**ÆNDRINGSFORSLAG 001-257**
af Udvalget om Industri, Forskning og Energi

**Betænkning**
**Angelika Niebler** **A8-0264/2018**
EU's forordning om cybersikkerhed

Forslag til forordning (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

---

**Ændringsforslag 1**

**Forslag til forordning**
**Betragtning 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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 ***(IKT)*** er grundlaget for de komplekse systemer, som understøtter samfundets ***hverdagsaktiviteter***, og sørger for, at vore økonomier fungerer inden for vigtige sektorer såsom sundhed, energi, finans og transport, og understøtter navnlig det indre markeds funktion. |

**Ændringsforslag 2**

**Forslag til forordning**
**Betragtning 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|

| | |
|---|---|
| (2) Borgerne, erhvervslivet og myndighederne i EU benytter i stort omfang net- og informationssystemer. Digitalisering og forbindelsesmuligheder er centrale elementer i et stadigt stigende antal produkter og tjenester og med fremkomsten af tingenes Internet (IoT) forventes millioner eller endog milliarder styk forbundet digitalt udstyr at blive udbredt i hele EU i løbet af det næste årti. Stadigt mere udstyr er forbundet til Internettet, men der tages ikke tilstrækkeligt hensyn til sikkerhed og modstandsdygtighed i udformningen, hvilket medfører utilstrækkelig cybersikkerhed. I denne forbindelse fører den begrænsede anvendelse af certificering til, at organisationer og individuelle brugere får utilstrækkelige oplysninger om IKT-produkters og -tjenesters cybersikkerhedsfunktioner, hvilket undergraver tilliden til digitale løsninger. | (2) Borgerne, erhvervslivet og myndighederne i EU benytter i stort omfang net- og informationssystemer. Digitalisering og forbindelsesmuligheder er centrale elementer i et stadigt stigende antal produkter og tjenester og med fremkomsten af tingenes Internet (IoT) forventes millioner eller endog milliarder styk forbundet digitalt udstyr at blive udbredt i hele EU i løbet af det næste årti. Stadigt mere udstyr er forbundet til Internettet, men der tages ikke tilstrækkeligt hensyn til sikkerhed og modstandsdygtighed i udformningen, hvilket medfører utilstrækkelig cybersikkerhed. I denne forbindelse fører den begrænsede anvendelse af certificering til, at organisationer og individuelle brugere får utilstrækkelige oplysninger om IKT-produkters***, -processers*** og -tjenesters cybersikkerhedsfunktioner, hvilket undergraver tilliden til digitale løsninger. ***Denne ambition er kernen i Kommissionens reformdagsorden for at opnå et digitalt indre marked, da IKT-nettene er grundlaget for digitale produkter og tjenester, som kan være os til hjælp på alle områder af tilværelsen og være drivkraft i den økonomiske vækst i Europa. For at sikre, at det digitale indre markeds målsætninger opfyldes fuldt ud, skal der indføres vigtige teknologiske byggesten, som vigtige områder, såsom e-sundhed, tingenes internet, kunstig intelligens, Quantum-teknologi samt intelligente transportsystemer og avancerede produktionsmetoder, er afhængige af.*** |

**Ændringsforslag 3**

**Forslag til forordning**
**Betragtning 3**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (3) Øget digitalisering og konnektivitet medfører øgede cybersikkerhedsrisici, hvilket gør samfundet som helhed mere | (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. | 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. ***I denne forbindelse er handlingsplanen for digital uddannelse, som Kommissionen offentliggjorde den 17. januar 2018, et skridt i den rigtige retning, navnlig den EU-dækkende oplysningskampagne rettet mod undervisere, forældre og lærende for at fremme onlinesikkerhed, cyberhygiejne og mediekendskab og et initiativ til undervisning i cybersikkerhed, som bygger på den digitale kompetenceramme for borgerne, for at sætte dem i stand til at anvende teknologi på en sikker og ansvarlig måde.*** |

