Rådet for
Den Europæiske Union

Bruxelles, den 29. maj 2018
(OR. en)

9350/18

Interinstitutionel sag:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTE

fra:	formandskabet
til:	Rådet
Tidl. dok. nr.:	8834/18
Komm. dok. nr.:	12183/17
Vedr.:	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") - Generel indstilling

I. INDLEDNING

1. I forbindelse med strategien for det digitale indre marked vedtog Kommissionen den 13. september 2017 ovennævnte forslag[1] med artikel 114 i TEUF som retsgrundlag og fremsendte det til Rådet og Europa-Parlamentet. Dette forslag, som er en del af den såkaldte cybersikkerhedspakke, sigter mod et højt niveau af cybersikkerhed, cyberrobusthed og tillid i Unionen med henblik på at sikre et velfungerende indre marked.

2. Den foreslåede forordning fastsætter målene, opgaverne og de organisatoriske aspekter for ENISA, EU's Agentur for Net- og Informationssikkerhed, og fastlægger en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau for IKT-produkter og -tjenester i Unionen. Kommissionens forslag ledsages af en konsekvensanalyse, som undersøger et specifikt sæt af otte politiske muligheder, der omfatter gennemgangen af ENISA og IKT-cybersikkerhedscertificering.

3. Den foreslåede forordning indeholder to centrale elementer:

   - et permanent mandat til agenturet med begrænset omfang i betragtning af behovene under de nye politikprioriteter og -instrumenter, og et nyt sæt opgaver og funktioner til agenturet, der skal muliggøre effektiv og virkningsfuld støtte til indsatsen i medlemsstaterne og EU-institutionerne og hos andre interessenter med henblik på et sikkert cyberspace

   - En europæisk cybersikkerhedscertificeringsramme for IKT-produkter og -tjenester og regler for europæiske cybersikkerhedscertificeringsordninger, som skal sørge for, at attester udstedt i henhold til sådanne ordninger er gyldige og anerkendes i alle medlemsstater, og som imødegår den nuværende fragmentering af markedet.

[1] Dok. 12183/17, 12183/1/17 REV 1, 12183/2/17 REV 2.

4. I oktober 2017 opfordrede Det Europæiske Råd[2] til, at Kommissionens cybersikkerhedsforslag udvikles på en helhedsorienteret måde, leveres rettidigt og gennemgås straks på grundlag af en handlingsplan, der skal udarbejdes af Rådet.

5. Den 12. december 2017 vedtog Rådet (almindelige anliggender) handlingsplanen[3] for gennemførelse af Rådets konklusioner[4] om den fælles meddelelse[5] til Europa-Parlamentet og Rådet: "Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU". Handlingsplanen afspejlede Rådets ambition om at nå frem til en generel indstilling senest i juni 2018.

6. I Europa-Parlamentet er Angelika NIEBLER (ITRE, PPE) blevet udpeget til ordfører. ITRE-udvalgets afstemning om betænkningen er fastsat til den 19. juni 2018.

7. Det Europæiske Økonomiske og Sociale Udvalg vedtog sin udtalelse den 14. februar 2018.

II. ARBEJDET I RÅDET

8. Kommissionen forelagde den 26. september 2017 dette forslag og sin konsekvensanalyse for Den Horisontale Gruppe vedrørende Cyberspørgsmål (i det følgende benævnt "gruppen") efterfulgt af en gennemgang af konsekvensanalysen den 20. oktober i gruppen. De efterfølgende drøftelser drejede sig om agenturets operationelle kapacitet og omfanget af interaktionen med de nationale kompetente myndigheder og om certificeringsrammens virkning på markedet og virksomhedernes konkurrenceevne. Generelt blev både konsekvensanalysen og forslaget positivt modtaget af delegationerne.

---

2 EUCO 14/17, punkt 11.
3 Dok. 15748/17.
4 Dok. 14435/17.
5 Dok. 12211/17.

9. Drøftelsen af selve forslaget i gruppen begyndte i november 2017 under det estiske formandskab og fortsatte under det bulgarske formandskab. Der har været afholdt 12 møder om dette forslag, hvilket har resulteret i otte på hinanden følgende reviderede udgaver af forslaget med henblik på at nå til enighed om en generel indstilling på den kommende samling i TTE-Rådet (telekommunikation) den 8. juni 2018.

10. Resultatet af drøftelserne i gruppen den 14.-15. maj 2018 og formandskabets reviderede kompromistekst findes i bilaget til denne note. Betragtningerne er blevet tilpasset for at afspejle ændringerne i substansbestemmelserne. Alle ændringer i forhold til Kommissionens forslag er angivet med **fed** skrift eller [...]. Ændringer i forhold til det nyeste dokument fra gruppen 8834/18 er angivet med **fed skrift og understregning** og udgået tekst med **[...]**.

III. KONKLUSION

11. Formandskabets kompromistekst, jf. bilaget, afspejler formandskabets og medlemsstaternes indsats for at sikre en passende balance i teksten.

12. Den 25. maj 2018 nåede De Faste Repræsentanters Komité til enighed om formandskabets kompromistekst med forbehold af ændringerne i artikel 19, stk. 5, og artikel 48, stk. 5, jf. bilaget.

13. Rådet opfordres derfor til at vedtage en generel indstilling på samlingen den 8. juni 2018 og give formandskabet mandat til at indlede forhandlinger med repræsentanterne for Europa-Parlamentet og Europa-Kommissionen om denne sag.

BILAG

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

om ENISA, "*[...]Den Europæiske Unions 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[6],

under henvisning til udtalelse fra Regionsudvalget[7],

efter den almindelige lovgivningsprocedure, og

[6] EUT C [...] af [...], s. [...].
[7] EUT C [...] af [...], s. [...].

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 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 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[8] 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[9] om forlængelse af agenturets mandat frem til marts 2012. Ved forordning (EU) nr. 580/2011[10] forlængedes agenturets mandat frem til den 13. september 2013. I 2013 vedtog Europa-Parlamentet og Rådet forordning (EU) nr. 526/2013[11] om ENISA og om ophævelse af forordning (EF) nr. 460/2004, som forlængede agenturets mandat frem til juni 2020.

---

8 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).

9 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).

10 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).

11 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).

(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, cloudcomputingtjenester 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 Europa-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 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 **støtte** [...] national indsats og **proaktivt bidrage til** Unionens indsats og udføre sine opgaver i fuldt samarbejde med EU's institutioner, [...] agenturer **og organer** samt 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 **og dets sektorspecifikke aspekter med henblik på at øge relevansen af EU-politikker og -lovgivning med en cybersikkerhedsdimension og sikre konsekvens i gennemførelsen heraf på nationalt plan** [...]. 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 cyberrobustheden. På baggrund af det hurtigt skiftende cybersikkerhedstrusselsbillede står det klart, at medlemsstaterne må støttes med en mere overgribende tværpolitisk tilgang til opbygningen af cyberrobusthed.

(15) Agenturet bør bistå medlemsstaterne og EU's institutioner, [...] agenturer **og organer** med at opbygge og forbedre deres kapacitet og beredskab med sigte på at forebygge, opdage og imødegå cyber**trusler** [...] 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. **Aktiviteter, der udføres af ENISA vedrørende medlemsstaternes operationelle kapacitet, bør udelukkende være et supplement til medlemsstaternes egen indsats for at opfylde deres forpligtelser i henhold til NIS-direktivet og bør således ikke erstatte dem** [...].

(15a) Agenturet bør også bistå med udviklingen og ajourføringen af Unionens og, på anmodning, medlemsstaternes strategier for net- og informationssystemers sikkerhed, herunder navnlig cybersikkerhed, fremme deres udbredelse og følge 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 [...] **bør agenturet** støtte **informationsudveksling i og mellem sektorer, navnlig i de sektorer, der er anført i bilag II til 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, for eksempel gennem lettelse af** [...] etablering af centre for informationsudveksling og analyse (ISAC'er) [...].

(18) Agenturet bør samle og analysere **frivilligt delte** nationale rapporter fra CSIRT'er og CERT-EU **med det formål at bistå medlemsstaterne med at** indføre fælles [...] **procedurer**, 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 [...] **inden for** CSIRT-netværket.

(19) Agenturet bør bidrage til en respons på EU-niveau i tilfælde af væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser. Denne funktion bør **udføres i overensstemmelse med dets mandat i henhold til denne forordning og en tilgang, der skal godkendes af medlemsstaterne i forbindelse med Kommissionens henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser. Den kan** 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 [...] **regelmæssige** cybersikkerhedsøvelser.

(20) [...] **I forbindelse med støtte til** operationel**t samarbejde** [...] bør agenturet gøre brug af den tilgængelige **tekniske og operationelle** ekspertise hos CERT-EU gennem et struktureret samarbejde [...]. [...] 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 **og undgå overlapning af aktiviteter**.

(21) I overensstemmelse med sine [...] opgaver **med at støtte operationelt samarbejde inden for CSIRT-netværket** bør agenturet være i stand til at yde støtte til medlemsstaterne **på deres anmodning**, f.eks. ved at yde rådgivning **om, hvordan de kan forbedre deres evne til at forebygge, opdage og reagere på hændelser, ved at [...] lette den** [...] tekniske **håndtering af hændelser, der har betydelige eller væsentlige konsekvenser** [...], eller **ved** at sikre analyse af trusler og hændelser. **Lettelse af den tekniske håndtering af hændelser, der har betydelige eller væsentlige konsekvenser, bør især omfatte, at ENISA støtter frivillig deling af tekniske løsninger mellem medlemsstaterne eller tilvejebringer kombinerede tekniske oplysninger – såsom tekniske løsninger, der frivilligt deles af medlemsstaterne.** 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 [...] **støtte operationelt samarbejde**.

