og et cybersikkerhedsmarkedsobservatorium, ved at analysere de relevante udviklingstendenser på cybersikkerhedsmarkedet med sigte på at matche udbud og efterspørgsel bedre, og ved at understøtte EU's politikudvikling inden for IKT-standardisering og IKT-cybersikkerhedscertificering. Navnlig for så vidt angår standardisering vil Agenturet lette indførelsen og udbredelsen af cybersikkerhedsstandarder. ENISA vil også udføre de opgaver, der er fastsat i forbindelse med den fremtidige ramme for certificering (se i det følgende).

- **Forskning og innovation:** ENISA vil bidrage med sin ekspertise ved at rådgive EU og nationale myndigheder om fastsættelse af prioriteter inden for forskning og udvikling, herunder også i sammenhæng med det kontraktlige offentlig-private partnerskab vedrørende cybersikkerhed (cPPP). ENISA's rådgivning om forskning ville bidrage til det nye europæiske forsknings- og kompetencecenter for cybersikkerhed under den næste flerårige finansielle ramme. ENISA ville også – efter anmodning fra Kommissionen – være involveret i gennemførelsen af EU's finansieringsprogrammer inden for forskning og innovation.
- **Operationelt samarbejde og krisestyring:** Denne strøm af arbejde bør bygge på en styrkelse af de eksisterende forebyggende operationelle kapaciteter, herunder navnlig en opgradering af den fælleseuropæiske cybersikkerhedsøvelse (Cyber Europe) ved at gennemføre den årligt, og på en understøttende rolle i det operationelle samarbejde som sekretariat for CSIRT-netværket (jf. NIS-direktivet) ved bl.a. at sikre, at CSIRT-netværkets IT-infrastruktur og kommunikationskanaler er velfungerende. I denne sammenhæng er et struktureret samarbejde med CERT-EU, Det europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) og andre relevante EU-organer påkrævet. Derudover burde et struktureret samarbejde med CERT-EU, i tæt fysisk nærhed, føre til en funktion bestående af levering af teknisk bistand i tilfælde af væsentlige hændelser og støtte til analyse af hændelser. Medlemsstater, som anmoder om det, vil modtage bistand til at håndtere hændelser og støtte til analyser af sårbarheder, spor (artefacts) og hændelser med det formål at styrke deres egen forebyggende og reaktive kapacitet.
- ENISA vil også spille en rolle i **EU's cybersikkerhedsplan**, der forelægges som en del af denne pakke, og som fastlægger Kommissionens henstilling til medlemsstaterne om en koordineret reaktion på væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser på EU-plan[13]. ENISA vil lette samarbejdet mellem de enkelte medlemsstater, når disse skal håndtere en krise, ved at analysere og aggregere nationale situationsrapporter, der bygger på oplysninger, som medlemsstaterne og andre enheder frivilligt stiller til rådighed for Agenturet.

- **Cybersikkerhedscertificering af IKT-produkter og -tjenester**

Med henblik på at skabe og opretholde tillid og sikkerhed skal IKT-produkter og -tjenester direkte indeholde sikkerhedsfunktioner i de tidlige stader af deres tekniske udformning og udvikling (sikkerhed i designet). Herudover bør kunder og brugere kunne fastslå tillidsniveauet for sikkerheden af de produkter og tjenester, de kontraherer eller køber.

Certificering, som består af en formel evaluering af produkter, tjenester og processer foretaget af et uafhængigt og godkendt organ i forhold til et defineret sæt standardkriterier og udstedelsen af en attest for overensstemmelse, spiller en vigtig rolle med hensyn til at øge tilliden til og sikkerheden af produkter og tjenester. Selv om sikkerhedsevalueringer er et ret

[13] Denne plan anvendes i forbindelse med cybersikkerhedshændelser, der er så forstyrrende, at en medlemsstat ikke kan håndtere dem alene, eller som påvirker to eller flere medlemsstater med så vidtrækkende og væsentlige konsekvenser af teknisk eller politisk betydning, at de kræver rettidig politisk koordination og reaktion på EU-politisk niveau.

teknisk område, har certificering til formål at informere og berolige købere og brugere for så vidt angår sikkerhedsegenskaberne for de produkter og tjenester, som de køber eller bruger. Som nævnt i det foregående er dette særligt relevant for nye systemer, der i vidt omfang benytter digitale teknologier, og som kræver et højt sikkerhedsniveau, såsom forbundne og selvkørende biler, e-sundhedssystemer, industrielle automationsstyringssystemer (IACS)[14] eller intelligente net.

I øjeblikket foregår cybersikkerhedscertificering af IKT-produkter og -tjenester i EU på en meget uensartet måde. Der er en række internationale initiativer såsom de såkaldte fælles kriterier (CC) for evaluering af IT-sikkerhed (ISO 15408), som er en international standard for evaluering af computersikkerhed. Den er baseret på tredjepartsevaluering og arbejder med syv Evaluation Assurance Levels (EAL). CC og den ledsagende fælles evalueringsmetode (Common Methodology for Information Technology Security Evaluation (CEM)) er det tekniske grundlag for en international aftale, aftalen om anerkendelse af de fælles kriterier (CCRA), som sikrer at CC-attester anerkendes af alle underskriverne af CCRA. I den aktuelle version af CCRA er det dog kun evalueringer op til EAL 2, der gensidigt anerkendes. Der er desuden kun 13 medlemsstater, der har undertegnet denne aftale.

Certificeringsmyndighederne i 12 medlemsstater har indgået en aftale om gensidig anerkendelse med hensyn til attester, der er udstedt i overensstemmelse med aftalen på grundlag af de fælles kriterier[15]. Derudover findes der, eller der er ved at blive etableret en række IKT-certificeringsinitiativer i medlemsstaterne. Uanset hvor vigtige disse er, indebærer de en risiko for, at markedet fragmenteres, og at der opstår interoperabilitetsproblemer. Som følge heraf kan en virksomhed blive nødt til at gennemgå forskellige certificeringsprocedurer i en række medlemsstater for at være i stand til at udbyde sit produkt på flere markeder. F.eks. skal en producent af intelligente målere, som ønsker at sælge sit produkt i tre medlemsstater, f.eks. Tyskland, Frankrig og Det Forenede Kongerige, i øjeblikket overholde kravene i tre forskellige certificeringsordninger. Det drejer sig om Commercial Product Assurance (CPA) i Det Forenede Kongerige, Certification de Sécurité de Premier Niveau (CSPN) i Frankrig og en særlig beskyttelsesprofil baseret på de fælles kriterier i Tyskland.

Denne situation fører til højere omkostninger og er en betydelig administrativ byrde for virksomheder, som er aktive i flere medlemsstater. Certificeringsomkostningerne kan variere væsentligt afhængigt af det/den pågældende produkt/tjeneste, det ønskede evalueringsniveau og/eller andre komponenter, men har tendens til at være temmelig store for virksomhederne. For BSI's "Smart Meter Gateway"-attest er omkostningerne f.eks. mere end 1 mio. EUR (højeste test- og sikkerhedsniveau, ikke blot for ét produkt men for hele den omgivende infrastruktur også). I Det Forenede Kongerige er omkostningerne til certificering af intelligente målere næsten 150 000 EUR. I Frankrig er omkostningerne omtrent det samme som i Det Forenede Kongerige, nemlig 150 000 EUR eller mere.

---

[14] GD JRC har offentliggjort en rapport, som foreslår et første sæt fælleseuropæiske krav og brede retningslinjer vedrørende cybersikkerhedscertificering af IACS-komponenter. Findes på: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Gruppen af Højtstående Embedsmænd vedrørende Informationssystemers Sikkerhed (SOG-IS) omfatter 12 medlemsstater plus Norge og har udviklet nogle få beskyttelsesprofiler for et begrænset antal produkter såsom digital underskrift, digital tachograf og smartkort. Deltagerne arbejder sammen om at koordinere standardiseringen af CC-beskyttelsesprofiler og om at samordne udviklingen af beskyttelsesprofiler. Medlemsstaterne anmoder ofte om SOG-IS-certificering for nationale offentlige udbud.

Vigtige offentlige og private interessenter erkender, at når der ikke er en EU-dækkende certificeringsordning for cybersikkerhed, vil virksomheder i mange tilfælde skulle have foretaget en individuel certificering i hver medlemsstat, hvilket fører til markedsopsplitning. Vigtigst af alt – hvis der ikke er nogen EU-harmonisering af lovgivning for IKT-produkter og tjenester – vil forskelle i cybersikkerhedscertificeringsstandarder og -praksis i medlemsstaterne sandsynligvis skabe 28 separate cybersikkerhedsmarkeder i praksis, hvert med sine egne tekniske krav, testmetoder og certificeringsprocedurer for cybersikkerhed. Disse divergerende tilgange på nationalt plan vil - hvis der ikke træffes passende foranstaltninger på EU-plan - sandsynligvis medføre tilbageslag i gennemførelsen af det digitale indre marked ved at sinke eller forhindre de tilknyttede positive virkninger i form af vækst og beskæftigelse.

På denne baggrund opstiller forslaget til forordning en europæisk ramme for cybersikkerhedscertificering ("**rammen**") for IKT-produkter og -tjenester og præciserer de væsentlige funktioner og opgaver for ENISA inden for cybersikkerhedscertificering. Nærværende forslag fastsætter en samlet ramme af regler for europæiske cybersikkerhedscertificeringsordninger. Forslaget indfører ikke direkte operationelle certificeringsordninger, men skaber nærmere et system (en ramme) for indførelsen af specifikke certificeringsordninger for specifikke IKT-produkter/tjenester ("europæiske cybersikkerhedscertificeringsordninger"). Oprettelsen af europæiske cybersikkerhedscertificeringsordninger i overensstemmelse med rammen vil sørge for, at attester udstedt i henhold til sådanne ordninger er gyldige og anerkendes i alle medlemsstater og afhjælpe den aktuelle markedsopsplitning.

Det overordnede mål med en europæisk cybersikkerhedscertificeringsordning er at attestere, at de IKT-produkter og -tjenester, der er certificeret i overensstemmelse med en sådan ordning, opfylder de nærmere fastsatte cybersikkerhedskrav. Det vil f.eks. omfatte deres evne til at beskytte data (hvad enten de lagres, overføres eller på anden måde behandles) mod hændelig eller uautoriseret lagring, behandling, adgang, offentliggørelse, ødelæggelse, utilsigtet tab eller ændring. EU-ordninger for cybersikkerhedscertificering vil gøre brug af de eksisterende standarder i relation til de tekniske krav og evalueringsprocedurerne, som produkterne skal overholde, og vil ikke selv udvikle tekniske standarder[16]. F.eks. vil en EU-dækkende certificering for produkter såsom smartkort, der i øjeblikket testes i henhold til internationale CC-standarder under den multilaterale SOG-IS-ordning (som tidligere beskrevet) betyde, at denne ordning bliver gyldig i hele EU.

Ud over at beskrive et specifikt sæt sikkerhedsmålsætninger, som skal tages i betragtning i forbindelse med udformningen af en europæisk ordning for cybersikkerhedscertificering, er det også anført i forslaget, hvad sådanne ordninger mindst bør omfatte. Ordningerne vil bl.a. skulle fastsætte en række specifikke elementer, der angiver omfanget og indholdet af cybersikkerhedscertificeringen. Det omfatter bl.a. udpegelse af de omfattede produkter og tjenester, nærmere specifikation af cybersikkerhedskravene (f.eks. med henvisning til relevante standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder og det tillidsniveau, de påtænkes at garantere (dvs. grundlæggende, betydeligt eller højt).

De europæiske cybersikkerhedscertificeringsordninger udarbejdes af ENISA med bistand af og i tæt samarbejde med den europæiske cybersikkerhedscertificeringsgruppe (se nedenfor)

[16] Hvad angår europæiske standarder, sker det gennem de europæiske standardiseringsorganisationer og godkendes af Europa-Kommissionen ved offentliggørelse i *Den Europæiske Unions Tidende* (jf. forordning 1025/2012).

og vedtages af Kommissionen ved hjælp af gennemførelsesretsakter. Når der konstateres et behov for en cybersikkerhedscertificeringsordning, anmoder Kommissionen ENISA om at udarbejde en ordning for specifikke IKT-produkter eller -tjenester. ENISA's arbejde med ordningen foregår i tæt samarbejde med nationale certificeringsmyndigheder, som er repræsenteret i gruppen. Medlemsstaterne og gruppen kan foreslå Kommissionen, at den anmoder ENISA om at udarbejde en særlig ordning.

Certificering kan være en meget dyr proces, som kan medføre højere priser for kunderne og forbrugerne. Behovet for en certificering kan også variere betydeligt alt efter den specifikke sammenhæng, i hvilken produkter og tjenester anvendes, og hvor hurtigt den teknologiske udvikling forløber. At få foretaget en europæisk cybersikkerhedscertificering bør derfor fortsat være frivilligt, medmindre andet er fastsat i EU-lovgivningen eller national lovgivning om sikkerhedskrav for IKT-produkter og -tjenester.

For at sikre harmonisering og undgå fragmentering bør nationale cybersikkerhedscertificeringsordninger eller -procedurer for IKT-produkter og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, dog ophøre med at have virkning fra det tidspunkt, der er fastsat i den gennemførelsesretsakt, hvorved ordningen vedtages. Medlemsstaterne bør desuden ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der er omfattet af en bestående europæisk cybersikkerhedscertificeringsordning.

Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenterne af IKT-produkter og udbydere af IKT-tjenester indgive en ansøgning om certificering af deres produkter eller tjenester til et overensstemmelsesvurderingsorgan efter eget valg. Overensstemmelsesvurderingsorganer bør akkrediteres af et akkrediteringsorgan, hvis de opfylder visse nærmere fastsatte krav. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt overensstemmelsesvurderingsorganet opfylder kravene. Akkrediteringsorganer tilbagekalder akkrediteringen af et overensstemmelsesvurderingsorgan, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis foranstaltninger truffet af et overensstemmelsesvurderingsorgan er i modstrid med denne forordning.

I henhold til forslaget er det medlemsstaterne, der har ansvaret for overvågning, tilsyn og håndhævelse. Medlemsstaterne vil skulle sørge for, at der er en myndighed, som fører tilsyn med certificeringen. Denne myndighed vil få til opgave at føre tilsyn med overensstemmelsesvurderingsorganernes overholdelse af reglerne og med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, samt overholdelsen af kravene i denne forordning og de relevante europæiske cybersikkerhedscertificeringsordninger. De nationale certificeringstilsynsmyndigheder vil være kompetente til at behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område. De undersøger i det relevante omfang genstanden for klagen og underretter klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist. Herudover samarbejder de med andre certificeringstilsynsmyndigheder eller andre offentlige myndigheder, f.eks. ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings bestemmelser eller de specifikke europæiske cybersikkerhedscertificeringsordninger.

Endelig fastsætter forslaget oprettelsen af den europæiske cybersikkerhedscertificeringsgruppe ("gruppen"), som består af alle medlemsstaters nationale certificeringstilsynsmyndigheder. Gruppens vigtigste opgave er at rådgive Kommissionen om problemstillinger vedrørende cybersikkerhedscertificeringspolitik og at samarbejde med

ENISA om udarbejdelsen af udkast til europæiske cybersikkerhedscertificeringsordninger. ENISA vil bistå Kommissionen med at varetage sekretariatsfunktionen for gruppen og føre et ajourført offentligt register over ordninger, som er godkendt i henhold til den europæiske ramme for cybersikkerhedscertificering. ENISA vil også forestå kontakten med standardiseringsorganer for at sikre, at passende standarder bruges i godkendte ordninger, og for at udpege områder, hvor der er behov for cybersikkerhedsstandarder.

Den europæiske ramme for cybersikkerhedscertificering ("rammen") vil give en række fordele for borgere og virksomheder Det gælder navnlig følgende:

- Oprettelsen af EU-dækkende cybersikkerhedscertificeringsordninger for bestemte produkter eller tjenester vil give virksomhederne en "one-stop-shop" for cybersikkerhedscertificering i EU. Virksomhederne vil kunne få certificeret deres produkt én gang og få en attest, som er gyldig i alle medlemsstater. De vil ikke være forpligtet til at foretage en fornyet certificering af deres produkter hos forskellige nationale certificeringsorganer. Det vil sænke virksomhedernes omkostninger væsentligt og lette grænseoverskridende transaktioner og i sidste ende mindske opsplitningen af det indre marked for de pågældende produkter.
- Rammen fastsætter, at de europæiske cybersikkerhedscertificeringsordninger har forrang frem for nationale ordninger: Denne bestemmelse betyder, at vedtagelsen af en europæisk cybersikkerhedscertificeringsordning træder i stedet for alle eksisterende parallelle nationale ordninger for de samme IKT-produkter og -tjenester på et givet tillidsniveau. Det vil give yderligere klarhed og begrænse den nuværende udbredelse af overlappende og potentielt modstridende nationale cybersikkerhedscertificeringsordninger.
- Forslaget supplerer og støtter gennemførelsen af NIS-direktivet ved at give de af direktivet omfattede virksomheder et meget nyttigt redskab til at påvise overensstemmelse med NIS-kravene i hele Unionen. Under udvikling af nye cybersikkerhedscertificeringsordninger vil Kommissionen og ENISA lægge særlig vægt på behovet for at sikre, at NIS-kravene afspejles i cybersikkerhedscertificeringsordningerne.
- Forslaget vil støtte og fremme udviklingen af en europæisk cybersikkerhedspolitik ved at harmonisere betingelserne og de materielle krav til cybersikkerhedscertificering af IKT-produkter og -tjenester i EU. De europæiske cybersikkerhedscertificeringsordninger vil henvise til fælles standarder eller evalueringskriterier og prøvningsmetoder. Det vil bidrage væsentligt (omend indirekte) til udbredelsen af fælles sikkerhedsløsninger i EU og dermed også til at fjerne hindringer på det indre marked.
- Rammen er udformet på en sådan måde, at den sikrer den nødvendige fleksibilitet for cybersikkerhedscertificeringsordninger. Afhængigt af de specifikke cybersikkerhedsbehov kan et produkt eller en tjeneste certificeres på et højere eller lavere sikkerhedsniveau. De europæisk cybersikkerhedscertificeringsordninger vil blive udformet med denne fleksibilitet i tankerne og vil derfor tilbyde forskellige tillidsniveauer (dvs. grundlæggende, betydeligt eller høj), så de kan anvendes til forskellige formål eller i forskellige sammenhænge.
- Alle elementer nævnt i det foregående vil gøre cybersikkerhedscertificering mere tiltrækkende for virksomhederne som et effektivt middel til at kommunikere cybersikkerhedstillidsniveauet for IKT-produkter og -tjenester. I det omfang cybersikkerhedscertificering bliver billigere, mere effektivt og kommercielt

tiltrækkende vil virksomhederne have større incitament til at certificere deres produkter mod cybersikkerhedsrisici og derved bidrage til udbredelsen af bedre cybersikkerhedspraksis inden for udformningen af IKT-produkter og -tjenester (cybersecurity by design).

- **Sammenhæng med de gældende regler på samme område**

Ifølge NIS-direktivet skal aktører i sektorer, som er af afgørende betydning for vores økonomi og samfund såsom energi, transport, vand, bankvirksomhed, finansmarkedsinfrastrukturer, sundhed og digital infrastruktur samt udbydere af digitale tjenester (dvs. søgemaskiner, cloud computing-tjenester og onlinemarkedspladser), træffe foranstaltninger for på passende vis at håndtere sikkerhedsrisici. De nye regler i dette forslag supplerer og sikrer sammenhængen med bestemmelserne i NIS-direktivet med sigte på at udbygge EU's cybermodstandsdygtighed gennem øget kapacitet, samarbejde, risikostyring og bevidsthed om cybersikkerhed.

Herudover tilvejebringer reglerne om cybersikkerhedscertificering et væsentligt redskab for virksomheder, der er omfattet af NIS-direktivet, idet de vil kunne certificere deres IKT-produkter og -tjenester mod cybersikkerhedsrisici på grundlag af cybersikkerhedscertificeringsordninger, der er gyldige og anerkendes i hele EU. De vil også supplere sikkerhedskravene nævnt i forordningen om elektronisk identifikation og tillidstjenester[17] og direktivet om radioudstyr[18].

- **Sammenhæng med Unionens politik på andre områder**

Forordning (EU) 2016/679 ("**den generelle forordning om databeskyttelse**")[19] fastsætter bestemmelser om indførelse af certificeringsordninger og databeskyttelsesmærkninger med sigte på at demonstrere, at dataansvarliges og databehandleres databehandlingsoperationer er i overensstemmelse med denne forordning. Nærværende forordning berører ikke certificeringen af databehandlingsoperationer, herunder hvis sådanne operationer er indeholdt i produkter og tjenester, som foretages i henhold til den generelle forordning om databeskyttelse.

Den foreslåede forordning vil sikre overensstemmelse med forordning (EF) nr. 765/2008 om akkreditering og markedsovervågning[20] ved at henvise til denne rammes regler om nationale akkrediteringsorganer og overensstemmelsesvurderingsorganer. For så vidt angår tilsynsmyndigheder, vil den foreslåede forordning pålægge medlemsstaterne at udpege nationale certificeringstilsynsmyndigheder, som er ansvarlige for tilsyn, overvågning og

---

17 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.

18 Europa-Parlamentets og Rådets direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF.

19 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).

20 Forordning (EF) nr. 765/2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93.

håndhævelse af reglerne. Disse organer vil forblive adskilt fra overensstemmelsesvurderingsorganer som foreskrevet i forordning (EF) nr. 765/2008.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Retsgrundlaget for EU's tiltag er artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), som omhandler tilnærmelse af medlemsstaternes love for at nå målene i artikel 26 TEUF, dvs. et velfungerende indre marked.

Retsgrundlaget for det indre marked om oprettelse af ENISA er blevet stadfæstet af Domstolen (i sag C-217/04 *Det Forenede Kongerige mod Europa-Parlamentet og Rådet*) og blev bekræftet ved forordningen fra 2013, som fastsatte Agenturets nuværende mandat. Herudover vil aktiviteter, som afspejler målene om øget samarbejde og koordinering mellem medlemsstaterne, og de aktiviteter, som tilfører EU-kapacitet til at supplere medlemsstaternes foranstaltninger, falde ind under kategorien "operationelt samarbejde". Dette er specifikt fastlagt i NIS-direktivet (for hvilket artikel 114 i TEUF er retsgrundlaget) som et mål, der bør nås i forbindelse med CSIRT-netværket, hvor "ENISA varetager sekretariatsopgaverne og støtter aktivt samarbejdet" (artikel 12, stk. 2). Navnlig artikel 12, stk. 3, litra f), beskriver nærmere udpegelsen af yderligere former for operationelt samarbejde som CSIRT-netværkets opgave, herunder for så vidt angår: i) kategorier af risici og hændelser, ii) tidlig varsling, iii) gensidig bistand og iv) principper og retningslinjer for koordination, når medlemsstaterne reagerer på grænseoverskridende risici og hændelser.

- Den nuværende fragmentering af certificeringsordningerne for IKT-produkter og -tjenester er også en følge af manglen på en fælles juridisk bindende og effektiv ramme, som gælder for medlemsstaterne. Det hindrer oprettelsen af et indre marked for IKT-produkter og -tjenester og hæmmer den europæiske industris konkurrenceevne i denne sektor. Det foreliggende forslag har til formål at afhjælpe den nuværende opsplitning og de dermed forbundne hindringer for det indre marked ved at skabe en fælles ramme for indførelsen af cybersikkerhedscertificeringsordninger, som gælder for hele EU.

Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)

Nærhedsprincippet indebærer en vurdering af nødvendigheden og merværdien af en indsats på EU-plan. Overholdelse af nærhedsprincippet på dette område blev allerede anerkendt i forbindelse med vedtagelsen af ENISA-forordningen[21].

Cybersikkerhed er et anliggende af fælles interesse i EU. Den gensidige afhængighed af net og informationssystemer er af en sådan art, at individuelle aktører (offentlige og private, herunder borgere) meget ofte ikke kan imødegå truslerne, styre risiciene og modvirke effekten af cyberhændelser på egen hånd. På den ene side gør den gensidige afhængighed mellem medlemsstaterne, herunder når det gælder driften af kritisk infrastruktur (energi, transport og vand for blot at nævne nogle få), at offentlig indgriben på EU-niveau ikke blot er gavnligt, men også påkrævet. På den anden side kan EU's intervention give en positiv "afsmittende"

[21] 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.

virkning, når der udveksles bedste praksis mellem medlemsstaterne, hvilket kan føre til en forbedret cybersikkerhed i EU.

Sammenfattende kan det siges, at en **forøgelse af Unionens kollektive cybermodstandsdygtighed** i den nuværende situation og med sigte på de fremtidige scenarier ikke vil kunne nås **gennem individuelle tiltag fra EU's medlemsstater og en fragmenteret tilgang til cybersikkerhed**.