**Ændringsforslag 4**

**Forslag til forordning**
**Betragtning 3 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(3 a) ENISA's mål og opgaver bør bringes i bedre overensstemmelse med den fælles meddelelse, hvad angår henvisningen til at fremme cyberhygiejne og bevidstgørelse. Cyberrobusthed kan opnås ved at indføre grundlæggende principper for cyberhygiejne.*** |

**Ændringsforslag 5**

**Forslag til forordning**
**Betragtning 3 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
| --- | --- |
| | ***(3b) ENISA bør give mere praktisk og informationsbaseret støtte til Unionens cybersikkerhedsindustri, navnlig til SMV'er og nystartede virksomheder, som er centrale kilder til innovative løsninger på cyberforsvarsområdet, og bør fremme et tættere samarbejde med universiteters forskningsorganisationer og store aktører med henblik på at mindske afhængigheden af cybersikkerhedsprodukter fra eksterne kilder og for at skabe en strategisk forsyningskæde inden for Unionen.*** |

**Ændringsforslag 6**

**Forslag til forordning**
**Betragtning 4**

| *Kommissionens forslag* | *Ændringsforslag* |
| --- | --- |
| (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. | (4) Mængden af cyberangreb er stigende og netforbundne økonomier og samfund, som er mere sårbare over for cybertrusler og -angreb, kræver stærkere ***og mere sikre*** 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***. Uddannelsesbehovet på cyberforsvarsområdet er omfattende og stigende og opfyldes mest virkningsfuldt i fællesskab på EU-plan.*** 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.

**Ændringsforslag 7**

**Forslag til forordning**
**Betragtning 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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, koordinering og ***informationsdeling*** 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***, samtidig med at vigtigheden af at opretholde og yderligere styrke de nationale kapaciteter til at reagere på cybertrusler af ethvert omfang skal understreges***. Der er også behov for yderligere bestræbelser på at ***give en koordineret EU-respons og*** øge borgernes og virksomhedernes kendskab til cybersikkerhed. ***Eftersom cyberhændelser undergraver*** tilliden til ***digitale tjenesteudbydere og til selve*** det digitale indre marked, ***især blandt forbrugerne,*** bør ***tilliden desuden*** forbedres yderligere ved at give gennemsigtige oplysninger om sikkerhedsniveauet af IKT-produkter***, -processer og -tjenester, idet det understreges, at selv et højt niveau for cybersikkerhedscertificering ikke kan garantere, at et IKT-produkt eller en IKT-*** |

***tjeneste er fuldt sikret***. Det kan fremmes ved EU-certificering, der anvender fælles cybersikkerhedskrav og evalueringskriterier på tværs af nationale markeder og sektorer***, samt ved fremme af cyberfærdigheder***. ***Sideløbende med EU-dækkende certificering og i betragtning af den voksende tilgængelighed af IoT-apparater er der en række frivillige foranstaltninger, som den private sektor bør træffe for at styrke tilliden til IKT-produkters, -processers og -tjenesters sikkerhed såsom kryptering og blockchainteknologier. Udfordringerne bør afspejles tilsvarende i det budget, der tildeles agenturet, så det sikres optimal funktionsevne under de aktuelle omstændigheder.***

**Ændringsforslag 8**

**Forslag til forordning**
**Betragtning 5 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(5 a) Med henblik på styrkelsen af de europæiske sikkerheds- og cyberforsvarsstrukturer er det vigtigt at opretholde og udvikle medlemsstaternes kapaciteter til på en fyldestgørende måde at reagere på cybertrusler, herunder grænseoverskridende hændelser, mens agenturets koordinering på EU-plan ikke bør medføre, at medlemsstaternes kapaciteter eller bestræbelser mindskes.*** |