(22) Som led i det regelmæssige samarbejde på teknisk niveau til støtte for Unionens situationsbevidsthed bør agenturet regelmæssigt **og i tæt samarbejde med medlemsstaterne** 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 [...] eller NIS-direktivets centrale kontaktpunkter **(begge på frivillig basis)**, Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol og CERT-EU samt, hvor det er relevant, Den Europæiske Unions Efterretnings- og Situationscenter (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) **Agenturets støtte til t**ekniske efterfølgende undersøgelser af hændelser med betydelig indvirkning [...] efter anmodning fra de [...] **berørte** medlemsstater [...] bør fokusere på forebyggelse af fremtidige hændelser [...]. **De berørte medlemsstater bør give de nødvendige oplysninger, så agenturet effektivt kan støtte tekniske undersøgelser.**

(24) [...]

(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 **offentligt tilgængelige eller frivilligt delte** 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 EU's institutioner, agenturer og organer med at identificere nye tendenser og forebygge [...] cybersikkerheds**hændelser** ved at udføre analyser af trusler og hændelser.

(27) Med henblik på at øge Unionens modstandsdygtighed bør agenturet udvikle ekspertise vedrørende **cyber**sikkerhed for **infrastrukturer, der understøtter navnlig de sektorer, som er anført i bilag II til NIS-direktivet, og dem, der anvendes af de udbydere af digitale tjenester, som er anført i bilag III til det pågældende direktiv** [...], 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 EU's institutioner, [...] agenturer **og organer** 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 phishingangreb, botnet, økonomisk svig og banksvindel, samt fremme af grundlæggende autentificering 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)**, Det Europæiske GNSS-Agentur (GSA)** 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 **i sin rolle** 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 [...] **regelmæssige** 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.

(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 EU's institutioner, [...] agenturer **og organer** og, hvor det er relevant, medlemsstaterne, hvis de anmoder herom, om forskningsbehov inden for [...] cybersikkerhed. **Med henblik på at klarlægge forskningsbehov og -prioriteter bør agenturet også høre de relevante brugergrupper.**

(37) Cybersikkerheds**trusler** [...] er af global karakter. Der er behov for et tættere internationalt samarbejde for at forbedre **cyber**sikkerhedsstandarderne, 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 EU's relevante institutioner, [...] agenturer **og organer**.

(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 udarbejde en årsberetning**, bl.a. om gennemførelsen af agenturets årlige arbejdsprogram**, 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[12]. 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[13]. 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.

---

[12] 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).

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

(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 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) [...]

(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-**processer**, -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 på sikkerhedscertificeringsområdet, [...] omfatter SOG-IS kun 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 **og EU-overensstemmelseserklæringer** for IKT-produkter og -tjenester i alle medlemsstater. Den europæiske ramme bør have 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 ikkediskriminerende og baseret på internationale og/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**-processer,** -produkter og -tjenester. Ordningerne bør gennemføres og overvåges af nationale **cybersikkerheds**certificerings[...]myndigheder, 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-**processer**, -produkter og -tjenester, der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastsatte krav **[...] med henblik på** at **[...] beskytte** 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 hele deres livscyklus** i denne forordnings betydning. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-**processer,** -produkter og -tjenester i denne forordning. IKT-**processer,** -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-**processer,** -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**, hvis der ikke findes hensigtsmæssige standarder**.

(55a) De tekniske specifikationer, der skal anvendes i en europæisk cybersikkerhedscertificeringsordning, bør fastlægges under overholdelse af principperne i bilag II til forordning (EU) nr. 1025/2012. Visse afvigelser fra disse principper kan dog anses for nødvendige i behørigt begrundede tilfælde, hvor de pågældende tekniske specifikationer skal anvendes i en europæisk cybersikkerhedscertificeringsordning, der henviser til tillidsniveauet "højt". Årsagerne til sådanne afvigelser skal gøres offentligt tilgængelige.

(55b) Certificeret overensstemmelsesvurdering er en proces, hvor det evalueres, om fastsatte krav til en IKT-proces eller -tjeneste eller et IKT-produkt er opfyldt. Denne proces gennemføres af en uafhængig tredjepart, som ikke er produktproducenten eller tjenesteudbyderen. Processen med udstedelse af en attest efterfølger processen med vellykket evaluering af en IKT-proces eller -tjeneste eller et IKT-produkt. Den bør anses som en bekræftelse af, at den pågældende evaluering er foretaget korrekt. Afhængigt af tillidsniveauet bør den europæiske cybersikkerhedsordning angive, om attesten udstedes af et privat eller offentligt organ. Overensstemmelsesvurdering og 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.

(55c) Attestbrugeres valg af et passende certificeringsniveau og tilhørende sikkerhedskrav bør bygge på en risikoanalyse for anvendelse af den pågældende IKT-proces eller -tjeneste eller det pågældende IKT-produkt. Tillidsniveauet bør således stå mål med risikoniveauet i forbindelse med den tilsigtede anvendelse af en IKT-proces eller -tjeneste eller et IKT-produkt.

(55d) En europæisk cybersikkerhedscertificeringsordning kan fastsætte, at overensstemmelsesvurdering skal foretages under eneansvar af producenter og udbydere af IKT-produkter og -tjenester (selvvurdering af overensstemmelse). I sådanne tilfælde er det tilstrækkeligt, at producenten eller udbyderen selv foretager al kontrol med henblik på at sikre de pågældende IKT-processers, -produkters eller -tjenesters overensstemmelse med certificeringsordningen. Denne type overensstemmelsesvurdering bør betragtes som passende for IKT-produkter og -tjenester med lav kompleksitet (f.eks. enkel konstruktions- og produktionsmekanisme), som udgør en lav risiko for samfundets interesser. Desuden kan kun IKT-produkter og -tjenester, der svarer til tillidsniveauet "grundlæggende", blive genstand for selvvurdering af overensstemmelse.

(55e) En europæisk cybersikkerhedscertificeringsordning kan give mulighed for både certificering og selvvurdering af overensstemmelse for IKT-produkter og -tjenester. I så fald bør ordningen fastsætte klare og forståelige måder, hvorpå forbrugerne eller andre brugere kan skelne mellem produkter og tjenester, der er vurderet under producentens eller udbyderens ansvar, og produkter og tjenester, der er certificeret af en tredjepart.

(55f) Producenter og udbydere af IKT-produkter og -tjenester, som foretager selvvurdering af overensstemmelse, bør udarbejde og undertegne en EU-overensstemmelseserklæring som led i overensstemmelsesvurderingsproceduren. En EU-overensstemmelseserklæring er et dokument, der angiver, at et bestemt IKT-produkt eller en bestemt IKT-tjeneste opfylder kravene i ordningen. Ved at udarbejde og undertegne en EU-overensstemmelseserklæring påtager producenten eller udbyderen sig ansvaret for, at IKT-produktet eller -tjenesten opfylder de retlige krav i ordningen. Et eksemplar af EU-overensstemmelseserklæringen bør indgives til den nationale cybersikkerhedscertificeringsmyndighed og ENISA.

(55g) Producenter og udbydere af IKT-produkter og -tjenester bør stille EU-overensstemmelseserklæringen og den tekniske dokumentation for alle relevante oplysninger vedrørende IKT-produkternes eller -tjenesternes overensstemmelse med en ordning til rådighed for den kompetente nationale cybersikkerhedscertificeringsmyndighed i en periode fastsat i den specifikke tilsvarende europæiske cybersikkerhedscertificeringsordning. Den tekniske dokumentation bør præcisere de gældende krav og, i det omfang det er relevant for vurderingen, omfatte IKT-produktets eller -tjenestens udformning, fremstilling og drift. Den tekniske dokumentation bør være udarbejdet på en måde, der gør det muligt at vurdere et IKT-produkts eller en IKT-tjenestes overensstemmelse med de relevante krav.

(55h) Medlemsstaterne og relevante interesseorganisationer bør have ret til at foreslå Den Europæiske Cybersikkerhedscertificeringsgruppe udarbejdelse af forslag til en ordning. Relevante interesseorganisationer er branche- eller forbrugerrepræsentantorganisationer, herunder repræsentanter for SMV-organisationer, der har en legitim interesse i udviklingen af en særlig europæisk cybersikkerhedscertificeringsordning. Sådanne forslag bør undersøges i lyset af de kriterier, som Den Europæiske Cybersikkerhedscertificeringsgruppe har opstillet i form af retningslinjer baseret på principperne om gennemsigtighed, åbenhed, upartiskhed, konsensus, effektivitet, relevans og sammenhæng.

(56) Kommissionen **og gruppen** bør have beføjelse til at anmode ENISA om **hurtigst muligt** at udarbejde forslag til ordninger for specifikke IKT-**processer**, -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**-processer**, -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 og/eller højt **og evalueringsniveauerne, hvor det er relevant**.

(56a) Tillidsniveauet for en europæisk certificeringsordning er grundlaget for tillid til, at en IKT-proces, et IKT-produkt eller en IKT-tjeneste opfylder sikkerhedskravene i en bestemt europæisk cybersikkerhedscertificeringsordning. For at sikre sammenhæng i rammerne for certificerede IKT-processer, -produkter og -tjenester kan en europæisk cybersikkerhedscertificeringsordning præcisere tillidsniveauer for europæiske cybersikkerhedsattester og EU-overensstemmelseserklæringer, der udstedes i henhold til den pågældende ordning. Den enkelte attest kan henvise til et af tillidsniveauerne - grundlæggende, betydeligt eller højt - mens EU-overensstemmelseserklæringen kun kan henvise til tillidsniveauet grundlæggende. Tillidsniveauerne indebærer en tilsvarende grad af [...] bestræbelser forud for evalueringen [...] og karakteriseres ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at afbøde eller forhindre cybersikkerhedshændelser. Hvert tillidsniveau bør være ensartet på tværs af de forskellige sektorspecifikke områder, hvor der anvendes certificering.