Det anses også for nødvendigt med en indsats på EU-plan for at afhjælpe fragmenteringen af de nuværende cybersikkerhedscertificeringsordninger. Det vil give producenterne mulighed for at drage fuld nytte af det indre marked og betydelige besparelser med hensyn til prøvnings- og nydesignomkostninger. Selv om den nuværende Gruppe af Højtstående Embedsmænd vedrørende Informationssystemers Sikkerheds (SOG-IS) aftale om gensidig anerkendelse (MRA) har givet vigtige resultater i denne henseende, har den også vist, at der er væsentlige begrænsninger, som gør den uegnet til at tilvejebringe langsigtede bæredygtige løsninger, der kan udnytte det indre markeds potentiale fuldt ud.

Merværdien af en indsats på EU-plan, herunder navnlig for at styrke samarbejdet mellem medlemsstaterne, men også mellem net- og informationssikkerhedsfællesskaberne, blev anerkendt i Rådets konklusioner[22] fra 2016 og fremgår også klart af evalueringen af ENISA.

- **Proportionalitet**

De foreslåede foranstaltninger går ikke ud over, hvad der er nødvendigt for at nå de politiske mål. Derudover er omfanget af EU's indgriben ikke til hinder for yderligere nationale tiltag i forbindelse med nationale sikkerhedsanliggender. En EU-indsats er således berettiget på grundlag af nærhedsprincippet og proportionalitetsprincippet.

- **Valg af retsakt**

Det foreliggende forslag reviderer forordning (EU) nr. 526/2013, som fastsætter det nuværende mandat og opgaver for ENISA. Med tanke på ENISA's vigtige rolle ved indførelsen og forvaltningen af en europæisk ramme for cybersikkerhedscertificering bør det nye mandat og de nævnte rammebestemmelser fastlægges i et enkelt retligt instrument, nemlig en forordning.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

Efterfølgende evalueringer/kvalitetskontrol af gældende lovgivning

Kommissionen vurderede i overensstemmelse med evalueringskøreplanen[23] **relevans, virkning, effektivitet, omkostningseffektivitet, sammenhæng og EU-merværdi** af Agenturet med hensyn til dets præstationer, styring, intern organisatorisk struktur og arbejdsmetoder i perioden 2013-2016. De vigtigste resultater kan opsummeres som følger (yderligere oplysninger findes i arbejdsdokumentet fra Kommissionens tjenestegrene, som ledsager konsekvensanalysen).

[22] Rådets konklusioner om styrkelse af Europas modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri – 15. november 2016.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

- **Relevans:** I en kontekst med hurtig teknologiske udvikling og skiftende trusler og i betragtning af det betydelige behov for øget cybersikkerhed i EU har ENISA's mål vist sig at være relevante. Medlemsstaterne og EU's organer baserer sig faktisk på Agenturets betydelige ekspertise inden for cybersikkerhed. Der må desuden opbygges kapacitet i medlemsstaterne til bedre at forstå og imødegå trusler, og interessenterne må samarbejde på tværs af temaområder og institutioner. Cybersikkerhed er fortsat en central politisk prioritet for EU, hvor ENISA forventes at reagere, men ENISA's udformning som et EU-agentur med en tidsbegrænset mandatperiode: i) giver ikke mulighed for langsigtet planlægning og bæredygtig støtte til medlemsstaterne og EU-institutionerne, ii) kan føre til et juridisk tomrum, idet bestemmelserne i NIS-direktivet, som overdrager opgaver til ENISA, har en permanent karakter[24], iii) hænger ikke sammen med en vision, hvor ENISA indgår i et udvidet EU-cybersikkerhedsøkosystem.
- **Effektivitet**: ENISA har samlet set nået sine mål og løst sine opgaver. Det bidrog til at øge net- og informationssikkerheden i Europa via sine vigtigste aktiviteter (kapacitetsopbygning, tilrådighedsstillelse af ekspertise, fællesskabsopbygning og støtte til politikker). Der var dog potentiale for forbedringer i forhold til alle aktiviteter. Evalueringen konkluderede, at ENISA effektivt har skabt stærke og tillidsfulde forhold til nogle af interessenterne, herunder navnlig medlemsstaterne og CSIRT'erne. Indgreb inden for kapacitetsopbygning blev opfattet som effektive, navnlig i medlemsstater med få ressourcer. Stimulering af bredt samarbejde har været et af højdepunkterne, og interessenterne er enige om den positive rolle, som ENISA spiller for at bringe aktørerne sammen. ENISA havde dog svært ved at have en stor virkning på det store net- og informationssikkerhedsområde. Det skyldtes også, at der var forholdsvis begrænsede menneskelige og finansielle ressourcer til at dække et meget bredt mandat. Evalueringen konkluderede også, at ENISA delvist opfyldte målet om at yde ekspertise, hvilket hang sammen med problemer med at rekruttere eksperter (se også afsnittet om omkostningseffektivitet).
- **Omkostningseffektivitet**: Til trods for sit lille budget – blandt de laveste sammenlignet med andre EU-agenturer – formåede Agenturet at bidrage til specifikke målsætninger, og udnyttede generelt sine ressourcer på en omkostningseffektiv måde. Evalueringen konkluderede, at processerne generelt var effektive, og der var en klar afgrænsning af ansvar i organisationen, som førte til en god gennemførelse af arbejdet. En af de største udfordringer for Agenturets omkostningseffektivitet vedrører ENISA's vanskeligheder med at rekruttere og fastholde højt kvalificerede eksperter. Resultaterne viser, at dette kan forklares med en kombination af faktorer, herunder de generelle vanskeligheder i hele den offentlige sektor med at konkurrere med den private sektor, når det forsøges at ansætte højt specialiserede eksperter, den type kontrakter (tidsbegrænset), som Agenturet oftest kunne tilbyde, og ENISA's placering, som ikke anses for så attraktiv, f.eks. i forbindelse med ægtefællers mulighed for at finde arbejde. En placering fordelt mellem Athen og Heraklion medførte en ekstra koordineringsindsats og ekstra omkostninger, men flytningen til Athen i 2013 af den centrale operationelle afdeling øgede Agenturets operationelle omkostningseffektivitet.

[24] Der henvises til artikel 7, 9, 11, 12 og 19 i direktivet om sikkerhed for net- og informationssystemer (NIS-direktivet).

- **Sammenhæng**: ENISA's aktiviteter har generelt været i overensstemmelse med interessenternes politikker og aktiviteter på nationalt plan og på EU-plan, men der er behov for en mere koordineret tilgang til cybersikkerhed på EU-plan. Potentialet for samarbejde mellem ENISA og andre EU-organer er ikke blevet udnyttet fuldt ud. Udviklingen i EU's juridiske og politiske landskab gør, at det aktuelle mandat nu er mindre sammenhængende.
- **Merværdi for EU**: ENISA's merværdi ligger primært i Agenturets evne til at forbedre samarbejdet, hovedsageligt mellem medlemsstaterne, men også med beslægtede net- og informationssikkerhedsfælleskaber. Der findes ingen anden aktør på EU-plan, der støtter samarbejdet mellem det samme udsnit af interessenter på net- og informationssikkerhedsområdet. Agenturets merværdi var forskelligt, alt efter dets interessenters forskellige behov og ressourcer (f.eks. store i forhold til små medlemsstater, medlemsstater i forhold til erhvervslivet) og Agenturets behov for at prioritere sine aktiviteter i overensstemmelse med arbejdsprogrammet. Evalueringen konkluderede, at en mulig lukning af ENISA ville være en tabt mulighed for alle medlemsstater. Det ville ikke være muligt at sikre samme grad af fælleskabsopbygning og samarbejde på tværs af medlemsstaterne inden for cybersikkerhed. Uden et mere centraliseret EU-agentur ville der ske en større opsplitning, hvor bilateralt eller regionalt samarbejde opstår for at fylde det tomrum, som ENISA efterlader.

For så vidt angår ENISA's tidligere resultater og fremtiden, er de vigtigste tendenser fra høringen i 2017 følgende[25]:

- ENISA's samlede resultater i perioden 2013 til 2016 blev positivt bedømt af et flertal af de adspurgte (74 %). Et flertal af respondenterne mente endvidere, at ENISA når sine forskellige mål (mindst 63 % for hvert enkelt mål). ENISA's tjenester og produkter bruges regelmæssigt (en gang om måneden eller hyppigere) af næsten halvdelen af respondenterne (46 %), og de værdsættes for den omstændighed, at de stammer fra et EU-organ (83 %) og for deres kvalitet (62 %).
- Respondenterne pegede på en række lakuner og udfordringer for fremtidens cybersikkerhed i EU, hvoraf de vigtigste 5 (på en liste over 16) var: samarbejde på tværs af medlemsstaterne, kapacitet til at forebygge, opdage og finde løsninger på væsentlige cyberangreb, samarbejdet mellem medlemsstaterne i spørgsmål om cybersikkerhed, samarbejde og informationsudveksling mellem forskellige interessenter, herunder offentlig-private partnerskaber, beskyttelse af kritisk infrastruktur mod cyberangreb.
- Et stort flertal (88 %) af respondenterne mente, at de aktuelle instrumenter og mekanismer, der er til rådighed på EU-plan hertil, er utilstrækkelige eller kun delvis fyldestgørende. Et stort flertal af respondenterne (98 %) mente, at der var behov for

[25] 90 interessenter fra 19 medlemsstater svarede under høringen (88 besvarelser og 2 holdningsdokumenter), herunder nationale myndigheder fra 15 medlemsstater, herunder Frankrig, Italien, Irland og Grækenland, og 8 paraplyorganisationer, som repræsenterer et betydeligt antal europæiske organisationer, f.eks. European Banking Federation, Digital Europe (som repræsenterer den digitale teknologiindustri i Europa) og European Telecommunications Network Operators' Association (ETNO). Den offentlig høring om ENISA blev suppleret med en række andre kilder, herunder: i) dybtgående interview med ca. 50 centrale aktører i cybersikkerhedsfællesskabet, ii) rundspørge til CSIRT-netværket og iii) rundspørge til ENISA's bestyrelse, forretningsudvalget og den stående gruppe af interessenter.

et EU-organ til at tackle udfordringerne, og 99 % af respondenterne anså ENISA for at være den rette organisation hertil.

Høring af interesserede parter

- Kommissionen afholdt en offentlig høring om revisionen af ENISA mellem den 12. april og den 5. juli 2016 og modtog 421 svar[26]. Ifølge resultaterne udtrykte 67,5 % af respondenterne den mening, at ENISA kan spille en rolle ved fastlæggelse af en harmoniseret ramme for sikkerhedscertificering af IT-produkter og -tjenester.

Resultaterne fra høringen i 2016 om cybersikkerhed cPPP[27] om afsnittet om certificering viser:

- 50,4 % (dvs. 121 ud af 240) af de adspurgte vidste ikke, om nationale certificeringsordninger gensidigt anerkendes på tværs af EU-medlemsstaterne. 25,8 % (62 ud af 240) svarede "nej", medens 23,8 % (57 ud af 240) svarede "ja".
- 37,9 % af de adspurgte (91 ud af 240) mente, at de bestående certificeringsordninger ikke dækker det europæiske erhvervslivs behov. På den anden side gav 17,5 % (42 ud af 240) – hovedsageligt verdensomspændende virksomheder, som er aktive på EU-markedet – udtryk for den modsatte opfattelse.
- 49,6 % (119 ud af 240) af de adspurgte anførte, at det ikke er let at påvise ækvivalensen mellem standarder, certificeringsordninger og mærkning. 37,9 % (91 ud af 240) svarede "ved ikke", medens 12,5 % (30 ud af 240) svarede "ja".

Ekspertbistand

Kommissionen har benyttet sig af følgende eksterne ekspertbistand:

- Study on the Evaluation of ENISA (Rambøll/Carsa 2017, SMART no. 2016/0077)
- Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment (PriceWaterhouseCoopers 2017, SMART no. 2016/0029).

Konsekvensanalyse

- Konsekvensanalysen om dette initiativ konstaterede følgende væsentlige problemer, der skal løses:
- opsplitning af politikker og strategier for cybersikkerhed på tværs af medlemsstaterne
- spredte ressourcer og fragmentering af tilgange til cybersikkerhed på tværs af EU's institutioner, agenturer og organer og
- utilstrækkeligt kendskabs- og oplysningsniveau hos borgerne, i sammenhæng med den stigende forekomst af flere nationale og sektorielle certificeringsordninger.

[26] 162 bidrag fra borgere, 33 fra civilsamfundet og forbrugerorganisationerne, 186 fra erhvervslivet og 40 fra offentlige myndigheder, herunder de kompetente myndigheder, der håndhæver e-databeskyttelsesdirektivet.

[27] Der indkom 240 svar fra interessenter fra nationale offentlige myndigheder, store virksomheder, SMV'er, mikrovirksomheder og forskningsorganer.

I analysen vurderedes følgende mulige løsninger med hensyn til ENISA's mandat:

- opretholdelse af status quo, dvs. et udvidet, men stadig tidsbegrænset mandat (referencescenariet)
- udløb af ENISA's aktuelle mandat uden fornyelse og opløsning af ENISA (ingen politiske tiltag)
- et "reformeret" ENISA og
- et EU-agentur for cybersikkerhed med fuld operationel kapacitet.

I analysen vurderedes følgende mulige løsninger med hensyn til cybersikkerhedscertificering:

- ingen politiske tiltag (referencescenariet)
- ikkelovgivningsmæssige foranstaltninger ("blød lovgivning")
- en EU-retsakt med henblik på at oprette et obligatorisk system for alle medlemsstaterne baseret på SOG-IS-systemet og
- en generel EU-ramme for cybersikkerhedscertificering.

I analysen konkluderes det, at et "reformeret" ENISA i kombination med en generel EU-ramme for cybersikkerhedscertificering er den foretrukne løsning.

Den foretrukne løsningsmodel er vurderet som den mest effektive for EU til at nå de identificerede mål: øget cybersikkerhedskapacitet, beredskab, samarbejde, oplysning, gennemsigtighed og undgåelse af en opsplitning af markedet. Denne løsningsmodel er også vurderet til at være den, der hænger bedst sammen med de politiske prioriteter i EU's strategi for cybersikkerhed og de tilknyttede politikker (f.eks. NIS-direktivet) samt den digitale strategi for det indre marked. Herudover fremgik det af høringsprocessen, at den foretrukne løsning støttes af størstedelen af interessenterne. Konsekvensanalysen viste også, at den foretrukne løsning ville nå målene gennem en fornuftig brug af ressourcer.

Kommissionens Udvalg for Forskriftskontrol afgav oprindeligt en negativ udtalelse den 24. juli og derefter en positiv udtalelse den 25. august 2017 efter fornyet forelæggelse. Den ændrede konsekvensanalyse indeholder yderligere støttedokumentation, de endelige konklusioner af evalueringen af ENISA og yderligere forklaringer på de forskellige politiske løsningsmodeller og deres konsekvenser. Bilag I til den endelige rapport om konsekvensanalysen summerer, hvordan bestyrelsens bemærkninger i den anden udtalelse er blevet behandlet. Rapporten blev navnlig ajourført for at beskrive cybersikkerhedskonteksten i EU nærmere, herunder de foranstaltninger, der er indeholdt i den fælles meddelelse "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", (JOIN(2017) 450), og hvad der er særlig relevant for ENISA: EU's plan for cybersikkerhedssamarbejde og det europæiske ekspertisecenter for cybersikkerhedsforskning, som Agenturet vil sammenkæde sin rådgivning om EU's forskningsbehov med.

Rapporten forklarer, hvordan reformen af Agenturet, herunder de nye opgaver, bedre ansættelsesvilkår og strukturelt samarbejde med EU-organer på området, vil forbedre dets tiltrækningskraft som arbejdsgiver og bidrage med at løse problemerne i forbindelse med rekruttering af eksperter. Bilag 6 til rapporten indeholder også et revideret overslag over udgifterne, der er forbundet med de politiske løsningsmodeller for ENISA. Hvad angår certificering, er rapporten ændret for at give en mere detaljeret forklaring, herunder en grafisk præsentation af den foretrukne løsningsmodel, og for at give omkostningsoverslag for medlemsstaterne og Kommissionen vedrørende den nye certificeringsramme. Begrundelsen for valget af ENISA som den centrale aktør i rammen er yderligere forklaret med

udgangspunkt i Agenturets ekspertise på området og den omstændighed, at det er det eneste Agentur på EU-plan for cybersikkerhed. Endelig er afsnittene om certificering blevet gennemgået for at afklare visse aspekter vedrørende forskellen mellem det nuværende SOG-IS-system, fordelene ved de forskellige politiske løsningsmodeller og for at forklare den omstændighed, at typen af IKT-produkter og -tjenester omfattet af en europæisk certificeringsordning vil blive fastlagt i selve den godkendte ordning.

Målrettet regulering og forenkling

Ikke relevant

Indvirkning på de grundlæggende rettigheder

Cybersikkerhed spiller en afgørende rolle i forbindelse med beskyttelse af privatlivets fred og personoplysninger i overensstemmelse med artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder. Cyberhændelser er en klar trussel mod privatlivets fred og beskyttelse af vores personoplysninger. Cybersikkerhed er således en nødvendig forudsætning for overholdelse af privatlivets fred og fortroligheden af vores personoplysninger. Set i dette perspektiv udgør forslaget ved at styrke cybersikkerheden i EU et vigtigt supplement til den eksisterende lovgivning om beskyttelse af den grundlæggende ret til beskyttelse af privatlivets fred og personoplysninger. Cybersikkerhed er også afgørende for at beskytte fortroligheden af elektronisk kommunikation og dermed for udøvelsen af ytringsfriheden og adgangen til oplysninger samt andre beslægtede rettigheder såsom retten til tanke-, samvittigheds- og religionsfrihed.

4. VIRKNINGER FOR BUDGETTET

Se finansieringsoversigten

5. ANDRE FORHOLD

- **Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

Kommissionen vil overvåge anvendelsen af forordningen og forelægge en rapport om evalueringen for Europa-Parlamentet og Rådet og Det Europæiske Økonomiske og Sociale Udvalg hvert femte år. I disse rapporter, der vil blive offentliggjort, vil der blive gjort rede for, hvordan forordningen anvendes og håndhæves i praksis.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Forordningens afsnit I indeholder de generelle bestemmelser: genstand (artikel 1), definitioner (artikel 2), herunder henvisninger til relevante definitioner fra andre EU-retsakter såsom Europa-Parlamentets og Rådets direktiv 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet), Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 og Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 om standardisering.

Forordningens afsnit II indeholder de centrale bestemmelser vedrørende ENISA, EU's Agentur for Cybersikkerhed.

I kapitel I i dette afsnit skitseres Agenturets mandat (artikel 3), mål (artikel 4) og opgaver (artikel 5-11).

I kapitel II beskrives opbygningen af ENISA og de centrale bestemmelser vedrørende Agenturets struktur (artikel 12). Her er anført sammensætningen, afstemningsregler og funktioner for bestyrelsen (afdeling 1, artikel 13-17), forretningsudvalget (afdeling 2, artikel 18) og den administrerende direktør (afdeling 3, artikel 19). Det omfatter også bestemmelser om sammensætning og funktion af den Stående Gruppe af Interessenter (afdeling 4, artikel 20). Sidst men ikke mindst fastsættes i afdeling 5 i dette kapitel de nærmere operationelle bestemmelser for Agenturet, herunder i forbindelse med programmeringen af dets aktiviteter, interessekonflikter, gennemsigtighed, fortrolighed og adgang til dokumenter (artikel 21-25).

Kapitel III vedrører opstilling af og strukturen for Agenturets budget (artikel 26 og 27) samt regler for dets gennemførelse (artikel 28 og 29). Det omfatter også bestemmelser for at lette bekæmpelsen af svig, korruption og andre ulovlige handlinger (artikel 30).

Kapitel IV vedrører Agenturets personale. Det omfatter generelle bestemmelser om vedtægten og ansættelsesvilkårene og reglerne for privilegier og immuniteter (artikel 31 og 32). Det fastsætter også de nærmere regler for ansættelse og udnævnelse af Agenturets administrerende direktør (artikel 33). Sidst men ikke mindst omfatter det bestemmelser vedrørende brugen af udsendte nationale eksperter eller andre medarbejdere, som ikke er ansat af Agenturet (artikel 34).

Endelig indeholder kapitel V de generelle bestemmelser for Agenturet. Det beskriver Agenturets retlige status (artikel 35) og indeholder bestemmelser om ansvar, sprogordning, beskyttelse af personoplysninger (artikel 36-38) samt sikkerhedsreglerne for beskyttelse af klassificerede og følsomme ikkeklassificerede oplysninger (artikel 40). Det beskriver reglerne for Agenturets samarbejde med tredjelande og internationale organisationer (artikel 39). Sidst men ikke mindst omfatter det også bestemmelser om Agenturets hjemsted og driftsbetingelser samt administrativ kontrol udøvet af Ombudsmanden (artikel 41 og 42).

I forordningens afsnit III fastlægges den europæiske ramme for cybersikkerhedscertificering ("**rammen**") for IKT-produkter og -tjenester som *lex generalis* (artikel 1). Heri defineres det generelle formål med de europæiske cybersikkerhedscertificeringsordninger, nemlig at sikre, at IKT-produkter og -tjenester er i overensstemmelse med de fastlagte cybersikkerhedskrav for så vidt angår deres evne til, på et givet tillidsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne funktioner eller tjenester (artikel 43). Derudover anføres de sikkerhedsmål, som europæiske cybersikkerhedscertificeringsordninger skal søge at nå (artikel 45), bl.a. evnen til at beskytte data mod utilsigtet eller uautoriseret adgang eller videregivelse, ødelæggelse eller ændring, samt indholdet (dvs. elementerne) i de europæiske cybersikkerhedscertificeringsordninger, f.eks. den detaljerede beskrivelse af deres omfang, sikkerhedsmål, evalueringskriterier osv. (artikel 47).

I afsnit III fastsættes også de væsentligste retlige virkninger af de europæiske cybersikkerhedscertificeringsordninger, nemlig i) forpligtelsen til at gennemføre ordningen på nationalt plan og den frivillige karakter af certificering og ii) at de europæiske cybersikkerhedscertificeringsordninger gør nationale ordninger for de samme produkter eller tjenester ugyldige (artikel 48 og 49).

I dette afsnit fastsættes endvidere proceduren for vedtagelsen af europæiske cybersikkerhedscertificeringsordninger og Kommissionens, ENISA's og den europæiske cybersikkerhedscertificeringsgruppes ("gruppen") rolle (artikel 44). Endelig fastsættes i dette afsnit bestemmelser om overensstemmelsesvurderingsorganer, deres krav, beføjelser og opgaver, nationale tilsynsmyndigheder samt sanktioner.

Gruppen oprettes også i dette afsnit som et essentielt organ bestående af repræsentanter for nationale certificeringstilsynsmyndigheder, hvis vigtigste funktion er at samarbejde med ENISA ved udarbejdelsen af europæiske cybersikkerhedscertificeringsordninger og at rådgive Kommissionen om generelle eller specifikke problemstillinger vedrørende cybersikkerhedscertificeringspolitik.

Forordningens afsnit IV indeholder de afsluttende bestemmelser om udøvelsen af delegationen, evalueringskrav, ophævelse og afløsning samt ikrafttrædelse.

2017/0225 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ENISA, "EU's Agentur for Cybersikkerhed", om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi ("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[28],

under henvisning til udtalelse fra Regionsudvalget[29],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Net- og informationssystemer og telekommunikationsnet og -tjenester spiller en afgørende rolle i samfundet og har udviklet sig til rygraden i den økonomiske vækst. Informations- og kommunikationsteknologier er grundlaget for de komplekse systemer, som understøtter samfundets aktiviteter, og sørger for, at vore økonomier fungerer inden for vigtige sektorer såsom sundhed, energi, finans og transport, og understøtter navnlig det indre markeds funktion.

(2) Borgerne, erhvervslivet og myndighederne i EU 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 (IoT) forventes millioner eller endog milliarder styk forbundet digitalt udstyr at blive udbredt i hele EU 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 organisationer og individuelle brugere får utilstrækkelige oplysninger om IKT-produkters og -tjenesters cybersikkerhedsfunktioner, hvilket undergraver tilliden til digitale løsninger.

(3) Øget digitalisering og konnektivitet medfører øgede 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 denne risiko for

[28] EUT C […] af […], s. […].
[29] EUT C […] af […], s. […].

samfundet bør der træffes alle nødvendige foranstaltninger for at forbedre cybersikkerheden i EU, således at net- og informationssystemer, telekommunikationsnet, digitale produkter, tjenester og udstyr, der anvendes af borgerne, myndighederne og erhvervslivet – fra SMV'er til operatører af kritisk infrastruktur – er bedre beskyttet mod cybertrusler.

(4) 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 er grænseoverskridende, medens den politiske respons fra cybersikkerhedsmyndigheder og retshåndhævelsesbeføjelser hovedsageligt er et nationalt anliggende. Væsentlige cyberhændelser kunne afbryde leveringen af essentielle tjenester i hele EU. Dette kræver en effektiv indsats og krisestyring på EU-plan, der bygger på målrettede politikker og vidtrækkende instrumenter for europæisk solidaritet og gensidig bistand. Det er derfor 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.

(5) 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. Det omfatter behovet for yderligere at øge medlemsstaternes og virksomhedernes kapaciteter og beredskab samt at forbedre samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer. 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 væsentlige grænseoverskridende cyberhændelser og -kriser. Der er også behov for yderligere bestræbelser på at øge borgernes og virksomhedernes kendskab til cybersikkerhed. Herudover bør tilliden til det digitale indre marked forbedres yderligere ved at give gennemsigtige oplysninger om sikkerhedsniveauet af IKT-produkter og -tjenester. Det kan fremmes ved EU-certificering, der anvender fælles cybersikkerhedskrav og -evalueringskriterier på tværs af nationale markeder og sektorer.