**Ændringsforslag 9**

**Forslag til forordning**
**Betragtning 5 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(5b) Virksomheder samt den enkelte forbruger bør modtage præcise oplysninger om sikkerhedsniveauet for deres IKT-produkter. Samtidig er det*** |

***vigtigt at forstå, at intet produkt er cybersikkert, og at det er nødvendigt at fremme og prioritere grundlæggende regler for cyberhygiejne.***

**Ændringsforslag 10**

**Forslag til forordning**
**Betragtning 7**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (7) Unionen har gjort en stor indsats for at sikre cybersikkerheden og øge tilliden til de digitale teknologier. I 2013 blev EU's strategi for cybersikkerhed vedtaget for at vejlede Unionens politiske reaktion på cybersikkerhedstrusler og -risici. Som led i indsatsen for at beskytte EU's borgere bedre online vedtog Unionen i 2016 den første retsakt inden for cybersikkerhed, nemlig direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet). Ved NIS-direktivet blev der indført krav om nationale kapaciteter på cybersikkerhedsområdet, de første mekanismer til bedre strategisk og operationelt samarbejde mellem medlemsstaterne blev indført, og der blev indført forpligtelser vedrørende sikkerhedsforanstaltninger og anmeldelse af hændelser i sektorer af afgørende betydning for økonomien og samfundet såsom energi, transport, vand, bankvirksomhed, finansmarkedsinfrastrukturer, sundhed og digital infrastruktur samt for udbydere af digitale tjenester (dvs. søgemaskiner, cloud computing-tjenester og onlinemarkedspladser). ENISA fik tildelt en central rolle som støtte for gennemførelsen af dette direktiv. Hertil kommer, at den effektive bekæmpelse af cyberkriminalitet er en vigtig prioritet på den europæiske dagsorden om sikkerhed og bidrager til det overordnede mål om at | (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). NIS-direktivet ***– hvis succes er dybt afhængig af en effektiv gennemførelse fra medlemsstaternes side – opfylder det digitale indre markeds strategi og indfører sammen med andre instrumenter, såsom direktivet om en europæisk kodeks for elektronisk kommunikation, forordning (EU) 2016/679 og direktiv 2002/58/EF,*** krav om nationale kapaciteter på cybersikkerhedsområdet, de første mekanismer til bedre strategisk og operationelt samarbejde mellem medlemsstaterne blev indført, og der blev indført forpligtelser vedrørende sikkerhedsforanstaltninger og anmeldelse af hændelser i sektorer af afgørende betydning for økonomien og samfundet såsom energi, transport, vand, bankvirksomhed, finansmarkedsinfrastrukturer, sundhed og digital infrastruktur samt for udbydere af digitale tjenester (dvs. søgemaskiner, cloud computing-tjenester og |

nå et højere niveau af cybersikkerhed.

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.

**Ændringsforslag 11**

**Forslag til forordning**
**Betragtning 8**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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 ***i forbindelse med den positive rolle, som agenturet har spillet gennem årene med hensyn til pooling af ekspertise, koordinering, kapacitetsopbygning, samt*** 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. |

**Ændringsforslag 12**

**Forslag til forordning**
**Betragtning 11**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (11) I betragtning af de tiltagende ***trusler og*** 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***, hvorved ENISA sættes i stand til effektivt at udføre de opgaver, der tillægges det gennem nærværende forordning***. |