(56b) En europæisk cybersikkerhedscertificeringsordning kan fastsætte flere evalueringsniveauer, alt efter hvor stringent og dyb den anvendte evalueringsmetodologi er; denne bør svare til et af tillidsniveauerne og være ledsaget af en passende kombination af tillidskomponenter. For samtlige tillidsniveauer bør IKT-produktet eller -tjenesten indeholde en række sikre funktioner som defineret i ordningen, og som kan omfatte: sikker klar til brug-konfiguration, signeret kode, sikker opdatering og mekanismer til begrænsning af exploits og fuld stack/heap-hukommelsesbeskyttelse. Disse funktioner bør være udviklet og vedligeholdes ved hjælp af sikkerhedsorienterede udviklingstilgange og tilknyttede værktøjer for at sikre, at effektive mekanismer (både software og hardware) er indarbejdet på pålidelig vis. For det grundlæggende tillidsniveau bør evalueringen som minimum tage udgangspunkt i følgende tillidskomponenter: Evalueringen bør som minimum omfatte en gennemgang af den tekniske dokumentation for IKT-produktet eller -tjenesten foretaget af overensstemmelsesvurderingsorganet. Hvis certificeringen omfatter IKT-processer, bør den proces, der anvendes til at udforme, udvikle og vedligeholde et IKT-produkt eller en IKT-tjeneste, også være omfattet af den tekniske gennemgang. I tilfælde, hvor en europæisk cybersikkerhedscertificeringsordning giver mulighed for selvvurdering af overensstemmelsesniveauet, bør det være tilstrækkeligt, hvis producenten eller udbyderen har udført en selvvurdering af IKT-processens, -produkternes eller -tjenesternes overensstemmelse med certificeringsordningen. For tillidsniveauet betydeligt bør evalueringen ud over tillidsniveauet grundlæggende som minimum tage udgangspunkt i kontrol af overensstemmelsen af IKT-produktets eller -tjenestens sikkerhedsfunktioner med den tilhørende tekniske dokumentation. For det høje tillidsniveau bør evalueringen ud over det betydelige tillidsniveau som minimum tage udgangspunkt i en effektivitetstest, der vurderer modstandsdygtigheden af IKT-produktets eller -tjenestens sikkerhedsfunktioner over for dem, der med betydelige færdigheder og ressourcer udfører omfattende cyberangreb.

(56c) Ved udarbejdelsen af forslag til en ordning bør ENISA høre alle relevante interessenter, f.eks. de europæiske standardiseringsorganisationer, relevante nationale myndigheder, organisationer, der er baseret på aftaler om gensidig anerkendelse, såsom SOG-IS' MRA, SMV'er, forbrugerorganisationer samt miljøorganisationer og sociale interessenter.

(56d) ENISA bør drive et websted med oplysninger om og offentlig omtale af de europæiske cybersikkerhedscertificeringsordninger, der bl.a. bør indeholde anmodningerne om udarbejdelse af forslag til en europæisk cybersikkerhedscertificeringsordning samt den feedback, der modtages under den af ENISA gennemførte høringsproces i udarbejdelsesfasen. Dette websted bør også indeholde oplysninger om attester og EU-overensstemmelseserklæringer, der udstedes i henhold til denne forordning.

(57) Anvendelse af den europæiske cybersikkerhedscertificering **og EU-overensstemmelseserklæringer** bør fortsat være frivillig, medmindre andet er fastsat i EU-lovgivningen eller national lovgivning **, der er vedtaget i overensstemmelse med EU-retten**. **I mangel af harmoniseret lovgivning kan medlemsstaterne vedtage nationale tekniske forskrifter i overensstemmelse med direktiv (EU) 2015/1535, der fastsætter obligatorisk certificering i henhold til en europæisk cybersikkerhedscertificeringsordning. Medlemsstaterne kan også anvende den europæiske cybersikkerhedscertificering i forbindelse med offentlige udbud og direktiv 2014/214/EU**. [...]

(57a) 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, 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. Medlemsstaterne bør dog ikke være forhindret i at vedtage eller opretholde nationale certificeringsordninger af nationale sikkerhedshensyn.

(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. Akkrediteringsorganerne bør **begrænse, suspendere eller** tilbagekalde 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) [...] Medlemsstaterne [...] **bør** udpege en **eller flere** [...] cybercertificerings**myndigheder**, som skal føre tilsyn med overensstemmelsen **med de forpligtelser, der følger af denne forordning. Hvis en medlemsstat finder det hensigtsmæssigt, kan opgaverne også pålægges allerede eksisterende myndigheder. Medlemsstaterne bør også efter gensidig aftale med en anden medlemsstat kunne beslutte at udpege en eller flere tilsynsmyndigheder på denne anden medlemsstats område. Myndigheden bør navnlig overvåge og håndhæve de forpligtelser, som en producent eller udbyder af IKT-produkter og tjenester, der er etableret på deres respektive område, er underlagt i henhold til EU-overensstemmelseserklæringen, bistå de nationale akkrediteringsorganer med overvågning af og tilsyn med overensstemmelsesvurderingsorganers aktiviteter ved at stille ekspertise og relevante oplysninger til rådighed for dem, bemyndige overensstemmelsesvurderingsorganer til at udføre dens opgaver, hvis disse opfylder yderligere krav, der er fastsat i en ordning, og overvåge relevante udviklinger inden for cybersikkerhedscertificering** [...]. Nationale **cybersikkerheds**certificerings[...]myndigheder bør behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af **dem eller attester udstedt af overensstemmelsesvurderingsorganer med henvisning til det høje tillidsniveau** [...], undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist. Herudover bør de samarbejde med andre nationale **cybersikkerheds**certificerings[...]myndigheder 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 cybersikkerhedsordninger.

(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 **repræsentanter for** nationale **cybersikkerheds**certificerings[...]myndigheder **eller andre relevante nationale myndigheder**. 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 **agenturet vedrørende forslag til ordninger og til** Kommissionen vedrørende vedligeholdelse og revision af bestående europæiske cybersikkerhedscertificeringsordninger.

(60a) Gruppen bør lette udvekslingen af god praksis og ekspertise mellem de nationale cybersikkerhedscertificeringsmyndigheder, der er ansvarlige for bemyndigelse af overensstemmelsesvurderingsorganer og udstedelse af attester. Gruppen bør støtte udviklingen af en peer review-mekanisme for organer, der udsteder europæiske cybersikkerhedsattester for tillidsniveauet højt, i forbindelse med udarbejdelsen af forslag til en ordning og gennemførelsen heraf. Disse peer reviews bør navnlig vurdere, om de berørte organer har den nødvendige ekspertise, og om de gennemfører deres opgaver på en ensartet måde. Resultaterne af peer reviewene bør offentliggøres. Disse organer kan vedtage hensigtsmæssige foranstaltninger for at tilpasse deres praksis og ekspertise.

(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.

(61a) For yderligere at lette handelen og i erkendelse af, at IKT-forsyningskæderne er globale, kan aftaler om gensidig anerkendelse vedrørende attester udstedt af ordninger, som er oprettet i henhold til den europæiske ramme for cybersikkerhedscertificering, indgås af Unionen i overensstemmelse med artikel 218 i TEUF. Kommissionen kan under hensyntagen til rådgivningen fra ENISA og Den Europæiske Cybersikkerhedscertificeringsgruppe anbefale, at der indledes relevante forhandlinger. Hver ordning bør fastsætte specifikke betingelser for gensidig anerkendelse med tredjelande.

(62) [...]

(63) [...]

(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 **cybersikkerheds**certificerings[...]myndigheders 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

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

a) at fastsætte målene, opgaverne og de organisatoriske aspekter for ENISA, "[...]**Den Europæiske Unions** 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**-processer,** -produkter og -tjenester i Unionen. Denne ramme anvendes uden at det berører specifikke bestemmelser vedrørende frivillig eller obligatorisk certificering i andre af Unionens retsakter.

2. **Denne forordning 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 2

Definitioner

I denne forordning forstås ved:

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

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

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

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

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

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

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

8) "cybertrussel": enhver potentiel omstændighed eller begivenhed, som kan **skade, afbryde eller på anden måde** have en negativ indvirkning på net- og informationssystemer, deres brugere og berørte personer

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

9a) "national cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er udviklet og vedtaget af en national offentlig myndighed, og som finder anvendelse på certificeringen eller overensstemmelsesvurderingen af IKT-processer, -produkter og -tjenester, der er omfattet af den pågældende ordning

10) "europæisk cybersikkerhedsattest": et dokument [...], som attesterer, at en given IKT-**proces,** et givet IKT-produkt eller en given IKT-tjeneste [...] **er blevet evalueret med henblik på overensstemmelse med** specifikke **sikkerheds**krav fastsat i en europæisk cybersikkerhedscertificeringsordning

11) "IKT-produkt[...]": ethvert element eller enhver gruppe af elementer i net- og informationssystemer

11a) "IKT-tjeneste": enhver tjeneste, der helt eller hovedsagelig består i overførsel, lagring, hentning eller behandling af oplysninger ved hjælp af net- og informationssystemer

11b) "IKT-proces": et sæt aktiviteter, der udføres for at udforme, udvikle, levere og vedligeholde et IKT-produkt eller en IKT-tjeneste

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

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

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

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

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

16a) "teknisk specifikation": et dokument, der fastsætter de tekniske krav, som en IKT-proces, et IKT-produkt eller en IKT-tjeneste skal opfylde

16b) "tillidsniveau": et grundlag for tillid til, at en IKT-proces, et IKT-produkt eller en IKT-tjeneste opfylder sikkerhedskravene i en bestemt europæisk cybersikkerhedscertificeringsordning, og en angivelse af, på hvilket niveau processen, produktet eller tjenesten er blevet evalueret; tillidsniveauet måler ikke selve IKT-processens, -produktets eller -tjenestens sikkerhed.

AFSNIT II

ENISA – " *[...] Den Europæiske Unions Agentur for Cybersikkerhed*"

KAPITEL I

MANDAT OG FORMÅL *[...]*

Artikel 3

Mandat

1. Agenturet udfører de opgaver, det tillægges ved denne forordning, med det formål at bidrage til et højt cybersikkerhedsniveau [...] i **hele** Unionen**, navnlig ved at støtte medlemsstaterne og EU's institutioner, agenturer og organer i at forbedre cybersikkerheden**. **Agenturet fungerer som et referencepunkt for rådgivning om og ekspertise i cybersikkerhed for EU's institutioner, agenturer og organer.**

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.