(6) I 2004 vedtog Europa-Parlamentet og Rådet forordning (EF) nr. 460/2004[30] om oprettelse af ENISA med det formål at bidrage til målet om at sikre et højt net- og informationssikkerhedsniveau i Unionen og udvikle en net- og informationssikkerhedskultur til gavn for borgerne, forbrugerne, virksomhederne og de offentlige forvaltninger. I 2008 vedtog Europa-Parlamentet og Rådet forordning (EF) nr. 1007/2008[31] om forlængelse af Agenturets mandat frem til marts 2012. Ved forordning (EU) nr. 580/2011[32] forlængedes Agenturets mandat frem til den 13. september 2013. I 2013 vedtog Europa-Parlamentet og Rådet forordning (EU) nr.

---

30 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).

31 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).

32 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).

526/2013[33] om ENISA og om ophævelse af forordning (EF) nr. 460/2004, som forlængede Agenturets mandat frem til juni 2020.

(7) Unionen har gjort en stor indsats for at sikre cybersikkerheden og øge tilliden til de digitale teknologier. I 2013 blev EU's strategi for cybersikkerhed vedtaget for at vejlede Unionens politiske reaktion på cybersikkerhedstrusler og -risici. Som led i indsatsen for at beskytte EU's borgere bedre online vedtog Unionen i 2016 den første retsakt inden for cybersikkerhed, nemlig direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet). Ved NIS-direktivet blev der indført krav om nationale kapaciteter på cybersikkerhedsområdet, de første mekanismer til bedre strategisk og operationelt samarbejde mellem medlemsstaterne blev indført, og der blev indført forpligtelser vedrørende sikkerhedsforanstaltninger og anmeldelse af hændelser i sektorer af afgørende betydning for økonomien og samfundet såsom energi, transport, vand, bankvirksomhed, finansmarkedsinfrastrukturer, sundhed og digital infrastruktur samt for udbydere af digitale tjenester (dvs. søgemaskiner, cloud computing-tjenester og onlinemarkedspladser). ENISA fik tildelt en central rolle som støtte for gennemførelsen af dette direktiv. Hertil kommer, at den effektive bekæmpelse af cyberkriminalitet er en vigtig prioritet på den europæiske dagsorden om sikkerhed og bidrager til det overordnede mål om at nå et højere niveau af cybersikkerhed.

(8) Det anerkendes, at den overordnede politiske kontekst siden vedtagelsen af EU's strategi for cybersikkerhed i 2013 og den seneste revision af Agenturets mandat har ændret sig væsentligt, også i forbindelse med et mere usikkert og mindre sikkert globalt miljø. I denne sammenhæng og inden for rammerne af EU's nye cybersikkerhedspolitik er det nødvendigt at gennemgå ENISA's mandat for at fastlægge Agenturets rolle i det forandrede cybersikkerhedsøkosystem og for at sikre, at det bidrager effektivt til Unionens reaktioner på de cybersikkerhedsudfordringer, der opstår som følge af dette radikalt ændrede trusselsbillede, hvilket Agenturets aktuelle mandat ikke er tilstrækkeligt til, som det også blev anerkendt i evalueringen af Agenturet.

(9) Agenturet, som oprettet ved nærværende forordning, bør afløse ENISA som oprettet ved forordning (EU) nr. 526/2013. Agenturet bør udføre de opgaver, det pålægges i kraft af nærværende forordning og EU-retsakter inden for cybersikkerhedsområdet, bl.a. ved at levere ekspertise og rådgivning og fungere som et center for information og viden i EU. Det bør fremme udveksling af bedste praksis mellem medlemsstaterne og private interessenter, forelægge politiske initiativer for EU-Kommissionen og medlemsstaterne, agere som et referencepunkt for EU's sektorielle politiske initiativer med hensyn til cybersikkerhed, fremme det operationelle samarbejde mellem medlemsstaterne og mellem medlemsstaterne og EU's institutioner, agenturer og organer.

(10) Inden for rammerne af afgørelse 2004/97/EF, Euratom, vedtaget på Det Europæiske Råds møde den 13. december 2003, besluttede repræsentanterne for medlemsstaterne, at ENISA skulle have sit sæde i en by i Grækenland, som skulle fastlægges nærmere af den græske regering. Agenturets værtsmedlemsstat bør sikre de bedst mulige betingelser for, at Agenturet kan fungere problemfrit og effektivt. For at Agenturet

[33] 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).

korrekt og effektivt kan udføre sine opgaver og rekruttere og fastholde personale samt øge effektiviteten af netværksaktiviteter, er det afgørende, at Agenturet er placeret på et passende sted, hvor der bl.a. er passende transportforbindelser og faciliteter for ægtefæller og børn, som følger med Agenturets personale. De nødvendige foranstaltninger bør fastlægges i en aftale, som efter godkendelse af Agenturets bestyrelse indgås mellem Agenturet og værtsmedlemsstaten.

(11) I betragtning af de tiltagende udfordringer på cybersikkerhedsområdet, som Unionen står over for, bør de finansielle og menneskelige ressourcer, der er tildelt Agenturet, forøges i overensstemmelse med dets udvidede rolle og opgaver og dets afgørende stilling, når det gælder forsvaret af det europæiske digitale økosystem.

(12) Agenturet 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 informationer, det videregiver, samt i kraft af den åbenhed, der er forbundet med dets procedurer og drift, og dets omhu ved udførelsen af sine opgaver. Agenturet bør proaktivt bidrage til medlemsstaternes og Unionens indsats og udføre sine opgaver i fuldt samarbejde med Unionens institutioner, organer, kontorer og agenturer og medlemsstaterne. Herudover bør Agenturet bygge på bidrag fra og samarbejde med den private sektor og andre relevante interessenter. Som grundlag for, hvordan Agenturet skal nå sine mål, bør der fastlægges et sæt opgaver, der samtidig giver Agenturet fleksibilitet i dets aktiviteter.

(13) Agenturet bør bistå Kommissionen ved at levere rådgivning, udtalelser og analyser om alle EU-spørgsmål vedrørende udvikling af politik og lovgivning samt ajourføring og revision på cybersikkerhedsområdet, herunder beskyttelse af kritisk informationsinfrastruktur og cybermodstandsdygtighed. Agenturet bør fungere som et referencepunkt for rådgivning og ekspertise for de sektorspecifikke politikker og lovgivningsinitiativer i tilfælde, hvor cybersikkerhed er involveret.

(14) Agenturets grundlæggende opgave er at fremme en konsekvent gennemførelse af den relevante retlige ramme, herunder navnlig en effektiv gennemførelse af NIS-direktivet, som er afgørende for at øge cybermodstandsdygtigheden. På baggrund af det hurtigt skiftende cybersikkerhedstrusselsbillede står det klart, at medlemsstaterne må støttes med en mere overgribende tværpolitisk tilgang til opbygningen af cybermodstandsdygtighed.

(15) Agenturet bør bistå medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer med at opbygge og forbedre deres kapacitet og beredskab med sigte på at forebygge, opdage og imødegå cybersikkerhedsproblemer og -hændelser og i forbindelse med sikkerheden af net- og informationssystemer. Agenturet bør især støtte udvikling og forbedring af nationale CSIRT'er for at nå et højt fælles niveau af deres modenhed i Unionen. Agenturet bør også bistå med udviklingen og ajourføringen af Unionens og medlemsstaternes strategier for net- og informationssystemers sikkerhed, herunder navnlig cybersikkerhed, fremme deres udbredelse og følge op på deres gennemførelse. Agenturet bør også tilbyde uddannelse og uddannelsesmateriale til offentlige organer og i givet fald "uddanne underviserne" med sigte på at bistå medlemsstaterne med at udvikle deres egne uddannelseskapaciteter.

(16) Agenturet bør bistå den samarbejdsgruppe, der nedsættes ved NIS-direktivet, med udførelsen af dens opgaver, navnlig ved at levere ekspertise og rådgivning og fremme udvekslingen af bedste praksis vedrørende risici og hændelser, især med hensyn til

medlemsstaternes identificering af operatører af væsentlige tjenester, herunder i forbindelse med grænseoverskridende afhængighed.

(17) 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 kritisk infrastruktur bør Agenturet fremme etableringen af centre for informationsudveksling og analyse (ISAC'er) ved at stille bedste praksis og vejledning om tilgængelige værktøjer og procedurer til rådighed samt ved at vejlede om håndtering af lovgivningsmæssige spørgsmål relateret til informationsudveksling.

(18) Agenturet bør samle og analysere de nationale rapporter fra CSIRT'er og CERT-EU og indføre fælles regler, sprog og terminologi med henblik på udveksling af oplysninger. Agenturet bør også inddrage den private sektor inden for rammerne af NIS-direktivet, som fastsatte grundlaget for frivillig teknisk informationsudveksling på det operationelle plan med oprettelsen af CSIRT-netværket.

(19) Agenturet bør bidrage til en respons på EU-niveau i tilfælde af væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser. Denne funktion bør omfatte indsamling af relevante oplysninger og etablering af kontakt mellem CSIRT-netværket og tekniske kredse samt de beslutningstagere, der er ansvarlige for krisestyringen. Derudover kunne Agenturet støtte 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. Agenturet bør støtte processen ved at afprøve metoderne for et sådant samarbejde gennem årlige cybersikkerhedsøvelser.

(20) For at løse sine operationelle opgaver bør Agenturet gøre brug af den tilgængelige ekspertise hos CERT-EU gennem et struktureret samarbejde i tæt fysisk nærhed. Det strukturerede samarbejde vil fremme de nødvendige synergier og opbygningen af ENISA's ekspertise. Hvor det er relevant, bør der indgås specifikke aftaler mellem de to organisationer med henblik på at fastlægge den praktiske gennemførelse af et sådant samarbejde.

(21) I overensstemmelse med sine operationelle opgaver bør Agenturet være i stand til at yde støtte til medlemsstaterne, f.eks. i form at rådgivning eller teknisk bistand, eller ved at sikre analyse af trusler og hændelser. Kommissionens henstilling om en koordineret reaktion på væsentlige cyberhændelser og -kriser anbefaler, at medlemsstaterne samarbejder i god tro og hurtigst muligt udveksler oplysninger med hinanden og med ENISA om væsentlige cybersikkerhedshændelser og -kriser. Sådanne oplysninger burde hjælpe ENISA med at udføre sine operationelle opgaver.

(22) Som led i det regelmæssige samarbejde på teknisk niveau til støtte for Unionens situationsbevidsthed bør Agenturet regelmæssigt udarbejde en teknisk EU-cybersikkerhedsrapport om hændelser og trusler, der skal være baseret på offentligt tilgængelige oplysninger, Agenturets egen analyse og rapporter tilsendt af medlemsstaternes CSIRT'er (på frivillig basis) eller NIS-direktivets centrale kontaktpunkter, Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol og CERT-EU samt, hvor det er relevant, Den Europæiske Unions Efterretningsanalysecenter (INTCEN) ved Tjenesten for EU's Optræden Udadtil (EU-Udenrigstjenesten). Rapporten bør stilles til rådighed for de relevante instanser i Rådet, Kommissionen, Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik og CSIRT-netværket.

(23) Tekniske efterfølgende undersøgelser af hændelser med betydelig virkning i mere end én medlemsstat, som understøttes eller udføres af Agenturet efter anmodning fra den pågældende medlemsstat eller med dennes samtykke bør fokusere på forebyggelse af fremtidige hændelser og udføres uden at foregribe eventuelle retlige eller administrative procedurer med henblik på at placere skyld eller ansvar.

(24) De berørte medlemsstater bør give Agenturet de nødvendige oplysninger og den nødvendige bistand med henblik på undersøgelsen uden at det berører artikel 346 i traktaten om Den Europæiske Unions funktionsmåde eller hensyn til den offentlige orden.

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

(26) For bedre at forstå udfordringerne inden for cybersikkerhed og med sigte på at levere strategisk langsigtet rådgivning til medlemsstaterne og EU-institutionerne er Agenturet nødt til at analysere både bestående og nye risici. Med dette mål for øje bør Agenturet i samarbejde med medlemsstaterne og, hvis relevant, statistiske kontorer og andre organer indsamle relevante oplysninger og udføre analyser af nye teknologier og tilvejebringe emnespecifikke vurderinger af de forventede sociale, retlige, økonomiske og lovgivningsmæssige konsekvenser af teknologiske innovationer inden for net- og informationssikkerhed, herunder navnlig cybersikkerhed. Agenturet bør desuden bistå medlemsstaterne og Unionens institutioner, agenturer og organer med at identificere nye tendenser og forebygge problemer på cybersikkerhedsområdet ved at udføre analyser af trusler og hændelser.

(27) Med henblik på at øge Unionens modstandsdygtighed bør Agenturet udvikle ekspertise vedrørende sikring af internettets infrastruktur og kritisk infrastruktur ved at stille rådgivning, vejledning og bedste praksis til rådighed. Med sigte på at give lettere adgang til bedre strukturerede oplysninger om cybersikkerhedsrisici og potentielle løsninger bør Agenturet udvikle og opretholde Unionens "informationsknudepunkt", en one-stop-shop-portal, som giver offentligheden adgang til oplysninger om cybersikkerhed, der kommer fra EU's og de enkelte landes institutioner, agenturer og organer.

(28) Agenturet bør bidrage til at bevidstgøre offentligheden om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere og organisationer. Agenturet bør også bidrage til at fremme bedste praksis og løsninger på enkeltpersons- og organisationsniveauet ved at indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og ved at sammenstille rapporter med henblik på at yde vejledning til virksomheder og borgere samt forbedre det generelle niveau af beredskab og modstandsdygtighed. Agenturet bør herudover i samarbejde med medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer tilrettelægge jævnlige informations- og oplysningskampagner for slutbrugere med sigte på at fremme en mere sikker individuel adfærd på nettet og øge bevidstheden om de potentielle farer på Internettet, herunder cyberkriminalitet, såsom phishing-angreb, botnet, økonomisk svig og banksvindel, samt fremme af grundlæggende autentificerings- og databeskyttelsesrådgivning. Agenturet bør spille en central rolle i bestræbelserne på at højne slutbrugernes oplysningsniveau om udstyrs sikkerhed.

(29) For at støtte de virksomheder, der er aktive i cybersikkerhedssektoren samt brugerne af cybersikkerhedsløsninger bør Agenturet 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.

(30) For at sikre, at det når sine mål fuldt ud, bør Agenturet etablere kontakt med de relevante institutioner, agenturer og organer, herunder CERT-EU, Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol, Det Europæiske Forsvarsagentur (EDA), Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-Systemer (eu-LISA), Det Europæiske Luftfartssikkerhedsagentur (EASA) og ethvert andet EU-agentur, der er involveret i cybersikkerhed. Det bør også samarbejde med myndigheder med ansvar for databeskyttelse for at udveksle knowhow og bedste praksis og yde rådgivning om cybersikkerhedsaspekter, der kan have betydning for deres arbejde. Repræsentanter for de retshåndhævende myndigheder på nationalt og EU-plan og myndigheder, der har ansvar for databeskyttelse, bør kunne være repræsenteret i Agenturets stående gruppe af interessenter. I sine kontakter med retshåndhævende myndigheder vedrørende aspekter af net- og informationssikkerhed, der kan have indflydelse på disse myndigheders arbejde, bør Agenturet respektere de eksisterende informationskanaler og etablerede netværk.

(31) Agenturet bør som medlem, der også fungerer som CSIRT-netværkets sekretariat, støtte medlemsstaternes CSIRT'er og CERT-EU i det operationelle samarbejde oven i alle CSIRT-netværkets relevante opgaver som defineret i NIS-direktivet. Agenturet 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 CERT'er, under behørig hensyntagen til CSIRT-netværkets standardprocedurer.

(32) Med henblik på at øge EU's beredskab, når det gælder om at reagere på cybersikkerhedshændelser, bør Agenturet tilrettelægge årlige cybersikkerhedsøvelser på EU-niveau og efter anmodning støtte medlemsstaterne og EU's institutioner, agenturer og organer i at tilrettelægge øvelser.

(33) Agenturet bør videreudvikle og opretholde sin ekspertise inden for cybersikkerhedscertificering med sigte på at understøtte EU's politik på dette område. Agenturet bør fremme udbredelsen af cybersikkerhedscertificering i Unionen, herunder ved at bidrage til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau, for at øge gennemsigtigheden af IKT-produkters og -tjenesters cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked.

(34) Effektive cybersikkerhedsstrategier bør baseres på velgennemtænkte risikovurderingsmetoder, både i den offentlige og den private sektor. Der anvendes risikovurderingsmetoder på forskellige niveauer, men der er ingen fælles praksis for, hvordan de anvendes effektivt. Ved at udvikle og fremme bedste praksis for risikovurdering og interoperable risikostyringsløsninger i den offentlige og den private sektors organisationer kan cybersikkerhedsniveauet i Unionen forbedres. Til dette formål bør agenturet 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.

(35) Agenturet bør tilskynde medlemsstaterne og tjenesteudbydere til at hæve deres generelle sikkerhedsstandarder, så alle internetbrugere kan tage de nødvendige skridt til at sikre deres egen personlige cybersikkerhed. Navnlig bør tjenesteudbydere og produktproducenter tilbagekalde eller genbruge produkter og tjenester, som ikke overholder cybersikkerhedsstandarderne. I samarbejde med de kompetente myndigheder kan ENISA formidle oplysninger om cybersikkerhedsniveauet for produkter og tjenester, som udbydes i det indre marked, og udstede advarsler til udbydere og producenter og pålægge dem at forbedre sikkerheden, herunder cybersikkerheden, af deres produkter og tjenester.

(36) Agenturet bør tage fuldt hensyn til igangværende forsknings-, udviklings- og teknologivurderingsaktiviteter, navnlig aktiviteter, der gennemføres som led i de forskellige EU-forskningsinitiativer, for at rådgive Unionen og, hvor det er relevant, medlemsstaterne, hvis de anmoder herom, om forskningsbehov inden for net- og informationssikkerhed, herunder navnlig cybersikkerhed.

(37) Cybersikkerhedsproblemer er af global karakter. Der er behov for et tættere internationalt samarbejde for at forbedre cybersikkerhedsstandarderne, herunder definitionen af fælles adfærdsnormer, og informationsudveksling, hvilket vil fremme hurtigere internationalt samarbejde om samt en fælles global tilgang til net- og informationssikkerhedsspørgsmål. Agenturet bør derfor støtte et fortsat 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.

(38) Agenturet bør være i stand til at reagere på ad hoc-anmodninger om rådgivning og bistand fra medlemsstaterne og EU's institutioner, agenturer og organer, som er omfattet af Agenturets mål.

(39) Det er nødvendigt at gennemføre visse principper om Agenturets forvaltning for at overholde den fælles erklæring og fælles tilgang, som den interinstitutionelle arbejdsgruppe om EU's decentrale agenturer nåede til enighed om i juli 2012, og som har til formål at strømline agenturernes aktiviteter og forbedre deres resultater. Den fælles erklæring og fælles tilgang bør, alt efter hvad der er relevant, også afspejles i Agenturets arbejdsprogrammer, evalueringer og rapporterings- og administrationspraksis.

(40) For at sikre, at Agenturet fungerer effektivt, bør medlemsstaterne og Kommissionen være repræsenteret i bestyrelsen, som bør fastlægge de overordnede retningslinjer for Agenturets 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 dets gennemførelse, vedtage passende finansielle bestemmelser, fastlægge transparente arbejdsprocedurer for Agenturets beslutningstagning, vedtage Agenturets samlede programmeringsdokument, vedtage sin egen forretningsorden, udnævne den administrerende direktør og træffe afgørelse om at forlænge den administrerende direktørs mandatperiode eller bringe den til ophør.

(41) For at Agenturet kan fungere korrekt, bør Kommissionen og medlemsstaterne sikre, at personer, der udpeges til bestyrelsen, har en hensigtsmæssig faglig ekspertise og erfaring inden for de relevante områder. 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.

(42) Et velfungerende Agentur 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, og at den administrerende direktørs opgaver udføres i fuld uafhængighed. Den administrerende direktør bør efter høring af Kommissionen udarbejde et forslag til Agenturets arbejdsprogram og træffe alle nødvendige foranstaltninger til at sikre, at Agenturets arbejdsprogram gennemføres korrekt. Den administrerende direktør bør hvert år udarbejde en årsberetning, der skal forelægges for bestyrelsen, udfærdige et udkast til overslag over Agenturets indtægter og udgifter samt gennemføre budgettet. Den administrerende direktør bør endvidere kunne nedsætte ad hoc-arbejdsgrupper til at behandle specifikke spørgsmål, særlig af videnskabelig, teknisk, retlig eller samfundsøkonomisk art. Den administrerende direktør bør sikre, at medlemmerne af ad hoc-arbejdsgrupperne udvælges på grundlag af den højeste ekspertisestandard, og tage skridt til at sikre en passende repræsentativ balance, afhængigt af de specifikke spørgsmål, mellem medlemsstaternes offentlige forvaltninger, EU-institutionerne og den private sektor, herunder erhvervslivet, brugerne og akademiske eksperter i net- og informationssikkerhed.

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

(44) Agenturet bør have en stående gruppe af interessenter som et rådgivende organ, der kan sikre en løbende dialog med den private sektor, forbrugerorganisationerne og andre relevante interessenter. Den stående gruppe af interessenter, der nedsættes af bestyrelsen på forslag af den administrerende direktør, bør koncentrere sig om spørgsmål, der er relevante for interessenter, og forelægge dem for Agenturet. Sammensætningen af den stående gruppe af interessenter og de opgaver, som denne gruppe har, herunder navnlig at blive hørt i forbindelse med udkastet til arbejdsprogrammet, burde sikre en tilstrækkelig repræsentation af interessenter i Agenturets arbejde.

(45) Bestyrelsen bør vedtage regler for forebyggelse og håndtering af interessekonflikter. Agenturet bør også følge de relevante EU-bestemmelser om aktindsigt som fastlagt i Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001[34]. Agenturets behandling af personoplysninger bør være i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger[35]. Agenturet bør overholde de bestemmelser, der gælder for EU-institutionerne samt national lovgivning vedrørende behandling af oplysninger, herunder navnlig følsomme ikkeklassificerede oplysninger og EU-klassificerede oplysninger.

(46) For at Agenturet kan sikres fuld selvstændighed og uafhængighed og for at sætte det i stand til at udføre supplerende og nye opgaver, herunder uforudsete hasteopgaver, bør Agenturet råde over et tilstrækkeligt og selvstændigt budget, hvis indtægter

---

[34] 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).

[35] EFT L 8 af 12.1.2001, s. 1.

hovedsageligt kommer fra et bidrag fra Unionen og bidrag fra tredjelande, der deltager i Agenturets arbejde. Størstedelen af Agenturets ansatte bør være direkte involveret i den operationelle gennemførelse af Agenturets mandat. Værtsmedlemsstaten og enhver anden medlemsstat bør kunne yde frivillige bidrag til Agenturets indtægter. Unionens budgetprocedure bør finde anvendelse på ethvert bidrag, som kommer fra Unionens almindelige budget. Desuden bør revisionen af Agenturets regnskaber forestås af Revisionsretten for at sikre gennemsigtighed og ansvarlighed.

(47) Overensstemmelsesvurdering er den proces, hvorved det fastslås, om nærmere bestemte krav til et produkt, en proces, en tjeneste, et system, en person eller et organ er opfyldt. I forbindelse med denne forordning bør certificering betragtes som en form for overensstemmelsesvurdering for så vidt angår cybersikkerhedsegenskaberne for et produkt, en proces, en tjeneste, et system eller en kombination af disse ("IKT-produkter og -tjenester"), der foretages af en uafhængig tredjepart, som ikke er produktproducenten eller tjenesteudbyderen. Certificering kan ikke i sig selv garantere, at certificerede IKT-produkter og -tjenester er cybersikre. Det er snarere en procedure og en teknisk metode til at attestere, at IKT-produkter og -tjenester er blevet prøvet og at de opfylder visse krav til cybersikkerhed, som er fastsat andetsteds, f.eks. i tekniske standarder.

(48) Cybersikkerhedscertificering spiller en vigtig rolle for at øge tilliden til og sikkerheden af IKT-produkter og -tjenester. Det digitale indre marked og navnlig dataøkonomien og tingenes Internet kan kun trives, hvis offentligheden generelt har tillid til, at sådanne produkter og tjenester har et vist cybersikkerhedstillidsniveau. Netforbundne og selvkørende biler, elektronisk medicinsk udstyr, industrielle automatiseringskontrolsystemer eller intelligente forsyningsnet er kun nogle eksempler på sektorer, hvor certificering allerede bruges i vidt omfang eller snart vil blive brugt. De sektorer, der reguleres af NIS-direktivet, er også sektorer, hvor cybersikkerhedscertificering er afgørende.