**Ændringsforslag 13**

**Forslag til forordning**
**Betragtning 12**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (12) Agenturet bør udvikle og fastholde et højt ekspertiseniveau og fungere som et referencepunkt og skabe tillid til det indre marked i kraft af sin uafhængighed, kvaliteten af den rådgivning, det yder, og af de informationer, det videregiver, samt i kraft af den åbenhed, der er forbundet med dets procedurer og drift, og dets omhu ved udførelsen af sine opgaver. Agenturet bør proaktivt bidrage til medlemsstaternes og Unionens indsats og udføre sine opgaver i fuldt samarbejde med Unionens institutioner, organer, kontorer og agenturer og medlemsstaterne. Herudover bør agenturet bygge på bidrag fra og samarbejde med den private sektor og andre relevante interessenter. ***Som grundlag for***, ***hvordan*** agenturet skal nå ***sine mål***, bør ***der fastlægges et sæt opgaver, der samtidig giver agenturet*** fleksibilitet ***i*** dets aktiviteter. | (12) Agenturet bør udvikle og fastholde et højt ekspertiseniveau og fungere som et referencepunkt og skabe tillid til det indre marked i kraft af sin uafhængighed, kvaliteten af den rådgivning, det yder, og af de informationer, det videregiver, samt i kraft af den åbenhed, der er forbundet med dets procedurer og drift, og dets omhu ved udførelsen af sine opgaver. Agenturet bør proaktivt bidrage til medlemsstaternes og Unionens indsats og udføre sine opgaver i fuldt samarbejde med EU's institutioner, organer, kontorer og agenturer og medlemsstaterne ***og herved undgå dobbeltarbejde, fremme synergi og komplementaritet og dermed opnå koordinering og finanspolitiske besparelser***. Herudover bør agenturet bygge på bidrag fra og samarbejde med den private ***og den offentlige*** sektor og andre relevante interessenter. ***En klar dagsorden og et sæt opgaver og mål***, ***som*** agenturet skal nå***, og hvordan det skal nå dem***, bør ***fastlægges på en klar måde under behørig hensyntagen til den*** fleksibilitet***, der er nødvendig for*** dets aktiviteter. ***Hvor det er muligt, bør den*** |

***højeste grad af gennemsigtighed og formidling af oplysninger opretholdes.***

**Ændringsforslag 14**

**Forslag til forordning**
**Betragtning 12 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(12 a) Agenturets rolle bør være underlagt løbende vurdering og rettidig revision, navnlig hvad angår dets koordinerende rolle i forhold til medlemsstaterne og deres nationale myndigheder og hvad angår muligheden for at fungere som kvikskranke for medlemsstaterne og EU's organer og institutioner. Agenturets rolle med hensyn til at undgå opsplitning af det indre marked og den mulige indførelse af obligatoriske cybersikkerhedscertificeringsordninger, hvis situationen i fremtiden kræver et sådant skift, bør også vurderes, samt agenturets rolle med hensyn til vurderingen af tredjelandsprodukter, der indføres på EU-markedet, og en mulig sortlistning af virksomheder, der ikke opfylder EU-kriterierne.*** |

**Ændringsforslag 15**

**Forslag til forordning**
**Betragtning 12 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(12b) Med henblik på at være i stand til at yde medlemsstaterne tilstrækkelig støtte til det operationelle samarbejde bør ENISA yderligere styrke sin egen tekniske kapacitet og ekspertise. Med dette for øje bør agenturet gradvist styrke sit personale, der beskæftiger sig med denne opgave, således at agenturet kan indsamle og analysere forskellige typer af en bred*** |

| | |
|---|---|
| | ***vifte af cybersikkerhedstrusler og malware, foretage retsmedicinske analyser og bistå medlemsstaterne i forbindelse med håndteringen af væsentlige hændelser. For at undgå overlapning af eksisterende kapaciteter i medlemsstaterne bør ENISA øge sin knowhow og kapacitet på grundlag af de eksisterende ressourcer i medlemsstaterne, navnlig ved at udstationere nationale eksperter til agenturet, oprette puljer af eksperter, udvikle personaleudvekslingsprogrammer osv. Når agenturet udvælger det personale, der er ansvarligt på dette område, bør det løbende sikre, at de ansatte opfylder de relevante kriterier for at yde passende støtte.*** |