2a. Agenturet handler ved udførelsen af sine opgaver uafhængigt og tager størst muligt hensyn til medlemsstaternes relevante myndigheders ekspertise og undgår samtidig overlapning af aktiviteter.

3. [...]

Artikel 4

Mål

1. 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.

2. Agenturet bistår EU's institutioner, agenturer og organer samt medlemsstaterne med udvikling og gennemførelse af **EU**-politikker vedrørende cybersikkerhed**, herunder sektorspecifikke politikker om cybersikkerhed**.

3. Agenturet støtter kapacitetsopbygning og beredskab i hele Unionen ved at bistå **EU's institutioner, agenturer og organer samt** medlemsstaterne og offentlige og private interessenter for at øge beskyttelsen af deres net- og informationssystemer, udvikle **og forbedre cyberrobusthed og indsatskapaciteter og udvikle** færdigheder og kompetencer inden for cybersikkerhed [...].

4. Agenturet fremmer samarbejde og koordinering på EU-plan mellem medlemsstaterne, EU's institutioner, agenturer og organer og relevante **private og offentlige** interessenter [...] for så vidt angår spørgsmål vedrørende cybersikkerhed.

5. Agenturet **bidrager til at øge** [...] cybersikkerhedskapaciteten på EU-plan for at [...] **bistå** medlemsstaterne med at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser.

6. Agenturet fremmer brugen af certificering **med henblik på at undgå fragmentering af certificeringsordningerne i EU**. **Navnlig bidrager agenturet** [...] 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.

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

KAPITEL IA

OPGAVER

Artikel 5

[...] ***Udvikling og gennemførelse af Unionens politikker og lovgivning***

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

1. 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

2. bistå medlemsstaterne med en konsekvent gennemførelse af Unionens politikker og lovgivning om cybersikkerhed, navnlig i forbindelse med direktiv (EU) 2016/1148, herunder ved hjælp af 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

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

4. 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

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

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

    b) 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

    c) indberetninger af [...] sikkerhed**shændelser** 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

[...] ***Kapacitetsopbygning***

1. Agenturet bistår:

a) medlemsstaterne i deres bestræbelser på at forbedre forebyggelse, opdagelse og analyse af og kapaciteten til at reagere på cyber[...]**trusler** [...] og -hændelser ved at stille den nødvendige viden og ekspertise til rådighed for dem

b) EU's institutioner, [...] agenturer **og organer** i deres bestræbelser på at forbedre forebyggelse, opdagelse og analyse af og kapaciteten til at reagere på cyber[...]**trusler** [...] og -hændelser**, navnlig** gennem passende støtte til CERT'en for Unionens institutioner, agenturer og organer (CERT-EU)

c) 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

d) 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** gennemførelsen af disse strategier i hele Unionen med henblik på at fremme bedste praksis

e) Unionens institutioner med udviklingen og revisionen af EU's strategier vedrørende cybersikkerhed og fremmer deres udbredelse og følger fremskridtene med hensyn til deres gennemførelse

f) 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

g) medlemsstaterne ved at tilrettelægge **regelmæssige** [...] cybersikkerhedsøvelser 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

h) relevante offentlige organer ved at tilbyde kurser om cybersikkerhed, eventuelt i samarbejde med interessenter

i) samarbejdsgruppen , **i** [...] udveksling af [...] 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.

2. Agenturet **støtter udveksling af oplysninger inden for og mellem sektorer** [...], navnlig i de sektorer, der er nævnt i bilag II til direktiv (EU) 2016/1148, ved at stille bedste praksis og vejledning om tilgængelige værktøjer og procedurer samt om håndtering af lovgivningsmæssige spørgsmål relateret til informationsudveksling til rådighed.

Artikel 7

[...] ***Operationelt samarbejde på EU-plan***

1. Agenturet understøtter det operationelle samarbejde mellem **medlemsstaterne, Unionens institutioner, agenturer og** [...] organer og mellem interessenter.

2. Agenturet samarbejder på det operationelle plan og etablerer synergier med Unionens institutioner, [...] agenturer **og organer**, 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.

3. Agenturet varetager sekretariatsfunktionen for CSIRT-netværket, jf. artikel 12, stk. 2, i direktiv (EU) 2016/1148, og fremmer **i denne egenskab** [...] informationsudveksling og samarbejdet mellem dets medlemmer.

4. Agenturet **støtter** [...] det operationelle samarbejde i CSIRT-netværket og yder støtte til medlemsstaterne **på deres anmodning** ved at:

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

b) [...] **lette den** tekniske **håndtering** [...] af hændelser, der har betydelige eller væsentlige konsekvenser**, herunder navnlig ved at støtte den frivillige udveksling af tekniske løsninger mellem medlemsstaterne**

c) analysere sårbarheder [...] og hændelser

ca) yde støtte til efterfølgende tekniske undersøgelser af hændelser, der har betydelige eller væsentlige konsekvenser i henhold til direktiv (EU) 2016/1148.

Ved udøvelsen af disse opgaver indgår agenturet og CERT-EU i et struktureret samarbejde med henblik på at udnytte synergier **og undgå overlapning af aktiviteter** [...].

5. [...]

[...]

6. Agenturet tilrettelægger **regelmæssige** [...] cybersikkerhedsøvelser på EU-niveau og støtter medlemsstaterne og Unionens institutioner, agenturer og organer i at tilrettelægge øvelser på deres anmodning. **Sådanne øvelser på EU-plan kan omfatte tekniske, operationelle eller strategiske elementer** [...]. **Hvert andet år tilrettelægges en øvelse i stor skala, der omfatter alle disse elementer.** Agenturet bidrager også til og hjælper med at tilrettelægge, hvor det er relevant, sektorspecifikke cybersikkerhedsøvelser sammen med relevante [...] organisationer, der også kan deltage i [...] cybersikkerhedsøvelser på EU-plan.

7. Agenturet udarbejder **i tæt samarbejde med medlemsstaterne** 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 [...] eller NIS-direktivets centrale kontaktpunkter (**begge på frivillig basis** [...]), Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol og CERT-EU.

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

   a) at samle rapporter fra nationale kilder**, der er delt på frivillig basis,** med henblik på at bidrage til at skabe en fælles situationsforståelse

   b) at 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

c) [...] **på anmodning fra medlemsstaterne at lette** den tekniske håndtering af en hændelse eller en krise, herunder **navnlig** [...] ved at **støtte frivillig** deling af tekniske løsninger mellem medlemsstaterne

d) at støtte **Unionens institutioner, agenturer og organer og, på deres anmodning, medlemsstaterne i** kommunikation til offentligheden om hændelsen eller krisen

e) **på deres anmodning at støtte medlemsstaterne i** afprøvningen [...] af samarbejdsplaner for reaktionen på sådanne hændelser eller kriser.

Artikel 8

*[...] **Marked, cybersikkerhedscertificering og standardisering***

Agenturet skal:

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

1) forberede forslag til europæiske cybersikkerhedscertificeringsordninger for IKT**-processer,** -produkter og -tjenester i **samarbejde med branchen og i** overensstemmelse med 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 **cybersikkerheds**certificerings[...]myndigheder og branchen

3a) anbefale passende tekniske specifikationer til brug for udarbejdelsen af europæiske cybersikkerhedscertificeringsordninger som omhandlet i artikel 47, stk. 1, litra b), i tilfælde, hvor der ikke findes standarder

3b) bidrage til tilstrækkelig kapacitetsopbygning i forbindelse med evaluerings- og certificeringsprocesser ved at samle og offentliggøre retningslinjer og yde støtte til medlemsstaterne på deres anmodning

b) fremme indførelse og udbredelse af europæiske og internationale standarder for risikostyring og sikkerhed af IKT**-processer,** -produkter og -tjenester [...]

ba) 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

c) 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

[...] ***Viden*** *og* **information** [...]

Agenturet skal:

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

b) udføre langsigtede strategiske analyser af cybersikkerhedstrusler og -hændelser for at identificere nye tendenser og bidrage til at forebygge [...] cybersikkerheds**hændelser**

c) i samarbejde med eksperter fra medlemsstaterne levere rådgivning, vejledning og bedste praksis for sikkerheden af net- og informationssystemer, navnlig for sikkerheden af [...] de infrastrukturer, der understøtter sektorerne nævnt i bilag II til direktiv (EU) 2016/1148**, og dem, der anvendes af udbyderne af digitale tjenester nævnt i bilag III i det pågældende direktiv**

d) via en særlig webportal samle, organisere og offentliggøre oplysninger om cybersikkerhed, der leveres af Unionens institutioner, agenturer og organer **og på frivillig basis af medlemsstaterne og private og offentlige interessenter**

e) [...]

f) 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

g) [...].

Artikel 9a

Bevidstgørelse og uddannelse

Agenturet skal:

a) gøre offentligheden bevidst om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere og organisationer

b) i samarbejde med medlemsstaterne og Unionens institutioner, organer, agenturer og branchen tilrettelægge jævnlige informations- og oplysningskampagner for at øge cybersikkerheden og dens synlighed i Unionen

c) bistå medlemsstaterne i deres bestræbelser på at øge bevidstheden om cybersikkerhed og fremme uddannelse i cybersikkerhed

d) støtte en tættere koordinering og udveksling af bedste praksis mellem medlemsstaterne vedrørende uddannelse i og bevidsthed om cybersikkerhed ved at lette oprettelsen og vedligeholdelsen af et netværk af nationale kontaktpunkter.

Artikel 10

[...] ***Forskning og innovation***

I forbindelse med forskning og innovation skal agenturet:

a) 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

b) 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

[...] ***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:

a) 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

b) [...] **inden for de relevante internationale samarbejdsrammer** at fremme udveksling af bedste praksis [...]

c) efter anmodning at stille ekspertise til rådighed for Kommissionen

ca) i samarbejde med Den Europæiske Cybersikkerhedscertificeringsgruppe, der er oprettet i henhold til artikel 53, at yde rådgivning og støtte til Kommissionen i spørgsmål om aftaler om gensidig anerkendelse af cybersikkerhedsattester med tredjelande.