(49) I meddelelsen fra 2016 "Styrkelse af Europas modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri", beskrev Kommissionen nødvendigheden af cybersikkerhedsprodukter, som er af høj kvalitet, prismæssigt overkommelige og interoperable. Udbuddet af IKT- produkter og tjenester i det indre marked er fortsat meget opsplittet 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. På den ene side gør dette det vanskeligt for europæiske virksomheder at konkurrere på nationalt, europæisk og globalt plan. På den anden side begrænser det udbuddet af levedygtige og brugbare cybersikkerhedsteknologier, som enkeltpersoner og virksomheder har adgang til. Ligeledes fremhævede Kommissionen i midtvejsevalueringen om gennemførelsen af strategien for det digitale indre marked behovet for sikre netforbundne produkter og systemer og anførte, at indførelsen af en europæisk IKT-sikkerhedsramme, der fastsætter regler for IKT-sikkerhedscertificering i Unionen, både ville kunne bevare tilliden til Internettet og gøre noget ved den nuværende fragmentering af cybersikkerhedsmarkedet.

(50) I øjeblikket anvendes cybersikkerhedscertificering af IKT-produkter og -tjenester kun i begrænset omfang. Hvis den findes, er det som regel på medlemsstatsniveau eller inden for rammerne af en brancheordning. En attest udstedt af en national cybersikkerhedsmyndighed anerkendes i princippet ikke i andre medlemsstater.

Virksomhederne kan således være nødt til at certificere deres produkter og tjenester i flere medlemsstater, hvor de driver virksomhed, f.eks. hvis de vil deltage i nationale offentlige udbud. 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 bestående ordninger har væsentlige mangler og forskelle med hensyn til produktdækning, tillidsniveau, materielle kriterier og den faktiske udnyttelse.

(51) Der er tidligere taget tilløb til at få indført gensidig anerkendelse af attester i Europa. 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 af sikkerhedscertificering, har SOG-IS' MRA nogle væsentlige mangler i form af høje omkostninger og begrænset anvendelsesområde. Indtil videre er der kun udviklet nogle få beskyttelsesprofiler for digitale produkter såsom digital underskrift, digital tachograf og smartkort. Vigtigst er dog, at SOG-IS kun omfatter en del af Unionens medlemsstater. I forhold til det indre marked gør det, at SOG-IS' MRA kun er begrænset effektiv.

(52) På denne baggrund er det nødvendigt at 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 attester for IKT-produkter og -tjenester i alle medlemsstater. Den europæiske ramme har et dobbelt formål: På den ene side bør den bidrage til at øge tilliden til IKT-produkter og -tjenester, der er certificeret i henhold til sådanne ordninger. På den anden side bør den hindre udbredelsen af modstridende eller overlappende nationale cybersikkerhedscertificeringer og dermed mindske omkostningerne for virksomheder, der opererer på det digitale indre marked. Ordningerne bør være ikke-diskriminerende og baseret på internationale eller europæiske standarder, medmindre sådanne standarder er ineffektive eller uhensigtsmæssige til at opfylde EU's legitime mål i denne henseende.

(53) Kommissionen bør have beføjelse til at vedtage europæiske cybersikkerhedscertificeringsordninger for specifikke grupper af IKT-produkter og -tjenester. Ordningerne bør gennemføres og overvåges af nationale certificeringstilsynsmyndigheder, 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 forordningen. Sådanne organer kan dog foreslå Kommissionen at betragte sådanne ordninger som grundlaget for at godkende dem som en europæisk ordning.

(54) Bestemmelserne i denne forordning bør ikke berøre EU-lovgivning om specifikke regler for certificering af IKT-produkter og -tjenester. Navnlig den generelle forordning om databeskyttelse fastsætter bestemmelser om indførelse af certificeringsordninger og databeskyttelsesmærkninger med sigte på at demonstrere, at dataansvarliges og databehandleres databehandlingsoperationer er i overensstemmelse med forordningen. Sådanne certificeringsordninger og databeskyttelsesmærkninger bør give de registrerede mulighed for hurtigt at vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester. Nærværende forordning berører ikke certificeringen af databehandlingsoperationer, herunder hvis sådanne operationer er indeholdt i produkter og tjenester, som foretages i henhold til den generelle forordning om databeskyttelse.

(55) Målet med europæiske cybersikkerhedscertificeringsordninger er at sikre, at de IKT-produkter og -tjenester, der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastsatte krav. Kravene vedrører evnen til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, processer, tjenester og systemer i denne forordnings betydning. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-produkter og -tjenester i denne forordning. IKT-produkter og -tjenester og de tilhørende cybersikkerhedsbehov er så forskellige, at det er meget vanskeligt at komme med generelle cybersikkerhedskrav, der gælder for alting. Det er således nødvendigt at have en bred og generel opfattelse af cybersikkerhed med henblik på certificering, som suppleres af en række specifikke cybersikkerhedsmål, som skal tages i betragtning ved udformningen af europæiske cybersikkerhedscertificeringsordninger. De metoder, der skal anvendes til at nå disse mål for specifikke IKT-produkter og -tjenester bør så præciseres yderligere i den enkelte certificeringsordning, der vedtages af Kommissionen, f.eks. i form af henvisninger til standarder eller tekniske specifikationer.

(56) Kommissionen bør have beføjelse til at anmode ENISA om at udarbejde forslag til ordninger for specifikke IKT-produkter eller -tjenester. Kommissionen bør på grundlag af den af ENISA foreslåede ordning have beføjelse til at vedtage den europæiske cybersikkerhedscertificeringsordning ved hjælp af gennemførelsesretsakter. Under hensyntagen til de generelle formål og 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. Det bør bl.a. omfatte cybersikkerhedscertificeringens omfang og genstand, herunder de omfattede kategorier af IKT-produkter og -tjenester, nærmere specifikation af cybersikkerhedskravene, f.eks. med henvisning til standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder og det påtænkte tillidsniveau (dvs. grundlæggende, betydeligt eller højt).

(57) At få foretaget en europæisk cybersikkerhedscertificering bør fortsat være frivilligt, medmindre andet er fastsat i EU-lovgivningen eller den nationale lovgivning. Med sigte på at nå denne forordnings mål og undgå fragmentering af det indre marked bør nationale cybersikkerhedscertificeringsordninger eller -procedurer for IKT-produkter og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, dog ophøre med at have virkning fra det tidspunkt, der fastsættes af Kommissionen i gennemførelsesretsakten. Medlemsstaterne bør desuden ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der allerede er omfattet af en bestående europæisk cybersikkerhedscertificeringsordning.

(58) Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenterne af IKT-produkter og udbydere af IKT-tjenester indgive en ansøgning om certificering af deres produkter eller tjenester til et overensstemmelsesvurderingsorgan efter eget valg. Overensstemmelsesvurderingsorganer bør akkrediteres af et akkrediteringsorgan, hvis de opfylder visse nærmere fastsatte krav i denne forordning. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt overensstemmelsesvurderingsorganet opfylder kravene. Akkrediteringsorganer tilbagekalder akkrediteringen af et overensstemmelsesvurderingsorgan, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis

foranstaltninger truffet af et overensstemmelsesvurderingsorgan er i modstrid med denne forordning.

(59) Det er nødvendigt at pålægge alle medlemsstater at udpege en tilsynsmyndighed for cybercertificering, som skal føre tilsyn med overensstemmelsesvurderingsorganernes overholdelse af reglerne og med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, samt overholdelse af kravene i denne forordning og de relevante cybersikkerhedscertificeringsordninger. Nationale certificeringstilsynsmyndigheder bør behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist. Herudover samarbejder de med andre certificeringstilsynsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings krav eller specifikke cybersikkerhedscertificeringsordninger.

(60) Med henblik på at sikre en ensartet anvendelse af den europæiske ramme for cybersikkerhedscertificering bør der oprettes en europæisk cybersikkerhedscertificeringsgruppe ("gruppen"), som består af medlemsstaternes nationale certificeringstilsynsmyndigheder. Gruppens vigtigste opgaver bør være at rådgive og bistå Kommissionens i dens arbejde med at sikre en konsekvent gennemførelse og anvendelse af den europæiske ramme for cybersikkerhedscertificering, at bistå og arbejde tæt sammen med Agenturet ved udarbejdelsen af forslag til cybersikkerhedscertificeringsordninger, at anbefale, at Kommissionen anmoder Agenturet om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning og at vedtage udtalelser rettet til Kommissionen vedrørende vedligehold og revision af bestående europæiske cybersikkerhedscertificeringsordninger.

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

(62) Agenturets støtte til cybersikkerhed bør også omfatte kontakter til Rådets Sikkerhedsudvalg og det relevante nationale organ om kryptografisk godkendelse af produkter, der skal bruges i klassificerede net.

(63) Med sigte på at fastsætte de nærmere kriterier for akkrediteringen af overensstemmelsesvurderingsorganer bør Kommissionen tillægges beføjelser til at vedtage retsakter i henhold til artikel 290 i traktaten om Den Europæiske Unions Funktionsmåde. Kommissionen bør under sit forberedende arbejde gennemføre relevante høringer, herunder på ekspertniveau. Disse høringer bør gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016. For at sikre lige deltagelse i forberedelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(64) For at sikre ensartede betingelser for gennemførelsen af denne forordning bør Kommissionen tillægges gennemførelsesbeføjelser, når dette er fastsat i denne forordning. Disse beføjelser bør udøves i overensstemmelse med forordning (EU) nr. 182/2011.

(65) Undersøgelsesproceduren bør anvendes til at vedtage gennemførelsesretsakter om de europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, om Agenturets metoder i forbindelse med gennemførelsen af undersøgelser, samt om vilkår, formater og procedurer for de nationale certificeringstilsynsmyndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer til Kommissionen.

(66) Der bør foretages en uafhængig evaluering af Agenturets arbejde. Evalueringen bør tage stilling til, om Agenturets mål nås, om arbejdsmetoderne er effektive, og om dets opgaver er relevante. Evalueringen bør også vurdere virkningen, effektiviteten og omkostningseffektiviteten af den europæiske ramme for cybersikkerhedscertificering.

(67) Forordning (EU) nr. 526/2013 bør ophæves.

(68) Målene for denne forordning kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne og kan derfor bedre gennemføres på EU-plan; Unionen kan derfor træffe foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går denne forordning ikke ud over, hvad der er nødvendigt for at nå dette mål —

VEDTAGET DENNE FORORDNING:

AFSNIT I
GENERELLE BESTEMMELSER

Artikel 1
Genstand og anvendelsesområde

Med henblik på at sikre et velfungerende indre marked og sørge for et højt niveau af cybersikkerhed, cybermodstandsdygtighed og tillid i Unionen er hensigten med denne forordning:

(a) at fastsætte målene, opgaverne og de organisatoriske aspekter for ENISA, "EU's Agentur for cybersikkerhed" (i det følgende benævnt "Agenturet") og

(b) at fastlægge en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau af IKT-produkter og -tjenester i Unionen. Denne ramme anvendes uden at det berører specifikke bestemmelser vedrørende frivillig eller obligatorisk certificering i andre af Unionens retsakter.

Artikel 2
Definitioner

I denne forordning forstås ved:

(2) "cybersikkerhed": alle aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, deres brugere og berørte personer mod cybertrusler

(3) "net- og informationssystem": et system som defineret i artikel 4, nr. 1), i direktiv (EU) 2016/1148

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

(5) "operatør af væsentlige tjenester": en offentlig eller privat enhed som defineret i artikel 4, nr. 4), i direktiv (EU) 2016/1148

(6) "udbyder af digitale tjenester": enhver juridisk person, som udbyder en digital tjeneste, som defineret i artikel 4, nr. 6), i direktiv (EU) 2016/1148

(7) "hændelse": enhver begivenhed som defineret i artikel 4, nr. 7), i direktiv (EU) 2016/1148

(8) "håndtering af hændelser": alle procedurer som defineret i artikel 4, nr. 8), i direktiv (EU) 2016/1148

(9) "cybertrussel": enhver potentiel omstændighed eller begivenhed, som kan have en negativ indvirkning på net- og informationssystemer, deres brugere og berørte personer

(10) "europæisk cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er fastlagt på EU-plan, og som finder anvendelse på certificeringen af informations- og kommunikationsteknologiske (IKT-) produkter og tjenester, der er omfattet af den pågældende ordning

(11) "europæisk cybersikkerhedsattest": et dokument udstedt af et overensstemmelsesvurderingsorgan, som attesterer at et givet IKT-produkt eller en

given IKT-tjeneste opfylder de specifikke krav i en europæisk cybersikkerhedscertificeringsordning

(12) "IKT-produkter og tjenester": ethvert element eller enhver gruppe af elementer i net- og informationssystemer

(13) "akkreditering": akkreditering som defineret i artikel 2, nr. 10), i forordning (EF) nr. 765/2008

(14) "nationalt akkrediteringsorgan": et nationalt akkrediteringsorgan som defineret i artikel 2, nr. 11), i forordning (EF) nr. 765/2008

(15) "overensstemmelsesvurdering": overensstemmelsesvurdering som defineret i artikel 2, nr. 12), i forordning (EF) nr. 765/2008

(16) "overensstemmelsesvurderingsorgan": overensstemmelsesvurderingsorgan som defineret i artikel 2, nr. 13), i forordning (EF) nr. 765/2008

(17) "standard": en standard som defineret i artikel 2, nr. 1), i forordning (EU) nr. 1025/2012.

AFSNIT II
ENISA – "EU's Agentur for Cybersikkerhed"

KAPITEL I
MANDAT, FORMÅL OG OPGAVER

Artikel 3
Mandat

1. Agenturet udfører de opgaver, det tillægges ved nærværende forordning, med det formål at bidrage til et højt cybersikkerhedsniveau i Unionen.

2. Agenturet 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. Agenturets mål og opgaver berører ikke medlemsstaternes beføjelser med hensyn til cybersikkerhed og berører under ingen omstændigheder aktiviteter vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område.

Artikel 4
Mål

4. Agenturet fungerer som et ekspertisecenter for cybersikkerhed i kraft af sin uafhængighed, den videnskabelige og tekniske kvalitet af den rådgivning og bistand, det yder, og de informationer, det videregiver, samt i kraft af den åbenhed, der er forbundet med dets procedurer og drift, og dets omhu ved udførelsen af sine opgaver.

5. Agenturet bistår Unionens institutioner, agenturer og organer samt medlemsstaterne med udvikling og gennemførelse af politikker vedrørende cybersikkerhed.

6. Agenturet støtter kapacitetsopbygning og beredskab i hele Unionen ved at bistå Unionen, medlemsstaterne og offentlige og private interessenter med at øge beskyttelsen af deres net- og informationssystemer, udvikle færdigheder og kompetencer inden for cybersikkerhed og opnå cybermodstandsdygtighed.

7. Agenturet fremmer samarbejde og koordinering på EU-plan mellem medlemsstaterne, Unionens institutioner, agenturer og organer og relevante interessenter, herunder den private sektor, for så vidt angår cybersikkerhedsanliggender.

8. Agenturet øger cybersikkerhedskapaciteten på EU-plan for at supplere medlemsstaternes indsats for at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser.

9. Agenturet fremmer brugen af certificering, herunder ved at bidrage til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau, jf. afsnit III, for at øge gennemsigtigheden af IKT-produkters og -tjenesters cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked.

10. Agenturet fremmer et højt niveau for oplysning af borgere og virksomheder vedrørende cybersikkerhed.

Artikel 5

Opgaver relateret til udvikling og gennemførelse af Unionens politikker og lovgivning

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

11. bistå og rådgive, navnlig ved at levere uafhængige udtalelser og forberedende arbejde, ved udvikling og revision af Unionens politik og lovgivning på cybersikkerhedsområdet samt sektorspecifik politik og lovgivningsinitiativer, som involverer cybersikkerhedsanliggender

12. 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 udtalelser, retningslinjer, råd og bedste praksis om emner som risikostyring, indberetning af hændelser og informationsudveksling, samt lette udvekslingen af bedste praksis mellem de kompetente myndigheder i denne henseende

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

14. støtte:

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

    (2) fremme af et højere sikkerhedsniveau i elektronisk kommunikation, herunder gennem rådgivning og bistand samt ved at fremme udvekslingen af bedste praksis mellem de kompetente myndigheder

15. understøtte en jævnlig gennemgang af Unionens politiske aktiviteter ved at levere en årsrapport om status for gennemførelsen af de respektive retlige rammer vedrørende:

    (b) medlemsstaternes anmeldelser af hændelser til samarbejdsgruppen via de centrale kontaktpunkter i henhold til artikel 10, stk. 3, i direktiv (EU) 2016/1148

    (c) indberetninger af brud på sikkerheden eller tab af integritet, som er modtaget fra tillidstjenesteudbyderne, og som forelægges Agenturet af tilsynsorganerne i henhold til artikel 19, stk. 3, i forordning (EU) nr. 910/2014

    (d) indberetninger af brud på sikkerheden fra virksomheder, som leverer offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, og som forelægges Agenturet af de kompetente myndigheder i henhold til artikel 40 i [direktiv om en europæisk kodeks for elektronisk kommunikation].

Artikel 6

Opgaver relateret til kapacitetsopbygning

16. Agenturet bistår:

(b) medlemsstaterne i deres bestræbelser på at forbedre forebyggelse, opdagelse og analyse af og kapaciteten til at reagere på cybersikkerhedsproblemer og -hændelser ved at stille den nødvendige viden og ekspertise til rådighed for dem

(c) Unionens institutioner, organer, kontorer og agenturer i deres bestræbelser på at forbedre forebyggelse, opdagelse og analyse af og kapaciteten til at reagere på cybersikkerhedsproblemer og -hændelser gennem passende støtte til CERT'en for Unionens institutioner, agenturer og organer (CERT-EU)

(d) medlemsstaterne, på deres anmodning, med udviklingen af nationale enheder, der håndterer cybersikkerhedshændelser (CSIRT'er) i henhold til artikel 9, stk. 5, i direktiv (EU) 2016/1148

(e) medlemsstaterne, på deres anmodning, med udviklingen af nationale strategier for sikkerhed i net- og informationssystemer i henhold til artikel 7, stk. 2, i direktiv (EU) 2016/1148; Agenturet skal også fremme udbredelsen og følge 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 EU's strategier vedrørende cybersikkerhed og fremmer deres udbredelse og følger fremskridtene med hensyn til deres gennemførelse

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

(h) medlemsstaterne ved at tilrettelægge årlige cybersikkerhedsøvelser i stor skala på EU-plan som omhandlet i artikel 7, stk. 6, 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, eventuelt i samarbejde med interessenter

(j) samarbejdsgruppen ved at udveksle bedste praksis, navnlig med hensyn til medlemsstaternes identificering af operatører af væsentlige tjenester, herunder i forbindelse med en grænseoverskridende afhængighed vedrørende risici og hændelser i henhold til artikel 11, stk. 3, litra l), i direktiv (EU) 2016/1148

17. Agenturet fremmer etableringen af centre for informationsudveksling og analyse (ISAC'er), herunder navnlig i de sektorer, der er nævnt i bilag II i direktiv (EU) 2016/1148, ved at stille bedste praksis og vejledning om tilgængelige værktøjer og procedurer til rådighed samt ved at vejlede om håndtering af lovgivningsmæssige spørgsmål relateret til informationsudveksling.

Artikel 7

Opgaver relateret til operationelt samarbejde på EU-plan

18. Agenturet understøtter det operationelle samarbejde mellem de kompetente offentlige organer og mellem interessenter.

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

    (a) udveksle viden og bedste praksis

    (b) levere rådgivning og retningslinjer om relevante cybersikkerhedsspørgsmål

    (c) indførelse – efter høring af Kommissionen – af praktiske ordninger for udførelse af særlige opgaver.

20. Agenturet varetager sekretariatsfunktionen for CSIRT-netværket, jf. artikel 12, stk. 2, i direktiv (EU) 2016/1148, og skal aktivt fremme informationsudveksling og samarbejdet mellem dets medlemmer.

21. Agenturet bidrager til det operationelle samarbejde i CSIRT-netværket og yder støtte til medlemsstaterne ved at:

    (d) rådgive dem om, hvordan de forbedrer deres evne til at forebygge, opdage og reagere på hændelser

    (e) levere – på deres anmodning – teknisk bistand i tilfælde af hændelser, der har en betydelig eller væsentlig virkning

    (f) analysere sårbarheder, spor (artefacts) og hændelser.

Ved udøvelsen af disse opgaver indgår Agenturet og CERT-EU i et struktureret samarbejde med henblik på at udnytte synergier, herunder navnlig med hensyn til operationelle aspekter.

22. På anmodning af to eller flere berørte medlemsstater og alene med det formål at levere rådgivning om forebyggelse af fremtidige hændelser skal Agenturet yde støtte til eller foretage en efterfølgende teknisk undersøgelse efter underretning fra de berørte virksomheder om hændelser, der har en betydelig eller væsentlig virkning, i henhold til direktiv (EU) 2016/1148. Agenturet skal også foretage en sådan undersøgelse efter en behørigt begrundet anmodning fra Kommissionen og efter aftale med de berørte medlemsstater i tilfælde, hvor flere end to medlemsstater berøres af sådanne hændelser.

    Undersøgelsens omfang og proceduren, der skal følges under udførelsen af en sådan undersøgelse, skal aftales mellem de berørte medlemsstater og Agenturet og berører ikke en eventuel strafferetlig efterforskning af samme hændelse. Undersøgelsen afsluttes med en endelig teknisk rapport udarbejdet af Agenturet, der navnlig er baseret på oplysninger og bemærkninger fra de berørte medlemsstater og virksomheder, og som er aftalt med de berørte medlemsstater. En sammenfattende rapport fokuseret på anbefalinger for at forhindre fremtidige hændelser vil blive delt med CSIRT-netværket.

23. Agenturet tilrettelægger årlige cybersikkerhedsøvelser på EU-niveau og på deres anmodning støtte medlemsstaterne og EU's institutioner, agenturer og organer i at tilrettelægge øvelser. Årlige øvelser på EU-plan skal omfatte tekniske, operationelle

og strategiske elementer og bidrage til at forberede den samordnede indsats på EU-plan mod væsentlige grænseoverskridende cybersikkerhedshændelser. Agenturet bidrager også til og hjælper med at tilrettelægge, hvor det er relevant, sektorspecifikke cybersikkerhedsøvelser sammen med relevante ISAC'er og give ISAC'er mulighed for også at deltage i cybersikkerhedsøvelser på EU-plan.

24. Agenturet udarbejder regelmæssigt en teknisk EU-cybersikkerhedsrapport om hændelser og trusler, der skal være baseret på offentligt tilgængelige oplysninger, Agenturets egen analyse og rapporter, som deles af bl.a. medlemsstaternes CSIRT'er (på frivillig basis) eller NIS-direktivets centrale kontaktpunkter (jf. artikel 14, stk. 5, i NIS-direktivet), Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol og CERT-EU.

25. Agenturet bidrager til at udvikle en samarbejdsorienteret respons på EU- og medlemsstatsplan på væsentlige grænseoverskridende cybersikkerhedshændelser eller -kriser ved at:

(g) sammenstille rapporter fra nationale kilder med henblik på at bidrage til at skabe en fælles situationsforståelse

(h) sikre en effektiv informationsstrøm og sørge for, at der er eskalationsmekanismer på plads til brug mellem CSIRT-netværket og de tekniske og politiske beslutningstagere på EU-niveau

(i) understøtte den tekniske håndtering af en hændelse eller en krise, herunder ved at fremme delingen af tekniske løsninger mellem medlemsstaterne

(j) understøtte kommunikation til offentligheden om hændelsen eller krisen

(k) afprøve samarbejdsplaner for reaktionen på sådanne hændelser eller kriser.

Artikel 8

Opgaver relateret til markedet, cybersikkerhedscertificering og standardisering

Agenturet skal:

(k) støtte og fremme udviklingen og gennemførelsen af Unionens politik vedrørende cybersikkerhedscertificering af IKT-produkter og -tjenester, som fastsat i denne forordnings afsnit III, ved at

(1) forberede forslag til europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester i henhold til denne forordnings artikel 44

(2) bistå Kommissionen med at varetage sekretariatsfunktionen for den europæiske cybersikkerhedscertificeringsgruppe i henhold til denne forordnings artikel 53

(3) samle og offentliggøre retningslinjer og udvikle god praksis vedrørende cybersikkerhedskrav til IKT-produkter og -tjenester i samarbejde med nationale certificeringstilsynsmyndigheder og branchen

(l) fremme indførelse og udbredelse af europæiske og internationale standarder for risikostyring og sikkerhed af IKT-produkter og -tjenester og i samarbejde med medlemsstaterne udarbejde 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

(m) udføre og formidle regelmæssige analyser af de vigtigste tendenser på markedet for cybersikkerhed, både på efterspørgsels- og udbudssiden, med henblik på fremme af cybersikkerhedsmarkedet i Unionen.

Artikel 9

Opgaver relateret til viden, information og oplysning

Agenturet skal:

(n) udføre analyser af nye teknologier og tilvejebringe emnespecifikke vurderinger af de forventede sociale, retlige, økonomiske og lovgivningsmæssige konsekvenser af teknologiske innovationer inden for cybersikkerhed

(o) udføre langsigtede strategiske analyser af cybersikkerhedstrusler og hændelser for at identificere nye tendenser og bidrage til at forebygge cybersikkerhedsrelaterede problemer

(p) i samarbejde med eksperter fra medlemsstaterne levere rådgivning, vejledning og bedste praksis for sikkerheden af net- og informationssystemer, navnlig for sikkerheden af internetinfrastruktur og de infrastrukturer, der understøtter sektorerne nævnt i bilag II til direktiv (EU) 2016/1148

(q) via en særlig webportal samle, organisere og offentliggøre oplysninger om cybersikkerhed, der leveres af Unions institutioner, agenturer og organer

(r) højne offentlighedens oplysningsniveau om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere og organisationer

(s) indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og sammenstille rapporter med henblik på at yde vejledning til virksomheder og borgere i hele Unionen

(t) i samarbejde med medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer tilrettelægge jævnlige informations- og oplysningskampagner for at øge cybersikkerheden og dens synlighed i Unionen.

Artikel 10

Opgaver relateret til forskning og innovation

I forbindelse med forskning og innovation skal Agenturet:

(u) rådgive Unionen og medlemsstaterne om forskningsbehov på cybersikkerhedsområdet med henblik på at gøre det muligt effektivt at imødegå nuværende og kommende risici og -trusler, herunder hvad angår nye og kommende informations- og kommunikationsteknologier, og effektivt bruge risikoforebyggende teknologier

(v) i tilfælde, hvor Kommissionen har uddelegeret de relevante beføjelser til Agenturet, deltage i gennemførelsesfasen af programmer til finansiering af forskning og innovation eller som en støttemodtager.

Artikel 11
Opgaver relateret til internationalt samarbejde

Agenturet skal bidrage til Unionens indsats for at samarbejde med tredjelande og internationale organisationer med henblik på at fremme internationalt samarbejde om cybersikkerhed ved:

(w) at deltage, hvor det er relevant, som observatør og i tilrettelæggelsen af internationale øvelser, og analysere og rapportere om resultatet af sådanne øvelser til bestyrelsen

(x) på Kommissionens anmodning at fremme udveksling af bedste praksis mellem de relevante internationale organisationer

(y) efter anmodning at stille ekspertise til rådighed for Kommissionen.

KAPITEL II
AGENTURETS ORGANISATION

Artikel 12
Struktur

Agenturets administrative og ledelsesmæssige struktur består af:

(z) en bestyrelse, der varetager de funktioner, der er fastsat i artikel 14

(æ) et forretningsudvalg, der varetager de funktioner, der er fastsat i artikel 18

(ø) en administrerende direktør, der varetager de ansvarsområder, der er fastsat i artikel 19, og

(å) en stående gruppe af interessenter, der varetager de funktioner, der er fastsat i artikel 20.

AFDELING 1
BESTYRELSEN

Artikel 13
Bestyrelsens sammensætning

26. Bestyrelsen består af en repræsentant for hver medlemsstat og to repræsentanter, der udnævnes af Kommissionen. Alle repræsentanter har stemmeret.

27. Hvert medlem af bestyrelsen skal have en stedfortræder, der repræsenterer medlemmet, når det ikke er til stede.

28. Medlemmerne af bestyrelsen og deres stedfortrædere udpeges på grundlag af deres viden på cybersikkerhedsområdet og under hensyntagen til 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 en ligelig repræsentation af mænd og kvinder i bestyrelsen.

29. Embedsperioden for medlemmer af bestyrelsen og deres stedfortrædere er fire år. Perioden kan forlænges.

Artikel 14
Bestyrelsens opgaver

30. Bestyrelsen skal:

(a) fastlægge de overordnede retningslinjer for Agenturets drift og sikre, at Agenturet udfører sine opgaver i overensstemmelse med de regler og principper, der er fastsat i denne forordning. Den sikrer endvidere, at der er sammenhæng mellem Agenturets arbejde og aktiviteter, der udføres af medlemsstaterne og på EU-plan

(b) vedtage Agenturets udkast til det samlede programmeringsdokument, der er omhandlet i artikel 21, før det forelægges for Kommissionen med henblik på en udtalelse

(c) under hensyntagen til Kommissionens udtalelse vedtage Agenturets samlede programmeringsdokument med et flertal på to tredjedele af medlemmerne og i overensstemmelse med artikel 17

(d) med et flertal på to tredjedele af medlemmerne vedtage Agenturets årsbudget og varetage andre funktioner i relation til Agenturets budget i henhold til kapitel III

(e) evaluere og vedtage den konsoliderede årsberetning om Agenturets virksomhed og sende både rapporten og bestyrelsens evaluering til Europa-Parlamentet, Rådet, Kommissionen og Revisionsretten senest den 1. juli i det følgende år. Årsberetningen skal indeholde regnskaberne og beskrive, i hvilket omfang Agenturet har opfyldt sine resultatindikatorer. Årsberetningen offentliggøres

(f) vedtage de finansielle bestemmelser for Agenturet, jf. artikel 29

(g) vedtage en strategi for bekæmpelse af svig, som står i forhold til risikoen for svig, og som tager de påtænkte foranstaltningers omkostningseffektivitet i betragtning

(h) vedtage regler for forebyggelse og håndtering af interessekonflikter i forhold til medlemmerne

(i) sikre passende opfølgning på resultater og henstillinger, der stammer fra undersøgelser foretaget af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og fra forskellige interne eller eksterne revisions- og evalueringsrapporter

(j) vedtage sin forretningsorden

(k) over for Agenturets personale udøve de beføjelser, som personalevedtægten tillægger ansættelsesmyndigheden, og som ansættelsesvilkårene for Unionens øvrige ansatte tillægger den myndighed, der har kompetence til at indgå ansættelseskontrakter (i det følgende benævnt "beføjelserne som ansættelsesmyndighed"), jf. stk. 2

(l) vedtage passende gennemførelsesbestemmelser til personalevedtægten og ansættelsesvilkårene for Unionens øvrige ansatte i overensstemmelse med artikel 110 i personalevedtægten

(m) udnævne den administrerende direktør og, hvis relevant, forlænge den administrerende direktørs ansættelsesperiode eller afskedige vedkommende i overensstemmelse med denne forordnings artikel 33

(n) udnævne en regnskabsfører, som kan være Kommissionens regnskabsfører, som er fuldstændig uafhængig i udøvelsen af sit hverv

(o) træffe alle afgørelser vedrørende etablering af Agenturets organisatoriske struktur og om nødvendigt ændring heraf under hensyntagen til Agenturets aktivitetsbehov og under hensyntagen til forsvarlig budgetforvaltning

(p) bemyndige indgåelsen af samarbejdsaftaler i overensstemmelse med artikel 7 og 39.

31. Bestyrelsen vedtager i medfør af personalevedtægtens artikel 110 en afgørelse baseret på personalevedtægtens artikel 2, stk. 1, og artikel 6 i ansættelsesvilkårene for de øvrige ansatte om at delegere de relevante beføjelser som ansættelsesmyndighed til den administrerende direktør og fastlægger betingelserne for at suspendere denne delegation af beføjelser. Den administrerende direktør bemyndiges til at uddelegere disse beføjelser.

32. Under helt særlige omstændigheder kan bestyrelsen ved en afgørelse midlertidigt suspendere de beføjelser som ansættelsesmyndighed, der er delegeret til den administrerende direktør, og de beføjelser, denne måtte have videredelegeret, og selv udøve dem eller delegere dem til et af sine medlemmer eller en anden ansat end den administrerende direktør.

Artikel 15
Bestyrelsens formand

Bestyrelsen vælger – med to tredjedeles flertal – blandt sine medlemmer en formand og en næstformand for en periode på fire år, der kan forlænges én gang. Hvis en formand eller næstformand ophører med at være medlem af bestyrelsen under sin embedsperiode, ophører embedsperioden dog automatisk samtidig. Næstformanden træder uden videre i stedet for formanden, hvis denne er forhindret i at udøve sit hverv.

Artikel 16
Bestyrelsens møder

33. Det påhviler bestyrelsens formand at indkalde til dens møder.

34. 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.

35. Den administrerende direktør deltager uden stemmeret i bestyrelsens møder.

36. Medlemmerne af den stående gruppe af interessenter kan efter invitation fra formanden deltage i bestyrelsens møder uden stemmeret.

37. Bestyrelsesmedlemmerne og deres stedfortrædere kan under møderne, såfremt forretningsordenen tillader det, bistås af rådgivere eller eksperter.

38. Agenturet varetager sekretariatsopgaverne for bestyrelsen.

Artikel 17
Bestyrelsens afstemningsregler

39. Bestyrelsen træffer sine afgørelser med absolut flertal blandt medlemmerne.

40. 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 embedsperiode.

41. Hvert medlem har én stemme. Hvis et medlem ikke er til stede, har medlemmets stedfortræder stemmeretten.

42. Formanden deltager i afstemningen.

43. Den administrerende direktør deltager ikke i afstemningen.

44. I bestyrelsens forretningsorden fastsættes mere detaljerede afstemningsregler, navnlig regler om, hvornår et medlem kan handle på et andet medlems vegne.

AFDELING 2
FORRETNINGSUDVALGET

Artikel 18
Forretningsudvalget

45. Bestyrelsen bistås af et forretningsudvalg.

46. Forretningsudvalget skal:

(b) forberede de afgørelser, der skal træffes af bestyrelsen

(c) i samarbejde med bestyrelsen sikre passende opfølgning på de resultater og henstillinger, der stammer fra undersøgelser foretaget af OLAF og fra forskellige interne eller eksterne audit- og evalueringsrapporter

(d) uden at det berører den administrerende direktørs ansvar, jf. artikel 19, bistår forretningsudvalget den administrerende direktør i gennemførelsen af bestyrelsens afgørelser vedrørende administrative og budgetmæssige spørgsmål i henhold til artikel 19.

47. Forretningsudvalget består af fem medlemmer, der udpeges blandt medlemmerne af bestyrelsen, heriblandt formanden for bestyrelsen, der også kan være formand for forretningsudvalget, og en af repræsentanterne for Kommissionen. Den administrerende direktør deltager i forretningsudvalgets møder, men har ikke stemmeret.

48. Forretningsudvalgsmedlemmerne har en embedsperiode på fire år. Perioden kan fornys.

49. Forretningsudvalget mødes mindst én gang hver tredje måned. Formanden for forretningsudvalget indkalder til yderligere møder på anmodning af forretningsudvalgets medlemmer.

50. Bestyrelsen vedtager forretningsudvalgets forretningsorden.

51. Hvis det er nødvendigt i hastende tilfælde, kan forretningsudvalget træffe visse midlertidige afgørelser på bestyrelsens vegne, navnlig vedrørende den administrative forvaltning, herunder suspendering af delegationen af beføjelser som ansættelsesmyndighed, og budgetanliggender.

AFDELING 3
DEN ADMINISTRERENDE DIREKTØR

Artikel 19
Den administrerende direktørs opgaver

52. Agenturet ledes af den administrerende direktør, som udfører sit hverv i uafhængighed. Den administrerende direktør står til ansvar over for bestyrelsen.

53. 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.

54. Den administrerende direktør er ansvarlig for:

(a) den daglige administration af Agenturet

(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 om dets gennemførelse

(e) at udarbejde den konsoliderede årlige aktivitetsrapport om Agenturets aktiviteter og forelægge denne for bestyrelsen til vurdering og godkendelse

(f) at udarbejde en handlingsplan til opfølgning af konklusionerne fra efterfølgende evalueringer og aflæggelse af en statusrapport til Kommissionen hvert andet år

(g) at udarbejde en handlingsplan som opfølgning af konklusionerne i interne eller eksterne auditrapporter samt undersøgelser fra Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) og at aflægge statusrapport to gange om året til Kommissionen og regelmæssigt til bestyrelsen

(h) at udarbejde udkast til finansielle bestemmelser for Agenturet

(i) at udarbejde Agenturets udkast til et 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 Agenturets 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 de relevante interessenter

(m) andre opgaver, som den administrerende direktør pålægges ved denne forordning.

55. Er det nødvendigt og i overensstemmelse med Agenturets mandat og dets formål og opgaver, kan den administrerende direktør nedsætte ad hoc-arbejdsgrupper bestående af eksperter, bl.a. fra medlemsstaternes kompetente myndigheder. Bestyrelsen underrettes på forhånd herom. Procedurerne vedrørende især sammensætningen af arbejdsgrupperne, den administrerende direktørs udnævnelse af eksperterne til arbejdsgrupperne og arbejdsgruppernes virke fastsættes i Agenturets interne forretningsgange.

56. Den administrerende direktør beslutter, om det er nødvendigt at placere en eller flere medarbejdere i en eller flere medlemsstater med henblik på at udføre Agenturets opgaver på effektiv og virkningsfuld vis. Inden den administrerende direktør beslutter at oprette et lokalt kontor, indhenter han forudgående samtykke fra Kommissionen, bestyrelsen og den eller de berørte medlemsstater. I beslutningen fastsættes omfanget af de aktiviteter, der skal udføres af det lokale kontor, således at der undgås unødige omkostninger og overlapning af Agenturets administrative funktioner. Der indgås en aftale med den eller de berørte medlemsstater, hvor det er hensigtsmæssigt eller påkrævet.

AFDELING 4
DEN STÅENDE GRUPPE AF INTERESSENTER

Artikel 20
Den stående gruppe af interessenter

57. På forslag af den administrerende direktør nedsætter bestyrelsen en stående gruppe af interessenter bestående af anerkendte eksperter, der repræsenterer de relevante interessenter såsom IKT-industrien, udbydere af elektroniske kommunikationsnet og -tjenester til offentligheden, forbrugergrupper, akademiske eksperter i cybersikkerhed og repræsentanter for de kompetente myndigheder, der er givet meddelelse om i henhold til [direktiv om en europæisk kodeks for elektronisk kommunikation], samt retshåndhævende myndigheder og databeskyttelsestilsynsmyndigheder.

58. Procedurerne for den stående gruppe af interessenter, vedrørende især gruppens antal, sammensætning og bestyrelsens udpegelse af dens medlemmer, den administrerende direktørs forslag og gruppens virke, fastlægges i Agenturets interne forretningsgange og offentliggøres.

59. Den stående gruppe af interessenter ledes af den administrerende direktør eller af en person udpeget af den administrerende direktør fra sag til sag.

60. Embedsperioden for medlemmerne af den stående gruppe af interessenter er to et halvt år. Medlemmer af bestyrelsen kan ikke være medlemmer af den stående gruppe af interessenter. Eksperter fra Kommissionen og medlemsstaterne har ret til at være til stede på møderne og deltage i arbejdet i den stående gruppe af interessenter. Repræsentanter for andre organer, som den administrerende direktør skønner er relevante, og som ikke er medlemmer af den stående gruppe af interessenter, kan indbydes til at være til stede på møderne og deltage i arbejdet i den stående gruppe af interessenter.

61. Den stående gruppe af interessenter rådgiver Agenturet med hensyn til udførelsen af dets aktiviteter. Den rådgiver navnlig den administrerende direktør om udarbejdelsen af forslag til Agenturets arbejdsprogram samt om varetagelse af kommunikation med de relevante interessenter om alle spørgsmål, der vedrører arbejdsprogrammet.

AFDELING 5
DRIFT

Artikel 21
Det samlede programmeringsdokument

62. Agenturet udfører sine aktiviteter i overensstemmelse med det samlede programmeringsdokument, som omfatter det flerårige og det årlige arbejdsprogram, og som skal indeholde alle planlagte aktiviteter.

63. Hvert år udarbejder den administrerende direktør under hensyntagen til Kommissionens retningslinjer det samlede programmeringsdokument, som omfatter det flerårige og det årlige arbejdsprogram, med de modsvarende planer for menneskelige og finansielle ressourcer, jf. artikel 32 i Kommissionens delegerede forordning (EU) nr. 1271/2013[36].

64. 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 senere ajourførte udgaver af dokumentet.

65. Det samlede programmeringsdokument bliver endeligt efter den endelige vedtagelse af Unionens almindelige budget, og om nødvendigt justeres det i overensstemmelse hermed.

66. 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 finansielle ressourcer og personaleressourcer, 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 nævnte flerårige

---

[36] 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).

arbejdsprogram. Det skal klart anføres i programmet, hvilke opgaver der er blevet tilføjet, ændret eller slettet i forhold til det foregående regnskabsår.

67. Bestyrelsen ændrer det vedtagne årlige arbejdsprogram, hvis Agenturet 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.

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

69. Ressourceplanen ajourføres hvert år. Den strategiske programmering ajourføres efter behov, særlig med henblik på at tage højde for resultatet af den evaluering, der er omhandlet i artikel 56.

Artikel 22
Interesseerklæring

70. Medlemmerne af bestyrelsen, 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.

71. Medlemmerne af bestyrelsen, den administrerende direktør og eksterne eksperter, der deltager i ad hoc-arbejdsgrupper, skal hver især på præcis og fyldestgørende vis senest på hvert møde gøre opmærksom på eventuelle interesser, som kan anses for at berøre deres uafhængighed med hensyn til de punkter, der er på dagsordenen, og skal afholde sig fra at deltage i drøftelserne af og afstemningen om de pågældende punkter.

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

Artikel 23
Gennemsigtighed

73. Agenturet sikrer, at der er en høj grad af gennemsigtighed i dets aktiviteter i overensstemmelse med artikel 25.

74. Agenturet 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 22.

75. Bestyrelsen kan på forslag af den administrerende direktør give interesserede parter tilladelse til at følge procedurerne i forbindelse med nogle af Agenturets aktiviteter.

76. Agenturet fastsætter i sine interne forretningsgange bestemmelser om, hvordan de i stk. 1 og 2 omhandlede regler om gennemsigtighed gennemføres i praksis.

Artikel 24
Fortrolighed

77. Uden at det berører artikel 25, må Agenturet ikke til tredjemand videregive oplysninger, som det behandler eller modtager, og for hvilke der foreligger en begrundet begæring om, at de holdes helt eller delvist fortrolige.

78. Medlemmerne af bestyrelsen, den administrerende direktør, medlemmerne af den stående gruppe af interessenter, eksterne eksperter, der deltager i ad hoc-arbejdsgrupperne, samt Agenturets personale, herunder embedsmænd, der midlertidigt er stillet til rådighed af medlemsstaterne, skal, selv efter at deres hverv er ophørt, overholde forpligtelsen til fortrolighed som fastsat i artikel 339 i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

79. Agenturet fastsætter i sine interne forretningsgange bestemmelser om, hvordan de i stk. 1 og 2 omhandlede regler om fortrolighed gennemføres i praksis.

80. Bestyrelsen beslutter, såfremt det er nødvendigt for udførelsen af Agenturets opgaver, at tillade Agenturet at behandle klassificerede oplysninger. I så fald vedtager bestyrelsen efter aftale med Kommissionens tjenestegrene interne forretningsgange baseret på sikkerhedsprincipperne i Kommissionens afgørelse (EU, Euratom) 2015/443[37] og 2015/444[38]. Disse forretningsgange skal blandt andet indeholde bestemmelser om udveksling, behandling og opbevaring af klassificerede oplysninger.

Artikel 25
Aktindsigt

81. Forordning (EF) nr. 1049/2001 finder anvendelse på Agenturets dokumenter.

82. Bestyrelsen vedtager de praktiske bestemmelser til gennemførelse af forordning (EF) nr. 1049/2001 senest seks måneder efter, at Agenturet er oprettet.

83. De beslutninger, som agenturet træffer efter artikel 8 i forordning (EF) nr. 1049/2001, kan gøres til genstand for en klage til Ombudsmanden i henhold til artikel 228 i TEUF eller en klage indbragt for Den Europæiske Unions Domstol i henhold til artikel 263 i TEUF.

KAPITEL III
BUDGETTETS OPSTILING OG STRUKTUR

Artikel 26
Opstilling af budgettet

84. Hvert år udarbejder den administrerende direktør et udkast til overslag over Agenturets indtægter og udgifter for det følgende regnskabsår og forelægger det for

[37] Kommissionens afgørelse (EU, Euratom) 2015/443 af 13. marts 2015 om sikkerhedsbeskyttelse i Kommissionen (EUT L 72 af 17.3.2015, s. 41).

[38] 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).

bestyrelsen, ledsaget af et udkast til stillingsfortegnelse. Der skal være balance mellem indtægter og udgifter.

85. Hvert år vedtager bestyrelsen på grundlag af udkastet til overslag over indtægter og udgifter fra den administrerende direktør et overslag over Agenturets indtægter og udgifter for det kommende regnskabsår.

86. Bestyrelsen fremsender senest den 31. januar hvert år det i stk. 2 omhandlede overslag, der skal være en del af udkastet til det samlede programmeringsdokument, til Kommissionen og de tredjelande, som Unionen har indgået aftaler med i overensstemmelse med artikel 39.

87. På grundlag af dette overslag opfører Kommissionen i forslaget til Unionens budget de overslag, den skønner nødvendige for stillingsfortegnelsen, og de bidrag, der ydes over det almindelige budget, og fremsender forslaget til Europa-Parlamentet og Rådet i overensstemmelse med artikel 313 og 314 i TEUF.

88. Europa-Parlamentet og Rådet godkender bevillingen af bidraget til Agenturet.

89. Europa-Parlamentet og Rådet vedtager Agenturets stillingsfortegnelse.

90. Bestyrelsen vedtager Agenturets budget sammen med det samlede programmeringsdokument. Det bliver endeligt efter den endelige vedtagelse af Unionens almindelige budget. Om nødvendigt afpasser bestyrelsen Agenturets budget og dets samlede programmeringsdokument i overensstemmelse med Unionens almindelige budget.

Artikel 27
Budgettets struktur

91. Med forbehold af andre ressourcer udgøres Agenturets indtægter af:

(b) et bidrag fra EU-budgettet

(c) formålsbestemte indtægter med henblik på specifikke udgiftsposter i henhold til de finansielle bestemmelser omhandlet i artikel 29

(d) EU-finansiering i form af delegationsaftaler eller ad hoc-tilskud i henhold til de finansielle bestemmelser i artikel 29 og til bestemmelserne i de relevante instrumenter til gennemførelse af Unionens politik

(e) bidrag fra tredjelande, der deltager i Agenturets arbejde i henhold til artikel 39

(f) frivillige bidrag fra medlemsstaterne i form af pengebeløb eller naturalier. Medlemsstater, der yder frivillige bidrag, kan ikke påberåbe sig nogen specifikke rettigheder eller tjenester som et resultat heraf.

92. Agenturets udgifter omfatter udgifter til personale, administrativ og teknisk bistand, infrastruktur og driftsudgifter, samt udgifter som følge af kontrakter, der er indgået med tredjemand.

Artikel 28
Gennemførelse af budgettet

93. Den administrerende direktør er ansvarlig for gennemførelsen af Agenturets budget.

94. Kommissionens interne revisor varetager i forhold til Agenturet de samme funktioner, som er tildelt denne i forhold til Kommissionens tjenestegrene.

95. Agenturets regnskabsfører sender inden den 1. marts efter det afsluttede regnskabsår (1. marts i år N+1) det foreløbige årsregnskab til Kommissionens regnskabsfører og Revisionsretten.

96. Ved modtagelsen af Revisionsrettens bemærkninger om Agenturets foreløbige årsregnskab opstiller Agenturets regnskabsfører på eget ansvar agenturets endelige årsregnskab.

97. Den administrerende direktør forelægger det endelige årsregnskab til udtalelse for bestyrelsen.

98. Den administrerende direktør sender senest den 31. marts i år N + 1 det endelige årsregnskab, herunder beretningen om budgetforvaltningen og den økonomiske forvaltning til Europa-Parlamentet, Rådet, Kommissionen og Revisionsretten.

99. Regnskabsføreren sender senest den 1. juli i år N+1 det endelige årsregnskab ledsaget af bestyrelsens udtalelse til Europa-Parlamentet, Rådet, Kommissionens regnskabsfører og Revisionsretten.

100. Regnskabsføreren sender ligeledes en forvaltningserklæring, der dækker disse endelige årsregnskaber, til Revisionsretten, med kopi til Kommissionens regnskabsfører, på samme dato som fremsendelsen af disse endelige årsregnskaber.

101. Den administrerende direktør offentliggør det endelige regnskab senest den 15. november det følgende år.

102. 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.

103. Den administrerende direktør forelægger alle de oplysninger, der er nødvendige for, at dechargeproceduren for det pågældende regnskabsår kan forløbe tilfredsstillende, for Europa-Parlamentet på dettes anmodning, jf. artikel 165, stk. 3, i finansforordningen.

104. Efter henstilling fra Rådet meddeler Europa-Parlamentet inden den 15. maj i år N + 2 den administrerende direktør decharge for gennemførelsen af budgettet for regnskabsåret N.

Artikel 29
Finansielle bestemmelser

De finansielle bestemmelser for Agenturet vedtages af bestyrelsen efter høring af Kommissionen. De må ikke afvige fra forordning (EU) nr. 1271/2013, medmindre dette er strengt nødvendigt for Agenturets drift, og Kommissionen på forhånd har givet sit samtykke.

Artikel 30
Bekæmpelse af svig

105. For at lette bekæmpelsen af svig, korruption og andre retsstridige handlinger i henhold til Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013[39] tiltræder Agenturet, senest seks måneder fra den dag, det bliver operationelt, den interinstitutionelle aftale af 25. maj 1999 om de interne undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF), og vedtager de nødvendige bestemmelser, som skal finde anvendelse på Agenturets medarbejdere, under anvendelse af den model, der findes i bilaget til nævnte aftale.