KAPITEL II
AGENTURETS ORGANISATION

Artikel 12

Struktur

Agenturets administrative og ledelsesmæssige struktur består af:

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

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

c) en administrerende direktør, der varetager de ansvarsområder, der er fastsat i artikel 19 [...]

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

da) et netværk af nationale forbindelsesofficerer, som varetager de funktioner, der er fastsat i artikel 20a.

AFDELING 1
BESTYRELSEN

Artikel 13

Bestyrelsens sammensætning

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

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

3. 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.

4. Embedsperioden for medlemmer af bestyrelsen og deres stedfortrædere er fire år. Perioden kan fornys.

Artikel 14

Bestyrelsens opgaver

1. 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

ca) overvåge gennemførelsen af det flerårige og det årlige arbejdsprogram, der er omfattet af det samlede programmeringsdokument

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.

2. 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.

3. 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

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

2. Bestyrelsen afholder mindst to ordinære møder om året. Den afholder endvidere ekstraordinære møder efter anmodning fra formanden, på Kommissionens anmodning eller på anmodning af mindst en tredjedel af dens medlemmer.

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

4. Medlemmerne af Den Stående Gruppe af Interessenter kan efter invitation fra formanden deltage i bestyrelsens møder uden stemmeret.

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

6. Agenturet varetager sekretariatsopgaverne for bestyrelsen.

Artikel 17

Bestyrelsens afstemningsregler

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

2. Der kræves et flertal på to tredjedele af bestyrelsens medlemmer for at vedtage det samlede programmeringsdokument og årsbudgettet og for at udnævne eller afskedige den administrerende direktør eller forlænge dennes embedsperiode.

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

4. Formanden deltager i afstemningen.

5. Den administrerende direktør deltager ikke i afstemningen.

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

AFDELING 2
FORRETNINGSUDVALGET

Artikel 18

Forretningsudvalget

1. Bestyrelsen bistås af et forretningsudvalg.

2. Forretningsudvalget skal:

   a) forberede de afgørelser, der skal træffes af bestyrelsen

   b) 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

   c) 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.

3. 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.

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

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

6. Bestyrelsen vedtager forretningsudvalgets forretningsorden.

7. [...]

AFDELING 3

DEN ADMINISTRERENDE DIREKTØR

Artikel 19

Den administrerende direktørs opgaver

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

2. Den administrerende direktør aflægger rapport til Europa-Parlamentet om udførelsen af sit hverv, når denne anmodes herom. Rådet kan anmode den administrerende direktør om at aflægge rapport om udførelsen af dennes hverv.

3. Den administrerende direktør er ansvarlig for:

a) den daglige administration af 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 årsberetning om agenturets aktiviteter**, bl.a. om gennemførelsen af det årlige arbejdsprogram,** 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

la) den regelmæssige udveksling med EU-institutioner, -agenturer og -organer om deres cybersikkerhedsrelaterede aktiviteter for at sikre sammenhæng i udviklingen og gennemførelsen af EU's politik

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

4. 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.

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

AFDELING 4
DEN STÅENDE GRUPPE AF INTERESSENTER

Artikel 20

Den Stående Gruppe af Interessenter

1. 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, **operatører af væsentlige tjenester,** 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.

2. 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.

3. Den Stående Gruppe af Interessenter ledes af den administrerende direktør eller af en person udpeget af den administrerende direktør fra sag til sag.

4. 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.

5. 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.

5a. Den Stående Gruppe af Interessenter underretter regelmæssigt bestyrelsen om sine aktiviteter.

AFDELING 4A
NETVÆRK AF NATIONALE FORBINDELSESOFFICERER

Artikel 20a

Netværk af nationale forbindelsesofficerer

1. På forslag af den administrerende direktør opretter bestyrelsen et netværk af nationale forbindelsesofficerer bestående af repræsentanter for medlemsstaterne.

2. Netværket af nationale forbindelsesofficerer består af repræsentanter for alle medlemsstaterne. Hver medlemsstat udpeger én repræsentant. Netværkets møder kan afholdes i forskellige ekspertsammensætninger.

3. Netværket af nationale forbindelsesofficerer skal navnlig fremme udvekslingen af oplysninger mellem ENISA og medlemsstaterne. Det støtter især ENISA i formidlingen af dets aktiviteter, resultater og henstillinger i hele EU til de relevante interessenter.

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

5. Mens nationale forbindelsesofficerer bør arbejde tæt sammen med repræsentanterne fra deres respektive lande i bestyrelsen, må det arbejde, som netværket selv udfører, ikke overlappe hverken bestyrelsens eller andre EU-foras arbejde.

6. Funktionerne og procedurerne for netværket af nationale forbindelsesofficerer fastlægges i agenturets interne forretningsgange og offentliggøres.

AFSNIT 5
DRIFT

Artikel 21

Det samlede programmeringsdokument

1. 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.

2. 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[14].

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

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

5. Det årlige arbejdsprogram skal indeholde detaljerede mål og forventede resultater, herunder resultatindikatorer. Det skal også indeholde en beskrivelse af de foranstaltninger, der skal finansieres, og oplysninger om de 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 arbejdsprogram. Det skal klart anføres i programmet, hvilke opgaver der er blevet tilføjet, ændret eller slettet i forhold til det foregående regnskabsår.

---

14 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).

6. 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.

7. 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.

8. 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

1. 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.

2. 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.

3. 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

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

2. 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.

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

4. 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

1. 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.

2. 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).

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

4. Bestyrelsen beslutter, såfremt det er nødvendigt for udførelsen af 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[15] og 2015/444[16]. Disse forretningsgange skal blandt andet indeholde bestemmelser om udveksling, behandling og opbevaring af klassificerede oplysninger.

---

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

16 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).

Artikel 25

Aktindsigt

1. Forordning (EF) nr. 1049/2001 finder anvendelse på agenturets dokumenter.

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

3. 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

1. Hvert år udarbejder den administrerende direktør et udkast til overslag over agenturets indtægter og udgifter for det følgende regnskabsår og forelægger det for bestyrelsen, ledsaget af et udkast til stillingsfortegnelse. Der skal være balance mellem indtægter og udgifter.

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

3. 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.

4. 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.

5. Europa-Parlamentet og Rådet godkender bevillingen af bidraget til agenturet.

6. Europa-Parlamentet og Rådet vedtager agenturets stillingsfortegnelse.

7. 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

1. Med forbehold af andre ressourcer udgøres agenturets indtægter af:

   a) et bidrag fra EU-budgettet

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

   c) 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

d) bidrag fra tredjelande, der deltager i agenturets arbejde i henhold til artikel 39

e) 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.

2. 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

1. Den administrerende direktør er ansvarlig for gennemførelsen af agenturets budget.

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

3. 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.

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

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

6. 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.

7. 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.

8. 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.

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

10. Den administrerende direktør sender senest den 30. september i år N + 1 Revisionsretten et svar på dens bemærkninger og sender ligeledes en kopi af svaret til bestyrelsen og Kommissionen.

11. 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.

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

1. For at lette bekæmpelsen af svig, korruption og andre retsstridige handlinger i henhold til Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013[17] 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.

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

[17] 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).

3. 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[18] 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.

4. 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.

[18] 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

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

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

3. Med henblik på indgåelsen af kontrakten med den administrerende direktør repræsenteres agenturet af formanden for bestyrelsen.

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

5. Den administrerende direktørs embedsperiode er **fire** [...] 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.

6. 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.

7. 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 **fire** [...] år.

8. 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.

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

10. Den administrerende direktør kan kun afskediges ved en afgørelse truffet af bestyrelsen[...].

Artikel 34

Udstationerede nationale eksperter og andet personale

1. 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.

2. Bestyrelsen vedtager en afgørelse, der fastlægger regler for udstationering af nationale eksperter til agenturet.

KAPITEL V
GENERELLE BESTEMMELSER

Artikel 35

Agenturets retlige status

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

2. 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 [...].

3. Agenturet repræsenteres af sin administrerende direktør.

Artikel 36

Agenturets ansvar

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

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

3. 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.

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

5. De ansattes personlige ansvar over for agenturet fastsættes i de ansættelsesvilkår, der gælder for agenturets personale.

Artikel 37

Sprogordning

1. Bestemmelserne i forordning nr. 1 finder anvendelse på agenturet[19]. 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.

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

Artikel 38

Beskyttelse af personoplysninger

1. Agenturets behandling af personoplysninger er omfattet af Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001[20].

2. 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.

---

[19] 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).

[20] 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 39

Samarbejde med tredjelande og internationale organisationer

1. 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.

2. 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.

3. 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.

Artikel 41

Hjemstedsaftale og driftsvilkår

1. 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].

2. Agenturets værtsmedlemsstat [...] sørger for at skabe betingelser [...], der sikrer, 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

Europæisk ramme for cybersikkerhedscertificering[…]

1. **Den europæiske ramme for cybersikkerhedscertificering etableres for at forbedre betingelserne for et velfungerende indre marked ved at øge cybersikkerhedsniveauet i Unionen. Den fastlægger regler, der giver mulighed for en harmoniseret tilgang på EU-niveau for europæiske cybersikkerhedscertificeringsordninger med henblik på at skabe et digitalt indre marked for IKT-processer, -produkter og -tjenester.**

2. **Den europæiske ramme for cybersikkerhedscertificering definerer en mekanisme til fastlæggelse af** [...]europæisk**e** cybersikkerhedscertificeringsordning**er** [...]**og til** attestering af, at IKT-**processer,** -produkter og -tjenester, der er [...]**evalueret** i overensstemmelse med [...] sådanne ordning**er** opfylder de fastlagte **sikkerheds**krav [...] **med henblik på at beskytte** 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 **og** tjenester [...]**i hele deres livscyklus**.

Artikel 44

Forberedelse og vedtagelse af en europæisk cybersikkerhedscertificeringsordning

1. På anmodning fra Kommissionen **eller Den Europæiske Cybersikkerhedscertificeringsgruppe ("gruppen") , der er nedsat ved artikel 53,** skal ENISA udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning, som opfylder kravene i denne forordnings artikel 45, 46 og 47. [...]