106. Revisionsretten har beføjelse til gennem bilagskontrol og kontrol på stedet at kontrollere alle tilskudsmodtagere, kontrahenter og underkontrahenter, der har modtaget EU-midler gennem Agenturet.

107. OLAF kan efter bestemmelserne og procedurerne i Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 og Rådets forordning (Euratom, EF) nr. 2185/96[40] 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 foretage undersøgelser, herunder kontrol og inspektion på stedet, med henblik på at fastslå, om der er begået svig, korruption eller andre ulovlige aktiviteter, der berører Unionens finansielle interesser, i forbindelse med tilskud eller en kontrakt, der er finansieret af Agenturet.

108. Uden at det berører stk. 1, 2 og 3, skal Agenturets samarbejdsaftaler med tredjelande og med internationale organisationer, kontrakter, aftaler om tilskud 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 IV
AGENTURETS PERSONALE

Artikel 31
Generelle bestemmelser

Vedtægten for tjenestemænd og ansættelsesvilkårene for øvrige ansatte og de regler, som EU-institutionerne i fællesskab har vedtaget for anvendelsen af denne vedtægt og disse ansættelsesvilkår, gælder for Agenturets personale.

---

39 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).

40 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).

Artikel 32

Privilegier og immuniteter

Protokol nr. 7 vedrørende Den Europæiske Unions privilegier og immuniteter, der er vedhæftet som bilag til traktaten om Den Europæiske Union og til TEUF, gælder for Agenturet og dets personale.

Artikel 33

Den administrerende direktør

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

110. Den administrerende direktør udnævnes af bestyrelsen på grundlag af en liste over kandidater, som Kommissionen foreslår, efter en åben og gennemsigtig udvælgelsesprocedure.

111. Med henblik på indgåelsen af kontrakten med den administrerende direktør repræsenteres Agenturet af formanden for bestyrelsen.

112. Før udnævnelsen indbydes den ansøger, bestyrelsen har valgt, til at afgive en redegørelse for Europa-Parlamentets relevante udvalg og besvare spørgsmål fra medlemmerne.

113. Den administrerende direktørs embedsperiode er fem år. Ved udgangen af denne periode foretager Kommissionen en vurdering, der tager evalueringen af den administrerende direktørs resultater og Agenturets fremtidige opgaver og udfordringer i betragtning.

114. Afgørelser om udnævnelse af den administrerende direktør, forlængelse af dennes ansættelsesperiode og afskedigelse træffes af bestyrelsen med et flertal på to tredjedele af de stemmeberettigede bestyrelsesmedlemmer.

115. Bestyrelsen kan på grundlag af et forslag fra Kommissionen, der tager udgangspunkt i den i stk. 5 omhandlede vurdering, forny den administrerende direktørs embedsperiode én gang, dog højst for en periode på fem år.

116. Bestyrelsen underretter Europa-Parlamentet, hvis den har til hensigt at forlænge den administrerende direktørs embedsperiode. Inden for tre måneder inden forlængelsen af embedsperioden afgiver den administrerende direktør, såfremt denne indbydes hertil, en redegørelse for Europa-Parlamentets relevante udvalg og besvarer spørgsmål.

117. En administrerende direktør, hvis embedsperiode er blevet forlænget, kan ikke deltage i endnu en udvælgelsesprocedure til den samme stilling.

118. Den administrerende direktør kan kun afskediges ved en afgørelse truffet af bestyrelsen efter forslag fra Kommissionen.

Artikel 34

Udstationerede nationale eksperter og andet personale

119. Agenturet kan gøre brug af udstationerede nationale eksperter og andet personale, der ikke er ansat af Agenturet. Vedtægten for tjenestemænd og ansættelsesvilkårene for de øvrige ansatte gælder ikke for dette personale.

120. Bestyrelsen vedtager en afgørelse, der fastlægger regler for udstationering af nationale eksperter til Agenturet.

KAPITEL V
GENERELLE BESTEMMELSER

Artikel 35
Agenturets retlige status

121. Agenturet er et EU-organ og har status som juridisk person.

122. Agenturet har i hver medlemsstat den videstgående rets- og handleevne, som vedkommende stats lovgivning tillægger juridiske personer. Det kan bl.a. erhverve og afhænde fast ejendom og løsøre og optræde som part i retssager.

123. Agenturet repræsenteres af sin administrerende direktør.

Artikel 36
Agenturets ansvar

124. Agenturets ansvar i kontraktforhold reguleres af den lovgivning, der finder anvendelse på den pågældende kontrakt.

125. Den Europæiske Unions Domstol har kompetence til at træffe afgørelse i henhold til en voldgiftsbestemmelse i en kontrakt, som Agenturet har indgået.

126. For så vidt angår ansvar uden for kontraktforhold, skal Agenturet i overensstemmelse med de almindelige retsgrundsætninger, der er fælles for medlemsstaternes retssystemer, erstatte skader, der er forvoldt af Agenturet eller af dets ansatte under udøvelsen af deres hverv.

127. Den Europæiske Unions Domstol har kompetence til at træffe afgørelse i tvister vedrørende sådanne skadeserstatninger.

128. De ansattes personlige ansvar over for Agenturet fastsættes i de ansættelsesvilkår, der gælder for Agenturets personale.

Artikel 37
Sprogordning

129. Bestemmelserne i forordning nr. 1 finder anvendelse på Agenturet[41]. Medlemsstaterne og andre organer, der er udpeget af dem, kan henvende sig til Agenturet og modtage svar på det af EU-institutionernes officielle sprog, de ønsker.

130. De oversættelsesopgaver, der er påkrævet i forbindelse med Agenturets virksomhed, udføres af Oversættelsescentret for Den Europæiske Unions Organer.

[41] 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. 401).

Artikel 38

Beskyttelse af personoplysninger

131. Agenturets behandling af personoplysninger er omfattet af Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001[42].

132. Bestyrelsen vedtager gennemførelsesbestemmelser, som omhandlet i artikel 24, stk. 8, i forordning (EF) nr. 45/2001. Bestyrelsen kan vedtage supplerende foranstaltninger, der er nødvendige med henblik på Agenturets anvendelse af forordning (EF) nr. 45/2001.

Artikel 39

Samarbejde med tredjelande og internationale organisationer

133. I det omfang det er nødvendigt for at nå de i denne forordning fastsatte mål, kan Agenturet samarbejde med kompetente myndigheder i tredjelande og/eller med internationale organisationer. I det øjemed kan Agenturet, forudsat at Kommissionens giver sin forhåndsgodkendelse, etablere samarbejdsordninger med myndigheder i tredjelande og internationale organisationer. Disse ordninger må ikke skabe retlige forpligtelser for Unionen og dens medlemsstater.

134. Tredjelande, som har indgået aftaler med Unionen herom, kan deltage i Agenturets arbejde. Der fastlægges i henhold til de relevante bestemmelser i disse aftaler ordninger, hvori navnlig arten, omfanget og måden af disse landes deltagelse i Agenturets arbejde fastsættes, herunder bestemmelser om deltagelse i initiativer iværksat af Agenturet, økonomiske bidrag og personale. Hvad angår personaleanliggender, skal disse ordninger under alle omstændigheder være i overensstemmelse med personalevedtægten.

135. Bestyrelsen vedtager en strategi for forbindelser med tredjelande eller internationale organisationer for så vidt angår spørgsmål, der hører under Agenturets kompetenceområde. Ved indgåelse af en passende samarbejdsaftale med Agenturets administrerende direktør sikrer Kommissionen, at Agenturet arbejder inden for sit mandat og den gældende institutionelle ramme.

Artikel 40

Sikkerhedsregler for beskyttelse af klassificerede oplysninger og ikkeklassificerede følsomme oplysninger

I samråd med Kommissionen vedtager Agenturet egne sikkerhedsregler, der svarer til Kommissionens sikkerhedsforskrifter til beskyttelse af EU-klassificerede oplysninger (EUCI) og følsomme ikke-klassificerede oplysninger, som fastsat i Kommissionens afgørelse (EU, Euratom) 2015/443 og (EU, Euratom) 2015/444. Disse skal blandt andet omfatte bestemmelser om udveksling, behandling og opbevaring af disse oplysninger.

[42] Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

Artikel 41

Hjemstedsaftale og driftsvilkår

136. De nødvendige bestemmelser vedrørende de lokaler, der skal stilles til rådighed for Agenturet i værtsmedlemsstaten, og de faciliteter, der skal stilles til rådighed af værtsmedlemsstaten, samt de særlige regler, der skal finde anvendelse på den administrerende direktør, bestyrelsesmedlemmerne, Agenturets personale og deres familiemedlemmer i værtsmedlemsstaten, skal fastsættes i en hjemstedsaftale mellem Agenturet og den medlemsstat, hvor hovedsædet er beliggende; aftalen skal indgås med bestyrelsens godkendelse senest [2 år efter denne forordnings ikrafttræden].

137. Agenturets værtsmedlemsstat sikrer de bedst mulige betingelser for, at Agenturet kan fungere efter hensigten, herunder stedets tilgængelighed, tilbud om tilstrækkelige uddannelsesfaciliteter for personalets børn, tilstrækkelig adgang til arbejdsmarkedet, social sikring og lægebehandling for såvel børn som ægtefæller.

Artikel 42

Administrativ kontrol

Agenturets virke er underlagt ombudsmandens tilsyn i overensstemmelse med artikel 228 i TEUF.

AFSNIT III
RAMMEBESTEMMELSER FOR CYBERSIKKERHEDSCERTIFICERING

Artikel 43

Europæiske cybersikkerhedscertificeringsordninger

En europæisk cybersikkerhedscertificeringsordning skal attestere, at IKT-produkter og -tjenester, der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastlagte krav for så vidt angår deres evne til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, processer, tjenester og systemer.

Artikel 44

Forberedelse og vedtagelse af en europæisk cybersikkerhedscertificeringsordning

138. På anmodning fra Kommissionen skal ENISA udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning, som opfylder kravene i denne forordnings artikel 45, 46 og 47. Medlemsstaterne eller den europæiske cybersikkerhedscertificeringsgruppe ("gruppen"), der er nedsat ved artikel 53, kan foreslå Kommissionen, at der udarbejdes et forslag til en europæisk cybersikkerhedscertificeringsordning.

139. Under udarbejdelsen af forslaget til den i stk. 1 omhandlede ordning skal ENISA høre alle relevante interessenter og samarbejde tæt med gruppen. Gruppen yder ENISA den bistand og ekspertrådgivning, som ENISA har behov for i forbindelse med udarbejdelsen af forslaget til en ordning, herunder også udtalelser om nødvendigt.

140. ENISA fremsender forslaget til en europæisk cybersikkerhedscertificeringsordning udarbejdet i henhold til stk. 2 til Kommissionen.

141. Kommissionen kan på grundlag af den af ENISA foreslåede ordning vedtage gennemførelsesretsakter i overensstemmelse med artikel 55, stk. 2, vedrørende europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der opfylder kravene i denne forordnings artikel 45, 46 og 47.

142. ENISA skal drive en dedikeret hjemmeside, der giver oplysninger om og offentlig omtale af de europæiske cybersikkerhedscertificeringsordninger.

Artikel 45

Sikkerhedsmålene for de europæiske cybersikkerhedscertificeringsordninger

En europæisk cybersikkerhedscertificeringsordning skal være udformet således at den, alt efter relevans, tager hensyn til følgende sikkerhedsmål:

(e) beskyttelse af data, som lagres, overføres eller på anden måde behandles, mod utilsigtet eller uautoriseret lagring, behandling, adgang eller videregivelse

(f) beskyttelse af data, som lagres, overføres eller på anden måde behandles, mod utilsigtet eller uautoriseret ødelæggelse, utilsigtet tab eller ændring

(g) sikring af, at autoriserede personer, programmer eller maskiner udelukkende kan få adgang til data, tjenester eller funktioner, som de har adgangsret til

(h) registrering af, hvilke data, funktioner eller tjenester, der er blevet videregivet, på hvilket tidspunkt og til hvem

(i) sikring af, at det er muligt at kontrollere, hvilke data, tjenester og funktioner, der er tilgået eller anvendt, på hvilket tidspunkt og af hvem

(j) genetablering af tilgængelighed af og adgang til data, tjenester og funktioner hurtigt i tilfælde af fysiske eller tekniske hændelser

(k) sikring af, at IKT-produkter og -tjenester er forsynet med ajourført software og ikke indeholder kendte svagheder og har mekanismer til sikker opdatering af software.

Artikel 46

Tillidsniveauer for de europæiske cybersikkerhedscertificeringsordninger

143. En europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende tillidsniveauer: grundlæggende, betydeligt og/eller højt for IKT-produkter og -tjenester, der er certificeret under ordningen.

144. Tillidsniveauerne grundlæggende, betydeligt og højt skal opfylde følgende kriterier:

(l) tillidsniveauet "grundlæggende" henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en begrænset grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for et IKT-produkt eller en IKT-tjeneste, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for cybersikkerhedshændelser

(m) tillidsniveauet "betydeligt" henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en betydelig grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for et IKT-produkt eller en IKT-tjeneste, og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for cybersikkerhedshændelser betydeligt

(n) tillidsniveauet "højt" henviser til en attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en større grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for et IKT-produkt eller en IKT-tjeneste end attester med niveauet "betydelig", og som er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at forhindre cybersikkerhedshændelser.

Artikel 47

Elementer i europæiske cybersikkerhedscertificeringsordninger

145. En europæisk cybersikkerhedscertificeringsordning skal omfatte følgende elementer:

(o) certificeringens genstand og omfang, herunder typer eller kategorier af IKT-produkter og -tjenester, der er omfattet

(p) detaljeret specifikation af cybersikkerhedskravene, som de specifikke IKT-produkter og -tjenester evalueres i forhold til, f.eks. ved at henvise til europæiske eller internationale standarder eller tekniske specifikationer

(q) hvor det er relevant, et eller flere tillidsniveauer

(r) de specifikke evalueringskriterier og -metoder, der er anvendt, herunder typen af evaluering, for at påvise, at de specifikke mål omhandlet i artikel 45 er nået

(s) oplysninger til videresendelse til overensstemmelsesvurderingsorganer fra en ansøger, som er nødvendige med henblik på certificering

(t) hvis ordningen fastsætter mærker eller etiketter, omstændighederne under hvilke disse mærker eller etiketter kan anvendes

(u) hvis overvågningen er en del af ordningen, reglerne for overvågning af overensstemmelsen med attesternes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav

(v) betingelserne for udstedelse, bibeholdelse, forlængelse, udvidelse og indskrænkning af certificeringens omfang

(w) regler om følgerne af certificerede IKT-produkters og -tjenesters manglende overholdelse af certificeringskravene

(x) regler om, hvordan hidtil uopdagede cybersikkerhedssårbarheder i IKT-produkter og -tjenester skal indberettes og håndteres

(y) reglerne om overensstemmelsesvurderingsorganers opbevaring af optegnelser

(z) angivelse af nationale cybersikkerhedscertificeringsordninger, som dækker samme typer eller kategori af IKT-produkter og -tjenester

(æ) indholdet af den udstedte attest.

146. De krav, der er anført i ordningen, må ikke være i modstrid med eventuelle gældende retlige krav, herunder navnlig krav som følge af harmoniseret EU-lovgivning.

147. Hvis det er fastsat i en EU-retsakt, kan certificering i henhold til en europæisk cybersikkerhedscertificeringsordning anvendes til at påvise formodning om overensstemmelse med den pågældende retsakt.

148. I mangel af harmoniseret EU-lovgivning kan medlemsstaternes lovgivning også fastsætte, at en europæisk cybersikkerhedscertificeringsordning kan anvendes til at gå ud fra en formodning om overensstemmelse med retlige krav.

Artikel 48

Cybersikkerhedscertificering

149. IKT-produkter og -tjenester, der er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 44, skal antages at overholde kravene i en sådan ordning.

150. Certificeringen skal være frivillig, medmindre andet er fastsat i EU-retten.

151. En europæisk cybersikkerhedsattest i medfør af denne artikel skal udstedes af de overensstemmelsesvurderingsorganer, der er omhandlet i artikel 51, på grundlag af de kriterier, der fremgår af den europæiske cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 44.

152. Som en undtagelse fra stk. 3 kan det i behørigt begrundede tilfælde fastsættes i en europæisk cybersikkerhedscertificeringsordning, at en europæisk cybersikkerhedsattest, der fremgår af denne ordning, kun kan udstedes af et offentligt organ. Et sådant offentligt organ skal være en af følgende:

(ø) en national certificeringstilsynsmyndighed som omhandlet i artikel 50, stk. 1

(å) et organ, der er akkrediteret som overensstemmelsesvurderingsorgan i medfør af artikel 51, stk. 1

(aa) et organ, der er nedsat i henhold til en berørt medlemsstats lovgivning, retlige instrumenter eller andre officielle administrative procedurer, og som derudover opfylder kravene til organer, der certificerer produkter, processer og tjenester i henhold til ISO/IEC 17065:2012.

153. Den fysiske eller juridiske person, der indgiver sine IKT-produkter og -tjenester til certificeringsmekanismen, skal fremlægge alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, for det i artikel 51 omhandlede overensstemmelsesvurderingsorgan.

154. Attester udstedes for en periode på højst tre år og kan forlænges på samme betingelser, såfremt de relevante krav fortsat er opfyldt.

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

Artikel 49

Nationale cybersikkerhedscertificeringsordninger og -attester

156. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, skal ophøre med at have virkning fra det tidspunkt, der fastsættes i den gennemførelsesretsakt, som vedtages i medfør af artikel 44, stk. 4, jf. dog nærværende artikels stk. 3. Bestående nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT-produkter og -tjenester, der ikke er omfattet af en europæisk cybersikkerhedscertificeringsordning, fortsætter med at bestå.

157. Medlemsstaterne må ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der er omfattet af en gældende europæisk cybersikkerhedscertificeringsordning.

158. Eksisterende attester udstedt i henhold til en national cybersikkerhedscertificeringsordning forbliver gyldige indtil deres udløbsdato.

Artikel 50

Nationale certificeringstilsynsmyndigheder

159. Hver medlemsstat udpeger en national certificeringstilsynsmyndighed.

160. Hver medlemsstat underretter Kommissionen om den udpegede myndigheds identitet.

161. Hver national certificeringstilsynsmyndighed skal med hensyn til dens organisation, finansieringsbeslutninger, retlige struktur og beslutningstagning være uafhængig af de enheder, som den fører tilsyn med.

162. Medlemsstaterne sikrer, at de nationale certificeringstilsynsmyndigheder har tilstrækkelige ressourcer til at udøve deres beføjelser og udføre de opgaver, de er tillagt, på en effektiv og efficient måde.

163. Med henblik på en effektiv gennemførelse af forordningen er det hensigtsmæssigt, at disse myndigheder deltager i den europæiske cybersikkerhedscertificeringsgruppe, der er oprettet i henhold til artikel 53, på en aktiv, effektiv, efficient og sikker måde.

164. Nationale certificeringstilsynsmyndigheder skal:

(bb) overvåge og håndhæve anvendelsen af bestemmelserne i dette afsnit på nationalt niveau og føre tilsyn med, at de attester, der er udstedt af overensstemmelsesvurderingsorganer, som er etableret på deres respektive område, er i overensstemmelse med de krav, der er fastsat i dette afsnit og i den tilsvarende europæiske cybersikkerhedscertificeringsordning

(cc) overvåge og føre tilsyn med overensstemmelsesvurderingsorganers aktiviteter i forbindelse med denne forordning, herunder med hensyn til anmeldelsen af overensstemmelsesvurderingsorganer og de relaterede opgaver, der er fastsat i denne forordnings artikel 52

(dd) behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist

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

(ff) overvåge den relevante udvikling på cybersikkerhedscertificeringsområdet.

165. Hver national certificeringstilsynsmyndighed skal mindst have følgende beføjelser:

(gg) at kunne anmode overensstemmelsesvurderingsorganer og indehavere af en europæisk cybersikkerhedsattest om at forelægge alle oplysninger, som er nødvendige for udførelsen af dens opgaver

(hh) at kunne udføre undersøgelser i form af audit af overensstemmelsesvurderingsorganer og indehavere af en europæisk cybersikkerhedsattest med henblik på at verificere overholdelsen af bestemmelserne i afsnit III

(ii) at kunne træffende passende foranstaltninger, i overensstemmelse med national ret, til at sikre, at overensstemmelsesvurderingsorganer og indehavere af en europæisk cybersikkerhedsattest overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning

(jj) at kunne få adgang til alle lokaler hos overensstemmelsesvurderingsorganer og indehavere af en europæisk cybersikkerhedsattest med henblik på at udføre

undersøgelser i overensstemmelse med EU-retten eller medlemsstaternes retsplejeregler

(kk) at kunne tilbagekalde, i overensstemmelse med national ret, attester, som ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning

(ll) at kunne pålægge sanktioner, jf. artikel 54, i overensstemmelse med national ret, og at kunne kræve øjeblikkelig indstilling af overtrædelser af de forpligtelser, der er fastsat i denne forordning.

166. De nationale certificeringstilsynsmyndigheder skal samarbejde med hinanden og Kommissionen og navnlig udveksle oplysninger, dele erfaringer og god praksis med hensyn til cybersikkerhedscertificering og tekniske spørgsmål vedrørende cybersikkerhed af IKT-produkter og -tjenester.

Artikel 51
Overensstemmelsesvurderingsorganer

167. Overensstemmelsesvurderingsorganerne akkrediteres kun af det nationale akkrediteringsorgan, der er udpeget i henhold til forordning (EF) nr. 765/2008, hvis de opfylder kravene i bilaget til nærværende forordning.

168. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt overensstemmelsesvurderingsorganet opfylder de i denne artikel fastsatte krav. Akkrediteringsorganer tilbagekalder en akkreditering af et overensstemmelsesvurderingsorgan i henhold til stk. 1, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis foranstaltninger truffet af et overensstemmelsesvurderingsorgan er i modstrid med denne forordning.

Artikel 52
Anmeldelse

169. For hver europæisk cybersikkerhedscertificeringsordning, som vedtages i henhold artikel 44, underretter de nationale certificeringstilsynsmyndigheder Kommissionen om de akkrediterede overensstemmelsesvurderingsorganer, der er akkrediteret til at udstede attester på specifikke tillidsniveauer, jf. artikel 46, og hurtigst muligt om eventuelle senere ændringer heraf.

170. Et år efter ikrafttrædelsen af en europæisk cybersikkerhedscertificeringsordning offentliggør Kommissionen en liste over de anmeldte overensstemmelsesvurderingsorganer i Den Europæiske Unions Tidende.

171. Modtager Kommissionen en anmeldelse efter udløbet af den periode, der er fastsat i stk. 2, offentliggør den i Den Europæiske Unions Tidende ændringerne af den i stk. 2 omhandlede liste inden for to måneder fra datoen for modtagelsen af denne anmeldelse.

172. En national certificeringstilsynsmyndighed kan anmode Kommissionen om at fjerne et overensstemmelsesvurderingsorgan, der er anmeldt af den pågældende nationale certificeringstilsynsmyndighed, fra den i stk. 2 omhandlede liste. Kommissionen offentliggør i Den Europæiske Unions Tidende de tilsvarende ændringer af listen

inden for en måned fra datoen for modtagelsen af den nationale certificeringstilsynsmyndigheds anmodning.

173. Kommissionen kan ved hjælp af gennemførelsesretsakter fastlægge vilkår, formater og procedurer for anmeldelserne omhandlet i stk. 1. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren omhandlet i artikel 55, stk. 2.

Artikel 53
Den europæiske cybersikkerhedscertificeringsgruppe

174. Den europæiske cybersikkerhedscertificeringsgruppe (gruppen") oprettes.

175. Gruppen sammensættes af nationale certificeringstilsynsmyndigheder Myndighederne repræsenteres ved lederne af eller andre højtstående repræsentanter for de nationale certificeringstilsynsmyndigheder.

176. Gruppen har følgende opgaver:

(mm) at rådgive og bistå Kommissionen i dens arbejde med at sikre en konsekvent gennemførelse og anvendelse af dette afsnit, herunder navnlig hvad angår cybersikkerhedscertificeringspolitik, samordning af politiske tiltag og udarbejdelse af europæiske cybersikkerhedscertificeringsordninger

(nn) at bistå, rådgive og samarbejde med ENISA i forbindelse med udarbejdelse af forslag til ordninger i overensstemmelse med artikel 44

(oo) at foreslå Kommissionen, at den anmoder Agenturet om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning i overensstemmelse med artikel 44

(pp) at vedtage udtalelser til Kommissionen vedrørende bibeholdelse og revision af eksisterende europæiske cybersikkerhedscertificeringsordninger

(qq) at undersøge de relevante udviklinger inden for cybersikkerhedscertificering og udveksle god praksis om cybersikkerhedscertificeringsordninger

(rr) at fremme samarbejdet mellem nationale certificeringstilsynsmyndigheder i medfør af dette afsnit gennem udveksling af oplysninger, herunder navnlig ved at indføre metoder til effektiv udveksling af oplysninger vedrørende cybersikkerhedscertificeringsanliggender.