1a. Medlemsstaterne eller relevante interesseorganisationer kan foreslå gruppen, at der udarbejdes et forslag til en europæisk cybersikkerhedscertificeringsordning. Gruppen vurderer sådanne forslag ud fra kriterier, som gruppen har defineret ved hjælp af retningslinjer i overensstemmelse med artikel 53, stk. 3, litra ca), og kan anmode ENISA om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning.

2. Under udarbejdelsen af forslaget til den i stk. 1 omhandlede ordning hører ENISA alle relevante interessenter **i gennemsigtige høringsprocesser** og samarbejder tæt med gruppen. Gruppen yder ENISA [...] bistand og ekspertrådgivning [...] i forbindelse med udarbejdelsen af forslaget til en ordning **og vedtager en udtalelse om forslaget til en ordning, før det forelægges for Kommissionen** [...]. **ENISA sikrer, at forslagene til ordninger er i overensstemmelse med den gældende harmoniserede standard, der anvendes til akkreditering af overensstemmelsesvurderingsorganet.**

3. ENISA **tager størst muligt hensyn til gruppens udtalelse, før det** [...] fremsender forslaget til [...] ordning udarbejdet i henhold til stk. 2 til Kommissionen.

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

5. [...]

Artikel 44a

Vedligeholdelse af en europæisk cybersikkerhedscertificeringsordning

1. Agenturet vedligeholder en dedikeret hjemmeside, der oplyser om og reklamerer for de europæiske cybersikkerhedscertificeringsordninger, attester og EU-overensstemmelseserklæringer udstedt i henhold til artikel 47a.

2. Agenturet reviderer i tæt samarbejde med gruppen mindst hvert femte år de vedtagne europæiske cybersikkerhedscertificeringsordninger under hensyntagen til tilbagemeldinger fra interesserede parter. Hvis det anses for nødvendigt, kan Kommissionen eller gruppen anmode agenturet om at påbegynde processen med at udvikle et revideret forslag til ordning i overensstemmelse med artikel 44, stk. 2 og 3.

Artikel 45

Sikkerhedsmålene for de europæiske cybersikkerhedscertificeringsordninger

En europæisk cybersikkerhedscertificeringsordning skal være udformet således at den, alt efter relevans, **som minimum opfylder** [...] følgende sikkerhedsmål:

a) beskyttelse af data, som lagres, overføres eller på anden måde behandles, mod utilsigtet eller uautoriseret lagring, behandling, adgang eller offentliggørelse **i hele processens, produktets eller tjenestens livscyklus**

b) beskyttelse af data, som lagres, overføres eller på anden måde behandles, mod utilsigtet eller uautoriseret ødelæggelse, [...] tab eller ændring **eller manglende tilgængelighed i hele processens, produktets eller tjenestens livscyklus**

c) [...] autoriserede personer, programmer eller maskiner udelukkende kan få adgang til data, tjenester eller funktioner, som de har adgangsret til

d) registrering af, hvilke data, funktioner eller tjenester der er [...] **tilgået, anvendt eller på anden måde behandlet**, på hvilket tidspunkt og af hvem

e) [...] det er muligt at kontrollere, hvilke data, tjenester og funktioner der er tilgået**,** [...] anvendt **eller på anden måde behandlet**, på hvilket tidspunkt og af hvem

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

g) [...] IKT-**processer, -**produkter og -tjenester er forsynet med ajourført software **og hardware, der** ikke indeholder **offentligt** kendte svagheder, og som har mekanismer til sikker opdatering [...]

ga) IKT-processer, -produkter og -tjenester udvikles, fremstilles og leveres i henhold til sikkerhedskravene i den pågældende ordning.

Artikel 46

Tillidsniveauer for de europæiske cybersikkerhedscertificeringsordninger

1. En europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende tillidsniveauer: grundlæggende, betydeligt og/eller højt for IKT-**processer**, -produkter og -tjenester [...]. **Tillidsniveauet står mål med risikoniveauet i forbindelse med den tilsigtede anvendelse af en IKT-proces eller -tjeneste eller et IKT-produkt.**

2. Tillidsniveauerne grundlæggende, betydeligt og højt skal [...] **henvise til en attest eller en EU-overensstemmelseserklæring, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som for hvert enkelt sikkerhedsniveau fastlægger de respektive sikkerhedskrav, herunder sikkerhedsfunktioner og den tilsvarende grad af bestræbelser med henblik på evaluering af en IKT-proces, et IKT-produkt eller en IKT-tjeneste. Attesten eller EU-overensstemmelseserklæringen er karakteriseret ved henvisning til tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at mindske risikoen for eller forhindre cybersikkerhedshændelser som følger:**

a) **en europæisk cybersikkerhedsattest eller EU[...]-overensstemmelseserklæring, der henviser til** tillidsniveauet "grundlæggende"**, giver tillid til, at IKT-processer, -produkter og -tjenester opfylder de respektive sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret til at have et niveau, der sigter mod at minimere de kendte grundlæggende risici for cyberhændelser og cyberangreb. Evalueringsaktiviteterne skal som minimum omfatte en gennemgang af den tekniske dokumentation, eller, hvis dette ikke er relevant, skal de omfatte andre aktiviteter med tilsvarende virkning** [...].

b) **en europæisk cybersikkerhedsattest, der henviser til** tillidsniveauet "betydeligt", **giver tillid til, at IKT-processer, -produkter og -tjenester opfylder de respektive sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret til at have et niveau, der sigter mod at minimere kendte cyberrisici, cyberhændelser og cyberangreb udført af aktører med begrænsede færdigheder og ressourcer. Evalueringsaktiviteterne skal som minimum omfatte: revision af ikkeanvendeligheden af offentligt kendte sårbarheder og afprøvning af, at IKT-processer, -produkter eller -tjenester udfører de nødvendige sikkerhedsfunktioner korrekt; eller hvis det ikke er relevant, skal de omfatte andre aktiviteter med tilsvarende virkning.**[...]

c) **en europæisk cybersikkerhedsattest, der henviser til** tillidsniveauet "højt"**, giver tillid til, at IKT-processer, -produkter og -tjenester opfylder de respektive sikkerhedskrav, herunder sikkerhedsfunktioner, og at de er blevet evalueret til at have et niveau, der sigter mod at minimere risikoen for avancerede cyberangreb udført af aktører med betydelige færdigheder og ressourcer. Evalueringsaktiviteterne skal som minimum omfatte: revision af ikkeanvendeligheden af offentligt kendte sårbarheder, afprøvning af, at IKT-processer, -produkter eller -tjenester udfører den nødvendige sikkerhedsfunktion med den mest avancerede teknologi, og vurdering af deres modstandsdygtighed over for drevne angribere ved hjælp af penetrationstest, eller hvis det ikke er relevant, skal de omfatte andre aktiviteter med tilsvarende virkning** [...].

2a. En europæisk cybersikkerhedscertificeringsordning kan fastsætte flere evalueringsniveauer, alt efter hvor stringent og omfattende den anvendte evalueringsmetodologi er. Hvert enkelt evalueringsniveau skal svare til et af tillidsniveauerne og være defineret ved en passende kombination af tillidskomponenter.

Artikel 47

Elementer i europæiske cybersikkerhedscertificeringsordninger

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

a) certificering**sordningens** genstand og omfang, herunder typer eller kategorier af IKT-**processer, -**produkter og -tjenester, der er omfattet, **samt en uddybning af, hvordan certificeringsordningen opfylder de forventede målgruppers behov**

b) [...] henvisning til [...] internationale, **europæiske eller nationale** standarder, **der er fulgt i evalueringen. Hvis der ikke foreligger standarder, henvises der til** [...] tekniske specifikationer, som opfylder kravene i bilag II til forordning (EU) nr. 1025/2012, eller, hvis sådanne specifikationer ikke foreligger, til tekniske specifikationer eller andre cybersikkerhedskrav, der er fastlagt i ordningen.

c) hvor det er relevant, et eller flere tillidsniveauer

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

d) 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

e) **hvor det er relevant,** oplysninger, som en ansøger skal videresende **eller på anden måde stille til rådighed** for overensstemmelsesvurderingsorganerne, og som er nødvendige med henblik på certificering

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

g) [...] reglerne for overvågning af overensstemmelsen med attesternes **eller EU-overensstemmelseserklæringens** krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav

h) **hvor det er relevant,** betingelserne for udstedelse **og forlængelse af en attest**, **samt** vedligeholdelse, forlængelse, udvidelse **eller** indskrænkning af certificeringens omfang

i) regler om følgerne af certificerede **eller selvvurderede** IKT-produkters og -tjenesters manglende overholdelse af [...]kravene **i ordningen**

j) regler om, hvordan hidtil uopdagede cybersikkerhedssårbarheder i IKT**-processer**, -produkter og -tjenester skal indberettes og håndteres

k) **hvor det er relevant,** reglerne om overensstemmelsesvurderingsorganers opbevaring af optegnelser

l) angivelse af nationale **eller internationale** cybersikkerhedscertificeringsordninger, som dækker samme type eller kategorier af IKT**-processer**, -produkter og -tjenester, s**ikkerhedskrav og evalueringskriterier og -metoder**

m) indholdet af den udstedte attest **eller EU-overensstemmelseserklæringen**

ma) opbevaringsperioden hos producenter eller udbydere af IKT-produkter og -tjenester for EU-overensstemmelseserklæringen og den tekniske dokumentation for alle relevante oplysninger

mb[...]) attesters maksimale gyldighedsperiode

mc[...]) politikken for offentliggørelse af udstedte, ændrede og tilbagekaldte attester

md[...]) betingelserne for gensidig anerkendelse af certificeringsordninger med tredjelande

me[...]) hvor det er relevant, reglerne for en peer review-mekanisme for organer, der udsteder europæiske cybersikkerhedsattester for tillidsniveauet[...] højt i henhold til artikel 48, stk. 4a og 4b.

2. 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.

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

4. 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 47a

Selvvurdering af overensstemmelsesniveauet

1. En europæisk cybersikkerhedscertificeringsordning kan tillade, at der foretages en overensstemmelsesvurdering, som producenter og udbydere af IKT-produkter og tjenester har det fulde ansvar for. En sådan overensstemmelsesvurdering finder kun anvendelse på IKT-produkter og -tjenester med lav risiko svarende til det grundlæggende tillidsniveau.

2. Producenter og udbydere af IKT-produkter og tjenester kan udstede en EU-overensstemmelseserklæring, hvoraf det fremgår, at det er blevet påvist, at de krav, som er fastsat i ordningen, er opfyldt. Ved at udarbejde en sådan erklæring står producenter og udbydere af IKT-produkter og -tjenester inde for, at IKT-produktet eller tjenesten opfylder de krav, der er fastsat i ordningen.

3. Producenter og udbydere af IKT-produkter og -tjenester stiller EU-overensstemmelseserklæringen og den tekniske dokumentation for alle relevante oplysninger vedrørende IKT-produkternes eller -tjenesternes overensstemmelse med en ordning til rådighed for den nationale cybersikkerhedscertificeringsmyndighed som omhandlet i artikel 50, stk. 1, i en periode fastsat i den tilsvarende europæiske cybersikkerhedscertificeringsordning. En kopi af EU-overensstemmelseserklæringen indgives til den nationale cybersikkerhedscertificeringsmyndighed og til ENISA.

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

5. En EU-overensstemmelseserklæring, der er udstedt i henhold til denne artikel, skal anerkendes i alle medlemsstater.

Artikel 48

Cybersikkerhedscertificering

1. IKT**-processer,** -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.

2. Certificeringen skal være frivillig, medmindre andet er fastsat i EU-retten **eller i medlemsstaternes lovgivning**.

3. En europæisk cybersikkerhedsattest i medfør af denne artikel **med henvisning til tillidsniveauet grundlæggende eller tillidsniveauet betydeligt** 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.

4. Uanset [...] stk. 3 kan det i behørigt begrundede tilfælde fastsættes i en europæisk cybersikkerheds**certificerings**ordning, at en europæisk cybersikkerhedsattest, der fremgår af denne ordning, kun kan udstedes af et offentligt organ. Et sådant [...] organ skal være en af følgende:

a) en national **cybersikkerheds**certificerings[...]myndighed som omhandlet i artikel 50, stk. 1

b) et **offentligt** organ, der er akkrediteret som overensstemmelsesvurderingsorgan i medfør af artikel 51, stk. 1 [...]

c) [...].

4a. I tilfælde, hvor en europæisk cybersikkerhedscertificeringsordning i medfør af artikel 44 indeholder krav om et højt tillidsniveau, kan attesten kun udstedes af en national cybersikkerhedscertificeringsmyndighed, jf. artikel 50, stk. 1, eller, på følgende betingelser, af et overensstemmelsesvurderingsorgan, jf. artikel 51:

a) efter at den nationale cybersikkerhedscertificeringsmyndighed på forhånd har godkendt hver enkelt attest, som er udstedt af et overensstemmelsesvurderingsorgan, eller

b) efter at den nationale cybersikkerhedscertificeringsmyndighed på forhånd generelt har overdraget denne opgave til et overensstemmelsesvurderingsorgan.

5. Den fysiske eller juridiske person, der indgiver sine IKT-**processer**, -produkter og -tjenester til certificeringsmekanismen, **gør** [...] alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, **tilgængelige for** det i artikel 51 omhandlede overensstemmelsesvurderingsorgan **eller den i artikel 50 omhandlede nationale cybersikkerhedscertificeringsmyndighed**, **hvis denne myndighed er det organ, der har udstedt attesten**.

5a. Indehaveren af en attest underretter det organ, der har udstedt attesten, om eventuelle senere opdagede sårbarheder eller uregelmæssigheder i forbindelse med den certificerede IKT-proces', det certificerede IKT-produkts eller den certificerede IKT-tjenestes sikkerhed, som kan have en indvirkning på kravene til certificeringen. Organet sender hurtigst muligt disse oplysninger til den nationale cybersikkerhedscertificeringsmyndighed.

6. Attester udstedes for [...] **den periode, som fastsættes af den pågældende certificeringsordning,** og kan forlænges [...], såfremt de relevante krav fortsat er opfyldt.

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

Artikel 49

Nationale cybersikkerhedscertificeringsordninger og -attester

1. Nationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT**-processer,** -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. **N**ationale cybersikkerhedscertificeringsordninger og de tilknyttede procedurer for IKT**-processer,** -produkter og -tjenester, der ikke er omfattet af en europæisk cybersikkerhedscertificeringsordning, fortsætter med at bestå.

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

3. Eksisterende attester udstedt i henhold til en national cybersikkerhedscertificeringsordning **og omfattet af en europæisk cybersikkerhedscertificeringsordning** forbliver gyldige indtil deres udløbsdato.

Artikel 50

Nationale* cybersikkerheds*certificerings[...]myndigheder

1. Hver medlemsstat **[...] udpeger en eller flere** nationale **cybersikkerheds**certificerings[...]myndighed**er på sit område eller udpeger efter gensidig aftale med en anden medlemsstat en eller flere myndigheder, der er etableret i denne anden medlemsstat, som ansvarlig for overvågningsopgaverne i den udpegende medlemsstat**.

2. Hver medlemsstat underretter Kommissionen om de udpegede **myndigheders** identitet **[...] og om de opgaver, de er blevet pålagt.**

3. **Uden at det berører artikel 48, stk. 4, litra a), og artikel 48, stk. 4a,** [...] **skal h**ver national **cybersikkerheds**certificerings[...]myndighed [...] med hensyn til dens organisation, finansieringsbeslutninger, retlige struktur og beslutningstagning være uafhængig af de enheder, som den fører tilsyn med.

3a. Medlemsstaterne sikrer, at den nationale cybersikkerhedscertificeringsmyndigheds aktiviteter i tilknytning til udstedelsen af attester i overensstemmelse med artikel 48, stk. 4, litra a), og artikel 48, stk. 4a, overholder en stringent adskillelse af roller og ansvar med hensyn til tilsynsaktiviteterne i denne artikel, og at begge aktiviteter fungerer uafhængigt af hinanden.

4. Medlemsstaterne sikrer, at de nationale **cybersikkerheds**certificerings[...]myndigheder har tilstrækkelige ressourcer til at udøve deres beføjelser og udføre de opgaver, de er tillagt, på en virkningsfuld og effektiv måde.

5. 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, virkningsfuld og sikker måde.

6. Nationale **cybersikkerheds**certificerings[...]myndigheder skal:

a) [...]

aa) overvåge og håndhæve de forpligtelser, som påhviler producenter og udbydere af IKT-produkter og -tjenester, der er etableret på deres respektive område, som fastsat i artikel 47a, stk. 2 og 3, og i den tilsvarende europæiske cybersikkerhedscertificeringsordning.

b) [...] **bistå de nationale akkrediteringsorganer med overvågning af og tilsyn med** overensstemmelsesvurderingsorganers aktiviteter i forbindelse med denne forordning [...], **uden at det berører artikel 51, stk. 1b**

ba) overvåge og føre tilsyn med de aktiviteter, der udføres af de i artikel 48, stk. 4, omhandlede organer

bb) bemyndige overensstemmelsesvurderingsorganer, jf. artikel 51, stk. 1b, og begrænse, suspendere eller tilbagekalde eksisterende bemyndigelse i tilfælde af manglende overholdelse af kravene i denne forordning

c) behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af [...] **den nationale cybersikkerhedscertificeringsmyndighed eller, i overensstemmelse med artikel 48, stk. 4a, af overensstemmelsesvurderingsorganer,** [...] undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist

d) samarbejde med andre nationale **cybersikkerheds**certificerings[...]myndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-**processers,** -produkters og -tjenesters manglende overholdelse af denne forordnings eller specifikke europæiske cybersikkerhedscertificeringsordningers krav

e) overvåge den relevante udvikling på cybersikkerhedscertificeringsområdet.

7. Hver national **cybersikkerheds**certificerings[...]myndighed skal mindst have følgende beføjelser:

a) at kunne anmode overensstemmelsesvurderingsorganer**,** [...] indehavere af en europæisk cybersikkerhedsattest **og udstedere af EU-overensstemmelseserklæringer** om at forelægge alle oplysninger, som er nødvendige for udførelsen af dens opgaver

b) at kunne udføre undersøgelser i form af audit af overensstemmelsesvurderingsorganer, [...] indehavere af en europæisk cybersikkerhedsattest **og udstedere af EU-overensstemmelseserklæringer** med henblik på at verificere overholdelsen af bestemmelserne i afsnit III

c) at kunne træffe passende foranstaltninger, i overensstemmelse med national ret, til at sikre, at overensstemmelsesvurderingsorganer, [...] indehavere af en attest **og udstedere af EU-overensstemmelseserklæringer** overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning

d) 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

e) at kunne tilbagekalde, i overensstemmelse med national ret, attester, **der er udstedt af den nationale cybersikkerhedscertificeringsmyndighed eller, i overensstemmelse med artikel 48, stk. 4a, af overensstemmelsesvurderingsorganer,** som ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning

f) 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.

8. De nationale **cybersikkerheds**certificerings[...]myndigheder 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**-processer,** -produkter og -tjenester.

Artikel 51

Overensstemmelsesvurderingsorganer

1. 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.

1a. I tilfælde, hvor en europæisk cybersikkerhedsattest udstedes af en national cybersikkerhedscertificeringsmyndighed i henhold til artikel 48, stk. 4, litra a), og artikel 48, stk. 4a, akkrediteres den nationale cybersikkerhedscertificeringsmyndigheds certificeringsorgan som overensstemmelsesvurderingsorgan i henhold til denne artikels stk. 1.

1b. Hvis det er relevant, bemyndiges overensstemmelsesvurderingsorganerne af den nationale cybersikkerhedscertificeringsmyndighed til at udføre dens opgaver, hvis disse opfylder specifikke eller yderligere krav, som er fastsat i den europæiske certificeringsordning i henhold til artikel 47, stk. 1, litra ca).