177. Kommissionen varetager formandskabet og sekretariatsfunktionen for gruppen med bistand fra ENISA, som fastsat i artikel 8, litra a).

Artikel 54
Sanktioner

Medlemsstaterne fastsætter regler for, hvilke sanktioner der skal anvendes ved overtrædelse af bestemmelserne i dette afsnit og de europæiske cybersikkerhedscertificeringsordninger, og træffer alle nødvendige foranstaltninger for at sikre, at de iværksættes. Sanktionerne skal være effektive, stå i rimeligt forhold til overtrædelsen og have afskrækkende virkning. Medlemsstaterne giver [senest den ... /hurtigst muligt] Kommissionen meddelelse om disse bestemmelser og foranstaltninger og meddeler omgående senere ændringer af betydning for bestemmelserne og foranstaltningerne.

AFSNIT IV
AFSLUTTENDE BESTEMMELSER

Artikel 55
Udvalgsprocedure

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

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

Artikel 56
Evaluering og revision

180. Senest fem år efter den dato, der er omhandlet i artikel 58, og hvert femte år derefter vurderer Kommissionen virkning, effektivitet og efficiens af Agenturets arbejde og dets arbejdsmetoder samt behovet for at ændre Agenturets mandat og de finansielle virkninger af en sådan ændring. Evalueringen skal tage hensyn til enhver tilbagemelding til Agenturet som reaktion på dets aktiviteter. Hvis Kommissionen finder, at der ikke længere er grund til at videreføre Agenturet med de mål, det mandat og de opgaver, Agenturet er tillagt, kan den foreslå, at denne forordning ændres med hensyn til de bestemmelser, der vedrører Agenturet.

181. Evalueringen skal også vurdere virkning, effektivitet og efficiens af bestemmelserne i afsnit III med hensyn til målene om at sikre et tilstrækkeligt niveau af cybersikkerhed for IKT-produkter og -tjenester i EU og forbedre det indre markeds funktion.

182. Kommissionen sender evalueringsrapporten og dens konklusioner til Europa-Parlamentet, Rådet og bestyrelsen. Resultaterne i evalueringsrapporten offentliggøres.

Artikel 57
Ophævelse og afløsning

183. Forordning (EF) nr. 526/2013 ophæves pr. [...].

184. Henvisninger til forordning (EF) nr. 526/2013 og til ENISA betragtes som henvisninger til nærværende forordning og til Agenturet.

185. Agenturet afløser det agentur, der blev oprettet ved forordning (EF) nr. 526/2013, med hensyn til ethvert ejendomsforhold, enhver aftale, enhver retlig forpligtelse, enhver ansættelseskontrakt, enhver økonomisk forpligtelse og ethvert økonomisk ansvar. Alle eksisterende beslutninger truffet af bestyrelsen og forretningsudvalget forbliver gyldige, forudsat at de ikke er i strid med bestemmelserne i denne forordning.

186. Agenturet oprettes for en ubegrænset periode fra den [...].

187. Den administrerende direktør, der er udpeget i henhold til artikel 24 i forordning (EF) nr. 526/2013, er Agenturets administrerende direktør for den resterende del af dennes embedsperiode.

188. Bestyrelsens medlemmer og deres stedfortrædere, der er udpeget i henhold til artikel 6 forordning (EF) nr. 526/2013, er medlemmerne og deres stedfortrædere i Agenturets bestyrelse for den resterende del af deres embedsperiode.

Artikel 58

Ikrafttræden

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

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

Udfærdiget i Bruxelles, den […].

For Europa-Parlamentet	*På Rådets vegne*
Formand	*Formand*

FINANSIERINGSOVERSIGT

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til Europa-Parlamentets og Rådets forordning om "EU's Agentur for Cybersikkerhed" (ENISA) og om ophævelse af forordning (EU) nr. 526/2013 og om sikkerhedscertificering af informations- og kommunikationsteknologi ("forordningen om cybersikkerhed").

1.2. Berørt(e) politikområde(r)

Politikområde: 09 - Kommunikationsnet, indhold og teknologi

Aktivitet: 09.02 Det digitale indre marked

1.3. Forslagets/initiativets art

☒ Forslaget/initiativet vedrører en **ny foranstaltning (Afsnit III - Certificering)**

☐ Forslaget/initiativet vedrører en **ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[43]

☒Forslaget/initiativet vedrører en **forlængelse af en eksisterende foranstaltning (Afsnit II - ENISA's mandat)**

☐ Forslaget/initiativet vedrører **omlægning af en foranstaltning til en ny foranstaltning**

1.4. Mål

1.4.1. Det eller de af Kommissionens flerårige strategiske mål, som forslaget/initiativet vedrører

1. Øge modstandsdygtigheden i medlemsstaterne, virksomhederne og EU som helhed

2. Sikre den korrekte funktion af EU's indre marked for IKT-produkter og -tjenester

3. Øge den globale konkurrenceevne for de EU-virksomheder, der opererer inden for IKT

4. Tilnærme de af medlemsstaternes love og administrative bestemmelser, der vedrører cybersikkerhed

1.4.2. Specifikke mål

Med de generelle mål for øje har retsakten i en bredere sammenhæng med den reviderede strategi for cybersikkerhed gennem at afgrænse anvendelsesområdet og ENISA's mandat samt etableringen af en europæisk ramme for certificering af IKT-produkter og -tjenester til hensigt at nå følgende specifikke mål:

1. Øgede **kapaciteter og beredskab** i medlemsstaterne og virksomhederne
2. Forbedret **samarbejde og samordning** mellem medlemsstaterne og EU's institutioner, agenturer og organer
3. Øget **kapacitet på EU-niveau til at supplere medlemsstaternes indsats**, navnlig i tilfælde af grænseoverskridende cyberkriser
4. Øget **oplysning** til borgere og virksomhederne om cybersikkerhed
5. Styrkelse af tilliden til det digitale indre marked og digital innovation gennem øget overordnet **gennemsigtighed af cybersikkerhedstillidsniveauet**[44] for IKT-

[43] Jf. finansforordningens artikel 54, stk. 2, litra a) hhv. b).

produkter og -tjenester

ENISA vil bidrage til at nå ovennævnte mål gennem:

Øget støtte til politikudformning – yde vejledning og rådgivning til Kommissionen og medlemsstaterne med sigte på at ajourføre og udvikle holistiske normative rammer for cybersikkerhed samt sektorspecifikke politikker og initiativer, der involverer cybersikkerhedsanliggender, bidrage til arbejdet i samarbejdsgruppen (artikel 11 i direktiv (EU) 2016/1148) ved at stille ekspertise og bistand til rådighed, støtte udviklingen og gennemførelsen af politikker inden for elektronisk identifikation og tillidstjenester, fremme udveksling af bedste praksis blandt kompetente myndigheder.

Øget støtte til kapacitetsopbygning – yde støtte til medlemsstaterne, Unions institutioner, organer, kontorer og agenturer til at udvikle og forbedre forebyggelse, opdagelse, analyse og kapaciteten til at reagere på [cybersikkerheds]problemer og hændelser, efter anmodning bistå medlemsstaterne med at udvikle nationale CSIRT'er og nationale cybersikkerhedsstrategier, bistå Unionens institutioner ved udvikling og revision af Unionens strategier for cybersikkerhed, udbyde cybersikkerhedsuddannelsesforløb, gennem samarbejdsgruppen bistå medlemsstaterne med udveksling af bedste praksis, fremme oprettelsen af centre for informationsudveksling og analyse (ISAC'er).

Operationelt samarbejde og krisestyringsstøtte – støtte samarbejde mellem de kompetente offentlige organer og mellem interessenter ved at etablere et systematisk samarbejde med Unionens institutioner, organer, kontorer og agenturer, som håndterer cybersikkerhed, cyberkriminalitet og beskyttelsen af privatlivets fred og personoplysninger, varetage sekretariatsfunktionen for CSIRT-netværket (artikel 12, stk. 2, i direktiv (EU) 2016/1148) samt bidrage til det operationelle samarbejde i netværket ved i samarbejde med CERT-EU at yde støtte til medlemsstaterne på deres anmodning, tilrettelægge regelmæssige cybersikkerhedsøvelser, bidrage til at udvikle en samarbejdsorienteret respons på væsentlige grænseoverskridende cybersikkerhedshændelser eller -kriser, i samarbejde med CSIRT-netværket gennemføre efterfølgende tekniske undersøgelser af betydningsfulde hændelser og udstede opfølgende henstillinger.

Markedsrelaterede opgaver (standardisering, certificering) – udføre en række funktioner, som specifikt støtter det indre marked: cybersikkerhedsmarkedsobservatorium, ved at analysere de relevante udviklingstendenser på cybersikkerhedsmarkedet med sigte på at matche udbud og efterspørgsel bedre, støtte og fremme udviklingen og gennemførelsen af Unionens politik vedrørende cybersikkerhedscertificering af IKT-produkter og -tjenester ved at udarbejde forslag til europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, varetage sekretariatsfunktionen for Unionens cybersikkerhedscertificeringsgruppe, fremlægge retningslinjer og god praksis vedrørende sikkerhedskrav til IKT-produkter og -tjenester i samarbejde med de nationale certificeringstilsynsmyndigheder og branchen. **Bedre viden og information samt støtte til oplysningsindsats** – yde bistand og rådgivning til Kommissionen og medlemsstaterne med henblik på at nå et højt niveau af viden i EU om spørgsmål vedrørende net- og informationssikkerhed og at formidle denne viden til de berørte parter i erhvervslivet. Det forudsætter også via en særlig webportal samle, organisere og offentliggøre oplysninger om sikkerhed af net- og informationssystemer

[44] Gennemsigtighed af cybersikkerhedstillidsniveauet betyder, at brugerne får tilstrækkelige oplysninger om cybersikkerhedsegenskaber til objektivt at kunne bedømme sikkerhedsniveauet for et givet IKT-produkt, -tjeneste eller -proces.

[cybersikkerhed]. Et andet vigtigt element er oplysningsaktiviteter og informationskampagner om cybersikkerhedsrisici rettet mod den brede offentlighed.

Bedre støtte til forskning og innovation – yde rådgivning om forskningsbehov og fastlæggelse af prioriteter inden for cybersikkerhed.

Støtte til internationalt samarbejde – støtte til Unionens indsats for at samarbejde med tredjelande og internationale organisationer for at fremme internationalt samarbejde om cybersikkerhed.

CERTIFICERING

En ramme for certificering vil bidrage til at nå målene ved at øge den overordnede gennemsigtighed af cybersikkerhedstillidsniveauet[45]for IKT-produkter og -tjenester og dermed styrke tilliden til det digitale indre marked og digital innovation. Det vil også hjælpe med at undgå en opsplitning af certificeringsordningerne i EU og dermed forbundne sikkerhedskrav og evalueringskriterier på tværs af medlemsstater og sektorer.

1.4.3. Forventede resultater og virkninger

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgruppen.

Et styrket ENISA (støttekapaciteter, forebyggelse, samarbejde og sikkerhedsbevidsthed på EU-plan og derfor udformet til at øge EU's samlede cybermodstandsdygtighed) og støtte til EU's ramme for certificering af IKT-produkter og -tjenester forventes at få følgende virkninger (ikkeudtømmende liste):

Generelle virkninger:

- Generel positiv virkning på det indre marked takket være mindre opsplitning af markedet og opbygning af tillid til digitale teknologier gennem bedre samarbejde, mere harmoniseret tilgang EU's cybersikkerhedspolitikker og øget kapacitet på EU-plan. Det burde give en positiv økonomisk virkning ved at medvirke til at nedbringe cybersikkerhedshændelser og cyberkriminalitet, for hvilke den anslåede økonomisk virkning i Unionen er 0,41 % af EU's BNP (dvs. ca. 55 mia. EUR).

Konkrete resultater

Øgede cybersikkerhedskapaciteter og -beredskab i medlemsstaterne og virksomhederne

- Forbedrede cybersikkerhedskapaciteter og -beredskab i medlemsstaterne (takket være langsigtet strategisk analyse af cybertrusler og -hændelser, vejledning og rapporter, formidling af ekspertise og god praksis, uddannelse og uddannelsesmateriale til rådighed, styrkede Cyber Europe-øvelser).

- Forbedret kapacitet hos private aktører takket være støtte til etableringen af centre for informationsudveksling og analyse (ISAC'er) i forskellige sektorer.

- Forbedret cybersikkerhedsberedskab i EU og medlemsstaterne takket være tilgængeligheden af gennemøvede og aftalte planer i tilfælde af væsentlige grænseoverskridende cybersikkerhedshændelser, som gennemprøves i Cyber Europe-øvelser.

[45] Gennemsigtighed af cybersikkerhedstillidsniveauet betyder, at brugerne får tilstrækkelige oplysninger om cybersikkerhedsegenskaber til objektivt at kunne bedømme sikkerhedsniveauet for et givet IKT-produkt, -tjeneste eller -proces.

Forbedret samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer

- Forbedret samarbejde både inden for og mellem den offentlige og den private sektor

- Forbedret sammenhæng i tilgangen til NIS-direktivets gennemførelse på tværs af grænser og sektorer

- Forbedret samarbejde inden for certificering takket være en institutionel ramme, som gør det muligt at udvikle europæiske cybersikkerhedscertificeringsordninger, og udvikling af en fælles politik på dette område.

Øget kapacitet på EU-plan til at supplere medlemsstaternes indsats

- Forbedret "operationel EU-kapacitet" til at supplere medlemsstaternes indsats og støtte dem efter anmodning og i forbindelse med begrænsede og forud fastlagte ydelser. Dette forventes at have en positiv indvirkning på, hvorvidt det lykkes at forebygge, opdage og reagere på hændelser, både på medlemsstatsniveau og EU-niveau.

Øget oplysning til borgere og virksomhederne om cybersikkerhed

- Forbedret generelt oplysningsniveau for borgere og virksomheder om cybersikkerhed

- Forbedret evne til at træffe informerede købsbeslutninger i forbindelse med IKT-produkter og -tjenester takket være cybersikkerhedscertificering.

Styrket tillid til det digitale indre marked og digital innovation gennem øget gennemsigtighed af cybersikkerhedstillidsniveauet for IKT-produkter og -tjenester

- Øget gennemsigtighed af cybersikkerhedstillidsniveauet[46] for IKT-produkter og -tjenester takket være enklere procedurer for sikkerhedscertificering via en EU-ramme.

- Forbedret tillidsniveau for IKT-produkters og -tjenesters sikkerhedsegenskaber

- Øget udbredelse af sikkerhedscertificering fremmet af forenklede procedurer, mindskede omkostninger og forventning om EU-dækkende forretningsmuligheder, der ikke hæmmes af markedsopsplitning

- Forbedret konkurrenceevne inden for EU's cybersikkerhedsmarked på grund af lavere omkostninger og mindre administrativ byrde for SMV og fjernelse af potentielle hindringer for markedsadgang som følge af mange nationale certificeringsordninger.

Andet

- Der forventes ingen væsentlige miljømæssige virkninger for nogen af målene.

- Hvad angår EU-budgettet, kan der forventes effektivitetsgevinster som følge af øget samarbejde og koordinering af aktiviteter mellem EU's institutioner, agenturer og -organer.

1.4.4. Virknings- og resultatindikatorer

Angiv indikatorerne til kontrol af forslagets/initiativets gennemførelse.

(ss)

[46] Gennemsigtighed af cybersikkerhedstillidsniveauet betyder, at brugerne får tilstrækkelige oplysninger om cybersikkerhedsegenskaber til objektivt at kunne bedømme sikkerhedsniveauet for et givet IKT-produkt, -tjeneste eller -proces.

Mål: Øgede kapaciteter og beredskab i medlemsstaterne og virksomhederne

- Antal uddannelsesforløb organiseret af ENISA
- Geografisk dækning (antallet af lande og områder) af den direkte bistand fra ENISA
- Beredskabsniveau nået af medlemsstaterne i form af CSIRT-modenhed og tilsyn med cybersikkerhedsrelaterede lovtiltag
- Antal EU-dækkende god praksis for kritiske infrastrukturer formidlet af ENISA
- Antal EU-dækkende god praksis for SMV formidlet af ENISA
- ENISA's offentliggørelse af den årlige strategiske analyse af cybertrusler og -hændelser for at identificere nye tendenser
- ENISA's jævnlige bidrag til de europæiske standardiseringsorganisationers (ESO'er) cybersikkerhedsarbejdsgrupper.

Mål: Forbedret samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer

- Antallet af medlemsstater, der har fulgt ENISA's anbefalinger i deres politiske beslutningsproces
- Antallet af EU-institutioner, -agenturer og -organer, der har fulgt ENISA's anbefalinger i deres politiske beslutningsproces
- Jævnlig gennemførelse af CSIRT-netværkets arbejdsprogram og velfungerende IT-infrastruktur og kommunikationskanaler i CSIRT-netværket
- Antal tekniske rapporter stillet til rådighed for og anvendt af samarbejdsgruppen
- Konsekvent tilgang til NIS-direktivets gennemførelse på tværs af grænser og sektorer
- Antal lovpligtige overensstemmelsesvurderinger udført af ENISA
- Antal ISAC'er på plads i forskellige sektorer, herunder navnlig for kritiske infrastrukturer
- Oprettelse og regelmæssig brug af informationsplatform, der formidler cybersikkerhedsinformation fra EU's institutioner, agenturer og organer
- Regelmæssige bidrag til forberedelsen af EU's forsknings- og innovationsarbejdsprogrammer
- Samarbejdsaftale mellem ENISA, EC3 og CERT-EU på plads
- Antallet af certificeringsordninger inkluderet og udviklet inden for rammen.

Mål: Øget kapacitet på EU-niveau til at supplere medlemsstaternes indsats, navnlig i tilfælde af grænseoverskridende cyberkriser:

- ENISA's offentliggørelse af den årlige strategiske analyse af cybertrusler og -hændelser for at identificere nye tendenser
- ENISA's offentliggørelse af aggregerede oplysninger om hændelser indberettet under NIS-direktivet
- Antallet af fælleseuropæiske øvelser koordineret af Agenturet og antallet af involverede medlemsstater og organisationer

- Antal anmodninger om støtte til krisehåndtering fra medlemsstaterne til ENISA og antal anmodninger imødekommet af Agenturet
- Antal analyser af sårbarhed, spor (artefacts) og hændelser udført af ENISA i samarbejde med CERT-EU
- Tilgængelighed af EU-dækkende situationsrapporter baseret på oplysninger, som ENISA har stillet til rådighed for medlemsstaterne og andre enheder i tilfælde af væsentlige grænseoverskridende cyberhændelser.

Mål: Øget oplysning til borgere og virksomhederne om cybersikkerhed:

- Jævnlig gennemførelse af EU-dækkende og nationale oplysningskampagner og regelmæssig ajourføring af emnerne i henhold til nye læringsbehov
- Øget bevidsthed om cybersikkerhed blandt EU-borgerne
- Jævnlig afholdelse af en quiz om cybersikkerhedsviden og øgning over tid af andelen af korrekte svar
- Jævnlig offentliggørelse af god praksis inden for cybersikkerhed og cyberhygiejne rettet mod ansatte og organisationer.

Mål: Styrkelse af tilliden til det digitale indre marked og digital innovation gennem øget overordnet gennemsigtighed af cybersikkerhedstillidsniveauet[47] for IKT-produkter og -tjenester:

- Antallet af ordninger, der overholder EU's ramme
- Mindskede omkostninger for en IKT-sikkerhedsattest
- Antallet af overensstemmelsesvurderingsorganer, der er specialiseret i IKT-certificering på tværs af medlemsstaterne
- Oprettelsen af den europæiske cybersikkerhedscertificeringsgruppe og jævnlig afholdelse af møder
- Retningslinjer for certificering i henhold til EU's ramme på plads
- Jævnlig offentliggørelse af analyser af de vigtigste tendenser på cybersikkerhedsmarkedet i EU
- Antallet af IKT-produkter og -tjenester certificeret i henhold til reglerne i den europæiske ramme for IKT-sikkerhedscertificering
- Øget antal slutbrugere, som er bekendt med IKT-produkters og -tjenesters sikkerhedsfunktioner.

(tt)

1.4.5. Behov, der skal opfyldes på kort eller lang sigt

På baggrund af lovkravene og det hurtigt skiftende cybersikkerhedstrusselsmiljø må ENISA's mandat revideres med henblik på at fastsætte et nyt sæt opgaver og funktioner med sigte på effektiv og efficient støtte til medlemsstaternes, EU-institutionernes og andre interessenters indsats for et sikkert cyberspace i Den Europæiske Union. Det foreslåede omfang af mandatet afgrænses, idet de områder styrkes, hvor Agenturet har vist en klar merværdi, og der tilføjes de nye områder, hvor der er brug for støtte på grund af de nye

[47] Gennemsigtighed af cybersikkerhedstillidsniveauet betyder, at brugerne får tilstrækkelige oplysninger om cybersikkerhedsegenskaber til objektivt at kunne bedømme sikkerhedsniveauet for et givet IKT-produkt, -tjeneste eller -proces.

politiske prioriteter og instrumenter, navnlig NIS-direktivet, revisionen af EU's strategi for cybersikkerhed, den kommende plan for EU's cybersikkerhedssamarbejde i krisesituationer og IKT-sikkerhedscertificering. Det nye foreslåede mandat søger at give Agenturet en stærkere og mere central rolle, navnlig ved også at støtte medlemsstaterne mere aktivt for at modvirke særlige trusler på en mere aktiv måde (operationel kapacitet) og ved at blive et ekspertisecenter, som støtter medlemsstaterne og Kommissionen i forbindelse med cybersikkerhedscertificering.

Samtidig opstilles med forslaget en europæisk ramme for cybersikkerhedscertificering ("rammen") for IKT-produkter og -tjenester, og det præciserer de væsentlige funktioner og opgaver for ENISA inden for cybersikkerhedscertificering. Rammen fastsætter fælles bestemmelser og procedurer, som gør det muligt at indføre EU-dækkende cybersikkerhedscertificeringsordninger for specifikke IKT-produkter/tjenester eller cybersikkerhedsrisici. Oprettelsen af europæiske cybersikkerhedscertificeringsordninger i overensstemmelse med rammen vil sørge for, at attester udstedt i henhold til sådanne ordninger er gyldige og anerkendes i alle medlemsstater og afhjælpe den aktuelle markedsopsplitning.

1.4.6. Merværdien ved en indsats fra EU's side

Cybersikkerhed er et virkelig globalt anliggende, som i sagens natur er grænseoverskridende og i stigende grad tværsektorielt på grund af den indbyrdes afhængighed mellem net- og informationssystemer. Antallet, kompleksiteten og omfanget af cybersikkerhedshændelser og deres indvirkning på økonomien og samfundet vokser med tiden og forventes at vokse yderligere i takt med den teknologiske udvikling, f.eks. udbredelsen af tingenes Internet. Det indebærer, at der er behov for en øget fælles indsats fra medlemsstaterne, EU's institutioner og private interessenter for at imødegå cybersikkerhedstrusler, der ikke kan ikke forventes at mindskes i fremtiden.

Siden oprettelsen i 2004 har ENISA haft til formål at fremme samarbejdet mellem medlemsstaterne og interessenterne inden for net- og informationssikkerhed, herunder støtte til offentligt-privat samarbejde. Denne støtte til samarbejde inkluderede det tekniske arbejde med at skabe et EU-dækkende trusselsbillede, etableringen af ekspertgrupper og tilrettelæggelse af fælleseuropæiske cyberhændelses- og krisestyringsøvelser for offentlige og private sektorer (navnlig "Cyber Europe"). NIS-direktivet tillagde ENISA yderligere opgaver, herunder varetagelse af sekretariatsfunktionen for CSIRT-netværket til operationelt samarbejde mellem medlemsstaterne.

Merværdien af en indsats på EU-plan, herunder navnlig for at styrke samarbejdet mellem medlemsstaterne, men også mellem net- og informationssikkerhedsfællesskaberne, blev anerkendt i Rådets konklusioner fra 2016[48] og fremgår også klart af evalueringen af ENISA fra 2017, som viser, at Agenturets merværdi først og fremmest ligger i dets evne til at styrke samarbejdet mellem disse interessenter. Der findes ingen anden aktør på EU-plan, der støtter samarbejdet mellem det samme udsnit af interessenter på net- og informationssikkerhedsområdet.

ENISA's merværdi ved at samle cybersikkerhedsfællesskaber og interessenter er også aktuel inden for certificering. Stigningen i cyberkriminalitet og sikkerhedstrusler har ført til nye nationale initiativer, som fastsætter strenge cybersikkerheds- og certificeringskrav for IKT-komponenter, der anvendes i traditionelle infrastrukturer. Skønt de er vigtige,

[48] Rådets konklusioner om styrkelse af Europas modstandsdygtighed over for cyberangreb og fremme af en konkurrencedygtig og innovativ cybersikkerhedsindustri – 15. november 2016.

indebærer initiativerne en risiko for, at det indre marked fragmenteres, og at der opstår interoperabilitetsproblemer. En sælger af IKT-udstyr kan være nødt til at gennemgå forskellige certificeringsprocedurer for at kunne sælge i flere medlemsstater. De aktuelle certificeringsordningers manglende effektivitet/store omkostninger kan næppe afhjælpes uden et EU-tiltag. Hvis der ikke gribes ind, er det meget sandsynligt, at markedsfragmenteringen vil tiltage på kort og mellemlangt sigt (de næste 5-10 år) med fremkomsten af nye certificeringsordninger. Manglen på koordinering og interoperabilitet på tværs af sådanne ordninger er et element, som hæmmer potentialet i det digitale indre marked. Dette underbygger merværdien ved at opstille en europæisk ramme for cybersikkerhedscertificering af IKT-produkter og -tjenester gennem at skabe de rette betingelser for effektivt at tackle problemet med sameksistensen af flere certificeringsprocedurer i forskellige medlemsstater og mindske certificeringsomkostningerne og dermed gøre certificering i EU som helhed mere attraktivt, set fra et kommercielt og konkurrencemæssigt synspunkt.