2. 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 **træffer inden for en rimelig tidsfrist alle passende foranstaltninger med henblik på at begrænse, suspendere eller** tilbagekalde 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

1. For hver europæisk cybersikkerhedscertificeringsordning, som vedtages i henhold **til** artikel 44, underretter de nationale **cybersikkerheds**certificerings[...]myndigheder Kommissionen om de [...] overensstemmelsesvurderingsorganer, der er akkrediteret **og, hvor det er relevant, bemyndiget i henhold til artikel 51, stk. 1b,** til at udstede attester på specifikke tillidsniveauer, jf. artikel 46, og hurtigst muligt om eventuelle senere ændringer heraf.

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

3. Modtager Kommissionen en anmeldelse efter udløbet af den periode, der er omhandlet 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.

4. En national **cybersikkerheds**certificerings[...]myndighed kan anmode Kommissionen om at fjerne et overensstemmelsesvurderingsorgan, der er anmeldt af den pågældende medlemsstat, 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 **cybersikkerheds**certificerings[...]myndigheds anmodning.

5. 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

1. Den Europæiske Cybersikkerhedscertificeringsgruppe (gruppen") oprettes.

2. Gruppen sammensættes af **repræsentanter for** nationale **cybersikkerheds**certificerings[...]myndigheder **eller repræsentanter for andre relevante nationale myndigheder.** [...] **Et medlem af gruppen kan ikke repræsentere mere end én anden medlemsstat.**

3. Gruppen har følgende opgaver:

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

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

ba) at vedtage en udtalelse om forslaget til ordning i henhold til artikel 44

c) at [...] **anmode** agenturet om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning i overensstemmelse med artikel 44

ca) at udvikle og vedtage retningslinjer om kriterier for vurdering af forslag til udarbejdelse af forslag til ordning, som indsendes til [...] gruppen i henhold til artikel 44, stk. 1a

d) at vedtage udtalelser til Kommissionen vedrørende vedligeholdelse og revision af eksisterende europæiske cybersikkerhedscertificeringsordninger

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

f) at fremme samarbejdet mellem nationale **cybersikkerheds**certificerings[...]myndigheder i medfør af dette afsnit gennem **kapacitetsopbygning,** udveksling af oplysninger, herunder navnlig ved at indføre metoder til effektiv udveksling af oplysninger vedrørende cybersikkerhedscertificeringsanliggender

fa) at yde støtte til gennemførelsen af peer review-mekanismen i overensstemmelse med de regler, som er fastsat i en europæisk cybersikkerhedscertificeringsordning i henhold til artikel 47, stk. 1, litra md).

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

Artikel 53a

Retten til at indgive en klage til en national **cybersikkerheds** ***certificerings[...]myndighed***

1. Fysiske eller juridiske personer har ret til at indgive en klage til den nationale cybersikkerhedscertificeringsmyndighed vedrørende en attest, som er udstedt af samme myndighed eller, i overensstemmelse med artikel 48, stk. 4a, af overensstemmelsesvurderingsorganer.

2. Den nationale cybersikkerhedscertificeringsmyndighed, som klagen er indgivet til, underretter klageren om forløbet og resultatet af klagen, herunder om muligheden for anvendelse af retsmidler, jf. artikel 53b.

Artikel 53b

Retten til effektive retsmidler

1. Fysiske eller juridiske personer har ret til effektive retsmidler over for en juridisk bindende afgørelse truffet af en national cybersikkerhedscertificeringsmyndighed angående dem.

2. Fysiske eller juridiske personer har ret til effektive retsmidler, hvis den nationale cybersikkerhedscertificeringsmyndighed ikke behandler en klage.

3. En sag mod en national cybersikkerhedscertificeringsmyndighed skal anlægges ved domstolen i den medlemsstat, hvor myndigheden er etableret.

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

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

2. Når der henvises til dette stykke, finder artikel 5**, stk. 4, litra b),** i forordning (EU) nr. 182/2011, anvendelse.

Artikel 56

Evaluering og revision

1. 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.

2. 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.

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

Artikel 57

Ophævelse og afløsning

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

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

3. 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.

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

5. 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.

6. 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

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

1a. Denne forordning finder anvendelse fra den [...] med undtagelse af artikel 50, 51, 52, 53a, 53b og 54, som finder anvendelse fra den [24 måneder efter offentliggørelsen i Den Europæiske Unions Tidende].

2. 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*

KRAV, DER SKAL OPFYLDES AF OVERENSSTEMMELSESVURDERINGSORGANER

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

1. Et overensstemmelsesvurderingsorgan skal oprettes i henhold til national lovgivning og være en juridisk person.

2. Et overensstemmelsesvurderingsorgan skal være et tredjepartsorgan, der er uafhængigt af den organisation eller de IKT-produkter eller -tjenester, det vurderer.

3. Et organ, der er medlem af en erhvervsorganisation og/eller brancheforening, som repræsenterer virksomheder, der er involveret i konstruktion, fremstilling, levering, sammenbygning, brug eller vedligeholdelse af IKT-produkter eller -tjenester, som det vurderer, kan, forudsat at det er påvist, at det er uafhængigt, og at der ikke er tale om interessekonflikter, anses for at være et overensstemmelsesvurderingsorgan.

4. Et overensstemmelsesvurderingsorgan, dets øverste ledelse og det personale, der er ansvarligt for udførelsen af overensstemmelsesvurderingsopgaverne, må ikke være konstruktør, fabrikant, leverandør, installatør, køber, ejer, bruger eller vedligeholder af de produkter, der vurderes, eller repræsentere nogen af disse parter. Dette udelukker ikke, at overensstemmelsesvurderingsorganet bruger vurderede produkter, der er nødvendige for, at det kan udføre sit arbejde, eller personlig brug af sådanne produkter.

5. Et overensstemmelsesvurderingsorgan, dets øverste ledelse og det personale, der er ansvarligt for at udføre overensstemmelsesvurderingsopgaverne, må ikke være direkte involveret i udformning, fremstilling eller konstruktion, markedsføring, installering, anvendelse eller vedligeholdelse af IKT-produkterne eller -tjenesterne eller repræsentere parter, der er involveret i disse aktiviteter. De må ikke deltage i aktiviteter, som kan være i strid med deres objektivitet og integritet i forbindelse med de overensstemmelsesvurderingsaktiviteter, de er bemyndiget til at udføre. Dette gælder navnlig rådgivningstjenester.

6. Overensstemmelsesvurderingsorganet skal sikre, at dets dattervirksomheders eller underentreprenørers aktiviteter ikke påvirker fortroligheden, objektiviteten og uvildigheden af dets overensstemmelsesvurderingsaktiviteter.

7. Overensstemmelsesvurderingsorganet og dets personale skal udføre overensstemmelsesvurderingsaktiviteterne med den størst mulige faglige integritet og den nødvendige tekniske kompetence på det specifikke område og ikke påvirkes af nogen form for pression og incitament, herunder af økonomisk art, som kan have indflydelse på deres afgørelser eller resultaterne af deres overensstemmelsesvurderingsaktiviteter, særlig fra personer eller grupper af personer, som har en interesse i resultaterne af disse aktiviteter.

8. Et overensstemmelsesvurderingsorgan skal kunne gennemføre alle de overensstemmelsesvurderingsopgaver, som pålægges det i henhold til denne forordning, uanset om disse opgaver udføres af overensstemmelsesvurderingsorganet selv eller på dets vegne og på dets ansvar.

9. Til enhver tid og for hver overensstemmelsesvurderingsprocedure og hver art, kategori eller underkategori af IKT-produkter og -tjenester skal overensstemmelsesvurderingsorganet have følgende til rådighed:

a) personale med teknisk viden og tilstrækkelig og relevant erfaring til at udføre overensstemmelsesvurderingsopgaverne

b) beskrivelser af de procedurer, i overensstemmelse med hvilke overensstemmelsesvurdering foretages, og som sikrer gennemsigtighed i og mulighed for at reproducere disse procedurer. Det skal have indført hensigtsmæssige politikker og procedurer, som skelner mellem de opgaver, som det udfører i sin egenskab af bemyndiget organ, og andre aktiviteter

c) procedurer, der sætter det i stand til at udføre sine aktiviteter under behørig hensyntagen til en virksomheds størrelse, den sektor, som den opererer inden for, og dens struktur, til det pågældende IKT-produkts eller -tjenestes kompleksitet og til fremstillingsprocessens seriemæssige karakter.

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

11. Det personale, som skal udføre overensstemmelsesvurderingsaktiviteterne, skal have:

a) en god teknisk og faglig uddannelse omfattende alle overensstemmelsesvurderingsaktiviteter

b) et tilstrækkeligt kendskab til kravene vedrørende de vurderinger, de foretager, og den nødvendige bemyndigelse til at udføre sådanne vurderinger

c) et tilstrækkeligt kendskab til og en tilstrækkelig forståelse af de gældende krav og prøvningsstandarder

d) den nødvendige færdighed i at udarbejde de attester, redegørelser og rapporter, som dokumenterer, at vurderingerne er blevet foretaget.

12. Der skal være sikkerhed for overensstemmelsesvurderingsorganernes, deres øverste ledelses og vurderingspersonalets uvildighed.

13. Aflønningen af et overensstemmelsesvurderingsorgans øverste ledelse og vurderingspersonale må ikke afhænge af, hvor mange vurderinger de udfører, eller hvordan vurderingerne falder ud.

14. Overensstemmelsesvurderingsorganer skal tegne en ansvarsforsikring, medmindre staten er ansvarlig i henhold til national lovgivning, eller medlemsstaten selv er direkte ansvarlig for overensstemmelsesvurderingen.

15. Et overensstemmelsesvurderingsorgans personale har tavshedspligt med hensyn til alle oplysninger, det kommer i besiddelse af ved udførelsen af dets opgaver i henhold til denne forordning eller enhver bestemmelse i en national lov, som gennemfører den, undtagen over for de kompetente myndigheder i den medlemsstat, hvor aktiviteterne udføres.

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

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