1.4.7. Erfaringer fra lignende foranstaltninger

I overensstemmelse med ENISA's retsgrundlag har Kommissionen gennemført en evaluering af Agenturet, som omfattede en uafhængig undersøgelse og en offentlig høring. Evalueringen kom til den konklusion, at ENISA's målsætninger stadig er relevante i dag. I en kontekst med hurtig teknologisk udvikling og skiftende trusler og med et væsentligt behov for øget net- og informationssikkerhed i EU, er det nødvendigt at have teknisk ekspertise til rådighed om udviklingen af net- og informationssikkerhed. Der må opbygges kapacitet i medlemsstaterne til at forstå og imødegå trusler, og interessenterne må samarbejde på tværs af temaområder og institutioner.

Agenturet har med succes bidraget til at forbedre net- og informationssikkerheden i EU ved at tilbyde kapacitetsopbygning i 28 medlemsstater, ved at forbedre samarbejdet mellem medlemsstater og interessenter på net- og informationssikkerhedsområdet og ved at stille ekspertise til rådighed, opbygge fællesskaber og støtte politikker

ENISA har gjort en forskel, i hvert fald i et vist omfang, inden for det omfattende net- og informationssikkerhedsområde, men har ikke fuldt ud formået at udvikle et stærkt "brand" og opnå tilstrækkelig synlighed til at blive anerkendt som "det" europæiske ekspertisecenter. Årsagen hertil ligger i ENISA's brede mandat, idet der ikke blev tildelt tilsvarende tilstrækkelige ressourcer. Derudover er ENISA stadig det eneste EU-agentur med et tidsbegrænset mandat, hvilket begrænser dets evne til at udvikle en langsigtet vision og støtte sine interessenter på en bæredygtig måde. Dette er også i modstrid med bestemmelserne i NIS-direktivet, som overdrager opgaver til ENISA, som ikke har nogen slutdato.

Der findes i øjeblikket ingen europæisk ramme for cybersikkerhedscertificering af IKT-produkter og -tjenester. Stigningen i cyberkriminalitet og sikkerhedstrusler har dog ført til fremkomst af nationale initiativer, som giver en risiko for en fragmentering af det indre marked.

1.4.8. Sammenhæng med andre relevante instrumenter og eventuel synergivirkning

Initiativet hænger nøje sammen med de eksisterende politikker, herunder navnlig for det indre marked. Det er udformet i overensstemmelse med den overordnede tilgang til cybersikkerhed, som den er defineret ved revisionen af strategien for det digitale indre marked, med sigte på at supplere et omfattende sæt af foranstaltninger såsom revisionen af EU's strategi for cybersikkerhed, planen for cyberkrisesamarbejde og initiativerne til

bekæmpelse af cyberkriminalitet. Det vil sikre overensstemmelse med og bygge på bestemmelserne i den eksisterende lovgivning om cybersikkerhed, herunder navnlig NIS-direktivet, med henblik på at fremme EU's cybermodstandsdygtighed ved hjælp af øget kapacitet, samarbejde, krisestyring og kendskab til cybersikkerhed.

De foreslåede certificeringsforanstaltninger bør afhjælpe den potentielle opsplitning som følge af eksisterende og nye nationale certificeringsordninger og dermed bidrage til udviklingen af det digitale indre marked. Initiativet supplerer og støtter også gennemførelsen af NIS-direktivet ved at give de af direktivet omfattede virksomheder et redskab til at påvise overensstemmelse med NIS-kravene i hele Unionen.

Den europæiske ramme for cybersikkerhedscertificering af IKT-produkter og -tjenester berører ikke den generelle forordning om databeskyttelse[49] og navnlig ikke de relevante bestemmelser om certificering[50], da de finder anvendelse på sikkerheden i forbindelse med behandlingen af personoplysninger. Sidst men ikke mindst bør ordningerne foreslået inden for den kommende europæiske ramme bygge på internationale standarder, så det undgås at skabe handelshindringer og for at sikre overensstemmelsen med internationale initiativer.

[49] 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).

[50] F.eks. artikel 42 (certificering) og 43 (Certificeringsorganer) samt artikel 57, 58 og 70 om henholdsvis de nationale tilsynsmyndigheders relevante opgaver og beføjelser og Databeskyttelsesrådets opgaver.

1.5. Varighed og finansielle virkninger

☐ Forslag/initiativ af **begrænset varighed**

– ☐ Forslag/initiativ gældende fra [DD/MM]ÅÅÅÅ til [DD/MM]ÅÅÅÅ

– ☐ Finansielle virkninger fra ÅÅÅÅ til ÅÅÅÅ

☒ Forslag/initiativ af **ubegrænset varighed**

– Iværksættelse med en indkøringsperiode fra 2019 til 2020

– derefter gennemførelse i fuldt omfang

1.6. Påtænkt(e) forvaltningsmetode(r)[51]

☒ **Direkte forvaltning** ved Kommissionen (Afsnit III – Certificering)

– ☐ forvaltningsorganer

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☒ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

☐ internationale organisationer og deres organer (angives nærmere)

☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

☒ de organer, der er omhandlet i artikel 208 og 209 (Afsnit II - ENISA)

☐ offentligretlige organer

☐ privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som stiller tilstrækkelige finansielle garantier

☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er udpeget i den relevante basisretsakt

Bemærkninger

Forordningen omfatter: - Afsnit II i den foreslåede forordning gennemgår mandatet for Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) og giver det en vigtig rolle i forbindelse med certificering, medens - Afsnit III indfører en ramme for oprettelse af europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, hvor ENISA spiller en afgørende rolle.

[51] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

Angiv hyppighed og betingelser.

Overvågningen vil begynde lige efter vedtagelsen af retsakten og vil være fokuseret på anvendelsen. Kommissionen vil afholde møder med ENISA, medlemsstaternes repræsentanter (f.eks. ekspertgruppe) og de relevante interessenter for at lette gennemførelsen af reglerne for certificering såsom oprettelse af bestyrelsen.

Den første evaluering bør finde sted 5 år efter retsaktens ikrafttræden, såfremt der er tilstrækkelige data til rådighed. Der er inkluderet en udtrykkelig evaluerings- og revisionsklausul [artikel XXX], som pålægger Kommissionen af foretage en uafhængig evaluering. Kommissionen aflægger efterfølgende beretning til Europa-Parlamentet og Rådet om evalueringen, i givet fald ledsaget af et forslag til revision, for at måle virkningen af forordningen og dens merværdi. Yderligere evalueringer bør foretages hvert femte år. Kommissionens evalueringsmetode med henblik på bedre regulering anvendes. Evalueringerne gennemføres ved hjælp af målrettede ekspertdrøftelser, undersøgelser og omfattende høringer af interessenter.

ENISA's administrerende direktør bør forelægge bestyrelsen en efterfølgende evaluering af ENISA's aktiviteter hvert andet år. Agenturet bør også udarbejde en handlingsplan, der følger op på konklusionerne på efterfølgende evalueringer, og aflægge en statusrapport til Kommissionen hvert andet år. Bestyrelsen bør være ansvarlig for passende opfølgning af disse konklusioner.

Påståede tilfælde af dårlig administration i forbindelse med Agenturets aktiviteter er underlagt Den Europæiske Ombudsmands undersøgelser i overensstemmelse med traktatens artikel 228.

Datakilderne i forbindelse med den planlagte overvågning vil hovedsagelig være ENISA, den europæiske cybercertificeringsgruppe, samarbejdsgruppen, CSIRT-netværket og medlemsstaternes myndigheder. Ud over de data, der indsamles fra rapporterne (herunder de årlige aktivitetsrapporter) fra ENISA, den europæiske cybercertificeringsgruppe, samarbejdsgruppen og CSIRT-netværket, vil der blive anvendt særlige dataindsamlingsværktøjer efter behov (f.eks. rundspørger til nationale myndigheder, Eurobarometer og rapporter fra kampagnen "Cybersecurity Month" og de fælleseuropæiske øvelser).

2.2. Forvaltnings- og kontrolsystem

2.2.1. Konstaterede risici

De konstaterede risici er begrænsede: Der eksisterer allerede et EU-agentur og dets mandat afgrænses, idet de områder styrkes, hvor Agenturet har vist en klar merværdi, og der tilføjes de nye områder, hvor der er brug for støtte på grund af de nye politiske prioriteter og instrumenter, navnlig NIS-direktivet, revisionen af EU's strategi for cybersikkerhed, den kommende plan for EU's cybersikkerhedssamarbejde i krisesituationer og IKT-sikkerhedscertificering.

Forslaget præciserer således Agenturets opgaver og fører til effektivitetsgevinster. De øgede operationelle kompetencer og opgaver udgør ikke en reel risiko, idet de supplerer medlemsstaternes indsats og støtter dem, efter deres anmodning og i forbindelse med begrænsede og forud fastsatte ydelser

Herudover sikrer den foreslåede model for Agenturet, i henhold til den fælles tilgang, at der er tilstrækkelig kontrol til at sikre, at ENISA arbejder hen imod sine mål. De operationelle og finansielle risici ved de foreslåede ændringer synes at være begrænsede.

Samtidig er det nødvendigt at sikre tilstrækkelige finansielle ressourcer til ENISA til at udføre de opgaver, som Agenturet tillægges med de nye mandat, herunder inden for området certificering.

2.2.2. Påtænkt(e) kontrolmetode(r)

Agenturets regnskaber skal godkendes af Revisionsretten og er genstand for dechargeproceduren, og der planlægges audit.

Agenturets virke er desuden underlagt Ombudsmandens tilsyn i overensstemmelse med traktatens artikel 228.

Se punkt 2.1 og 2.2.1 i det foregående.

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger.

ENISA's forebyggelses- og beskyttelsesforanstaltninger finder anvendelse, herunder:

- Udbetalinger til tjenester eller bestilte undersøgelser forhåndskontrolleres af Agenturets tjenestegrene under hensyntagen til eventuelle kontraktlige forpligtelser, økonomiske principper og god finansiel og forvaltningsmæssig praksis. Alle aftaler og kontrakter mellem Agenturet og modtagere af udbetalinger vil indeholde bestemmelser om forholdsregler mod svig (tilsyn, rapporteringskrav m.v.).

- Bestemmelserne i 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), finder ubegrænset anvendelse i forbindelse med bekæmpelsen af svig, korruption og andre retsstridige handlinger.

- Agenturet skal inden seks måneder fra ikrafttrædelsesdatoen for nærværende forordning tiltræde 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), og udsteder straks de tilsvarende bestemmelser, som skal finde anvendelse på Agenturets personale.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

- Eksisterende udgiftsposter på budgettet

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
		OB/IOB[52]	fra EFTA-lande[53]	fra kandidatlande[54]	fra tredjelande	iht. finansforordningens artikel 21, stk. 2, litra b)
1a Konkurrenceevne for vækst og beskæftigelse	09.0203 ENISA og Sikkerhedscertificering af Informations- og Kommunikationsteknologi	OB	JA	NEJ	NEJ	NEJ
5 Administrationsudgifter	09.0101 Udgifter til tjenstgørende personale inden for politikområdet kommunikationsnet, indhold og teknologi 09.0102 Udgifter til eksternt tjenstgørende personale inden for politikområdet kommunikationsnet, indhold og teknologi	IOB	NEJ	NEJ	NEJ	NEJ

[52] OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.
[53] EFTA: Den Europæiske Frihandelssammenslutning.
[54] Kandidatlande og, efter omstændighederne, potentielle kandidatlande på Vestbalkan.

	09.010211 Andre administrationsudgifter					

3.2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	1a	Konkurrenceevne for vækst og beskæftigelse

ENISA			**Referenceværdi 2017 (31/12/2016)**		**2019** ***(fra og med den 1.7.2017)***	**2020**	**2021**	**2022**	**I ALT**
Afsnit 1: Personaleudgifter *(herunder også udgifter til ansættelse og uddannelse, socialmedicinske infrastrukturer og eksterne tjenester)*	Forpligtelser	1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Betalinger	2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Afsnit 2: Infrastruktur- og driftsudgifter	Forpligtelser	1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Betalinger	2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Afsnit 3: Driftsudgifter	Forpligtelser	3 a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Betalinger	3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
Bevillinger I ALT for ENISA	Forpligtelser	=1)+1 a) +3a)	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Betalinger	=2)+2 a) +3b)	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Udgiftsområde i den flerårige finansielle ramme	**5**	"Administration"

i mio. EUR (tre decimaler)

		2019 *(fra og med den 1.7.2017)*	**2020**	**2021**	**2022**	**I ALT**
GD: CNECT						
•Personaleressourcer		0,216	0,846	0,846	0,846	**2,754**
•Andre administrationsudgifter		0,102	0,235	0,238	0,242	**0,817**
I ALT GD CNECT	Bevillinger	0,318	1,081	1,084	1,088	**3,571**

Personaleudgifterne er beregnet i henhold til det planlagte ansættelsestidspunkt (arbejdet antages at begynde den 1.7.2019)

Ressourceprognosen for tiden efter 2020 er vejledende og berører ikke Kommissionens forslag om den flerårige finansielle ramme for perioden efter 2020

Bevillinger I ALT under UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	0,318	1,081	1,084	1,088	**3,571**

i mio. EUR (tre decimaler)

		2019	**2020**	**2021**	**2022**	**I ALT**
Bevillinger I ALT under UDGIFTSOMRÅDE 1-5 i den flerårige finansielle ramme	Forpligtelser	16,868	21,727	23,332	24,11	**86,038**
	Betalinger	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Anslåede virkninger for Agenturets bevillinger

– ☐ Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Der angives mål og resultater[55] ⇩	**2019**	**2020**	**2021**	**2022**	**I ALT**
Øgede kapaciteter og beredskab i medlemsstaterne og virksomhederne	1,408	1,900	1,931	1,969	7,208
Forbedret samarbejde og samordning mellem medlemsstaterne og EU's institutioner, agenturer og organer	0,939	1,266	1,288	1,313	4,806
Øget kapacitet på EU-plan til at supplere medlemsstaternes indsats, navnlig i tilfælde af grænseoverskridende cyberkriser	0,704	0,950	0,965	0,985	3,604
Øget oplysning til borgere og virksomhederne om cybersikkerhed:	0,704	0,950	0,965	0,985	3,604
Styrkelse af tilliden til det digitale indre marked og digital innovation gennem øget overordnet gennemsigtighed af cybersikkerhedstillidsniveauet for IKT-produkter og -tjenester:	0,939	1,266	1,288	1,313	4,806
OMKOSTNINGER I ALT	4.694	6,332	6,437	6,565	24,028

[55] Denne tabel viser kun operationelle udgifter under afsnit 3.

3.2.3. Anslåede virkninger for Agenturets menneskelige ressourcer

3.2.3.1. Resumé

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☒ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	3./4. kvartal 2019	**2020**	**2021**	**2022**
Midlertidigt ansatte (AD-medarbejdere)	4,242	5,695	6,381	6,709
Midlertidigt ansatte (AST-medarbejdere)	1,601	1,998	2,217	2,217
Kontraktansatte	2,041	2,041	2,041	2,041
Udstationerede nationale eksperter	0,306	0,447	0,656	0,796
I ALT	**8,190**	**10,181**	**11,295**	**11,763**

Personaleudgifterne er beregnet i henhold til det planlagte ansættelsestidspunkt (for nuværende ENISA-personale er antaget fuldtidsansættelse fra den 1.1.2019). For nyt personale er antaget gradvis ansættelse med begyndelse den 1.7.2019 og fuld beskæftigelse i 2022. Ressourceprognosen for tiden efter 2020 er vejledende og berører ikke Kommissionens forslag om den flerårige finansielle ramme for perioden efter 2020

Anslåede virkninger for medarbejderne (yderligere årsværk – stillingsfortegnelsen

Ansættelsesgrupper og lønklasser	2017 **ENISA aktuelt**	3./4. kvartal 2019)	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	

AD5					
AD i alt	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST i alt	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC i alt					
I ALT	48	12	10	7	3

Opgaver for yderligere AD/AST-personale for at nå instrumentets mål som beskrevet i afsnit 1.4.2:

Opgaver	AD	AST	UNE	I alt
Politik og kapacitetsopbygning	8	1		9
Operationelt samarbejde	8	1	7	16
Certificering (markedsrelaterede opgaver)	9	3	2	14
Viden, information og oplysning	1	1		2
I ALT	26	6	9	41

Opgavebeskrivelse:

Opgaver	**Yderligere påkrævede ressourcer**
Udvikling og gennemførelse af EU-politikker samt kapacitetsopbygning	Opgaverne vil omfatte bistand til samarbejdsgruppen, støtte til konsekvent gennemførelse af NIS-direktivet på tværs af grænserne, regelmæssig rapportering om status for gennemførelsen af EU's retlige ramme, rådgive og koordinere sektorspecifikke cybersikkerhedstiltag, herunder inden for energi,

	transport (f.eks. luftfart/vejtransport, søtransport/netforbundne køretøjer), sundhed, finans, støtte til oprettelsen af centre for informationsudveksling og analyse (ISAC'er) i forskellige sektorer.
Operationelt samarbejde og krisestyring:	**Opgaverne vil omfatte:** Varetagelse af sekretariatsfunktionen for CSIRT-netværket ved bl.a. at sørge for, at CSIRT-netværkets IT-infrastruktur og kommunikationskanaler fungerer godt. Sikre et struktureret samarbejde med CERT-EU, EC3 og andre relevante EU-organer. Opgaver i forbindelse med tilrettelæggelse af **Cyber Europe-øvelser**[56], bl.a. for at opskalere øvelsen fra hvert andet år til hvert år, og sørge for, at øvelserne håndterer hændelser fra start til slut. **Teknisk bistand – opgaverne vil omfatte et struktureret samarbejde med CERT-EU for at yde teknisk bistand i tilfælde af væsentlige hændelser og støtte analyse af hændelser. Det vil inkludere at bistå medlemsstaterne med håndteringen af hændelser og analyser af sårbarhed, sport (artefacts) og hændelser. Lette samarbejdet mellem de enkelte medlemsstater, når disse skal håndtere en krise ved at analysere og aggregere nationale situationsrapporter, der bygger på oplysninger, som medlemsstaterne og andre enheder frivilligt stiller til rådighed for Agenturet.** **Plan for en koordineret reaktion på væsentlige grænseoverskridende cybersikkerhedshændelser** Agenturet vil bidrage til at udvikle en samarbejdsorienteret respons, på EU-niveau og på medlemsstatsniveau, på væsentlige grænseoverskridende hændelser eller kriser i forbindelse med cybersikkerhed gennem en række opgaver, fra at bidrage til at etablere situationsbevidsthed på EU-niveau til at afprøve samarbejdsplaner i tilfælde af hændelser. **Efterfølgende tekniske undersøgelser af**

[56] Cyber Europa er den største og mest omfattende EU-øvelse for cybersikkerhed indtil nu og omfatter flere end 700 cybersikkerhedseksperter fra alle 28 medlemsstater. Den afholdes hvert andet år. Evalueringen af ENISA og EU's strategi for cybersikkerhed fra 2013 viser, at mange interessenter går ind for at opskalere Cyber Europe til en årlig begivenhed på grund af den hurtigt skiftende karakter af cybertrusler. Dette er dog ikke muligt på nuværende tidspunkt på grund af Agenturets begrænsede ressourcer.

	hændelser – foretage eller bidrage til gennemførelse af efterfølgende tekniske undersøgelser af hændelser i samarbejde med CSIRT-netværket med henblik på at udstede anbefalinger og styrke kapaciteten i form af offentlige rapporter med sigte på bedre at forhindre fremtidige hændelser.
Markedsrelaterede opgaver (standardisering, certificering)	Opgaverne vil omfatte aktiv støtte til det arbejde, der gennemføres inden for rammen for certificering, herunder yde teknisk ekspertise til udarbejdelsen af forslag til europæiske cybersikkerhedscertificeringsordninger. Opgaverne vil også omfatte støtte til udvikling af EU-politikker, udvikling og gennemførelse af standardisering, certificering og markedsobservatoriet - det vil kræve fremme af udbredelsen af risikostyringsstandarder for elektroniske produkter, net og tjenester og rådgivning til operatører af væsentlige tjenester og udbydere af digitale tjenester om tekniske sikkerhedskrav. Opgaverne vil også omfatte analyser af de vigtigste tendenser på cybersikkerhedsmarkedet.
Viden og information samt oplysning	Med henblik på at sikre lettere adgang til bedre struktureret information om cybersikkerhedsrisici og potentielle løsninger tillægges Agenturet en ny opgave, som er at udvikle og drive Unionens "informationsknudepunkt". Opgaven vil omfatte, via en særlig webportal, at samle, organisere og offentliggøre oplysninger om sikkerheden af net- og informationssystemer, herunder navnlig cybersikkerhed, der leveres af Unions institutioner, agenturer og organer. Opgaverne vil også omfatte støtte til ENISA's aktiviteter inden for oplysning, så Agenturet kan opskalere sin indsats.

3.2.3.2. Anslået behov for menneskelige ressourcer i det overordnede generaldirektorat

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☒ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i hele tal (eller med højst én decimal)

		Yderligere personale			
	Referenceværdi 2017	3./4. kvartal 2019	2020	2021	2020
• **Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)**					
09 01 01 01 (i hovedsædet og i Kommissionens repræsentationskontorer)	1	2	3		
• **Eksternt personale (i årsværk):**[57]					
09 01 02 01 (KA, UNE, V under den samlede bevillingsramme)	1	2			
I ALT		**4**	**3**		

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	Repræsentere Kommissionen i Agenturets bestyrelse. Udarbejde Kommissionens udtalelse om ENISA's samlede programmeringsdokument og overvåge dets gennemførelse. Føre tilsyn med udarbejdelsen af Agenturets budget og overvåge dets gennemførelse. Bistå Agenturet med at udvikle sine aktiviteter i overensstemmelse med Unionens politikker, herunder ved at deltage i relevante møder. Føre tilsyn med gennemførelsen af rammen for de europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester. Holde kontakten med medlemsstaterne og andre relevante interessenter med hensyn til certificeringsarbejdet. Samarbejde med ENISA om forslag til ordninger. Udarbejde

[57] KA: kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED: junioreksperter ved delegationerne.

	forslag til europæiske cybersikkerhedsordninger.
Eksternt personale	Som ovenfor

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

– ☐ Forslaget/initiativet er foreneligt med indeværende flerårige finansielle ramme

– ☒ Forslaget/initiativet kræver omlægning af det relevante udgiftsområde i den flerårige finansielle ramme

Forslaget kræver omprogrammering af artikel 09 02 03 på grund af revisionen af ENISA's mandat, som tillægger Agenturet nye opgaver i forbindelse med bl.a. gennemførelsen af NIS-direktivet og den europæiske rammer for cybersikkerhedscertificering. De modsvarende beløb:

År	Anslået	Anmodning
2019	10,739	16,550
2020	10,954	20,646
2021	Ikke relevant	22 248*
2022	Ikke relevant	23 023*

Dette er et skøn. EU's bidrag efter 2020 vil blive drøftet som led i en debat i Kommissionen som helhed om samtlige forslag for perioden efter 2020. Derfor vil Kommissionen, når den har fremsat sit forslag til forordning om den kommende flerårige finansielle ramme, forelægge en ændret finansieringsoversigt, hvor der tages hensyn til konklusionerne af konsekvensanalysen[58].

– ☐ Forslaget/initiativet kræver, at fleksibilitetsinstrumentet anvendes, eller at den flerårige finansielle ramme revideres[59].

3.2.5. Tredjemands bidrag til finansieringen

– ☐ Forslaget/initiativet indeholder ikke bestemmelser om samfinansiering med tredjemand.

– ☒ Forslaget/initiativet indeholder bestemmelser om samfinansiering, jf. følgende overslag:

[58] Link til siden med konsekvensanalyse

[59] Se artikel 11 og 17 i Rådets forordning (EU, Euratom) nr. 1311/2013 om fastlæggelse af den flerårige finansielle ramme for årene 2014-2020.

	År **2019**	År **2020**	År **2021**	År **2022**
EFTA	p.m[60].	p.m.	p.m.	p.m.

3.3. Anslåede virkninger for indtægterne

– ☒ Forslaget/initiativet har ingen finansielle virkninger for indtægterne.

– ☐ Forslaget/initiativet har følgende finansielle virkninger:

  – ☐ for egne indtægter

  – ☐ for diverse indtægter.

[60] Det nøjagtige beløb for de efterfølgende år kendes først, når EFTA's proportionalitetsfaktor fastsættes for det pågældende år.