**Ændringsforslag 16**

**Forslag til forordning**
**Betragtning 13**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (13) Agenturet bør bistå Kommissionen ved at levere rådgivning, udtalelser og analyser om alle EU-spørgsmål vedrørende udvikling af politik og lovgivning samt ajourføring og revision på cybersikkerhedsområdet, herunder beskyttelse af kritisk informationsinfrastruktur og cybermodstandsdygtighed. Agenturet bør fungere som et referencepunkt for rådgivning og ekspertise for de sektorspecifikke politikker og lovgivningsinitiativer i tilfælde, hvor cybersikkerhed er involveret. | (13) Agenturet bør bistå Kommissionen ved at levere rådgivning, udtalelser og analyser om alle EU-spørgsmål vedrørende udvikling af politik og lovgivning samt ajourføring og revision på cybersikkerhedsområdet, herunder beskyttelse af kritisk informationsinfrastruktur og cyberrobusthed. Agenturet bør fungere som et referencepunkt for rådgivning og ekspertise for de sektorspecifikke politikker og lovgivningsinitiativer i tilfælde, hvor cybersikkerhed er involveret. ***Der vil især være behov for dets ekspertise i forbindelse med forberedelsen af EU's flerårige arbejdsprogram for europæiske cybersikkerhedscertificeringsordninger. Agenturet bør regelmæssigt forsyne Europa-Parlamentet med ajourføringer, analyser og revisioner på cybersikkerhedsområdet samt med oplysninger om udviklingen i dets*** |

***opgaver.***

**Ændringsforslag 17**

**Forslag til forordning**
**Betragtning 14**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (14) Agenturets grundlæggende opgave er at fremme en konsekvent gennemførelse af den relevante retlige ramme, herunder navnlig en effektiv gennemførelse af NIS-direktivet, som er afgørende for at øge cybermodstandsdygtigheden. På baggrund af det hurtigt skiftende cybersikkerhedstrusselsbillede står det klart, at medlemsstaterne må støttes med en mere overgribende tværpolitisk tilgang til opbygningen af cybermodstandsdygtighed. | (14) Agenturets grundlæggende opgave er at fremme en konsekvent gennemførelse af den relevante retlige ramme, herunder navnlig en effektiv gennemførelse af NIS-direktivet, ***direktivet om en europæisk kodeks for elektronisk kommunikation, forordning (EU) 2016/679 og direktiv 2002/58/EF,*** 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. |

**Ændringsforslag 18**

**Forslag til forordning**
**Betragtning 15**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (15) Agenturet bør bistå medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer med at opbygge og forbedre deres kapacitet og beredskab med sigte på at forebygge, opdage og imødegå cybersikkerhedsproblemer og -hændelser og i forbindelse med sikkerheden af net- og informationssystemer. Agenturet bør især støtte udvikling og forbedring af nationale CSIRT'er for at nå et højt fælles niveau af deres modenhed i Unionen. Agenturet bør også bistå med udviklingen og ajourføringen af Unionens og medlemsstaternes strategier for net- og informationssystemers sikkerhed, herunder navnlig cybersikkerhed, fremme deres udbredelse og følge op på deres | (15) Agenturet bør bistå medlemsstaterne og EU's institutioner, organer, kontorer og agenturer med at opbygge og forbedre deres kapacitet og beredskab med sigte på at forebygge, opdage og imødegå cybersikkerhedsproblemer og -hændelser og i forbindelse med sikkerheden af net- og informationssystemer. Agenturet bør især støtte udvikling og forbedring af nationale CSIRT'er for at nå et højt fælles niveau af deres modenhed i Unionen. Agenturet bør også bistå med udviklingen og ajourføringen af Unionens og medlemsstaternes strategier for net- og informationssystemers sikkerhed, herunder navnlig cybersikkerhed, fremme deres udbredelse og følge op på deres |

| | |
|---|---|
| gennemførelse. ***Agenturet*** bør også tilbyde uddannelse og uddannelsesmateriale til offentlige organer og i ***givet fald*** "uddanne underviserne" med sigte på at bistå medlemsstaterne med at udvikle deres egne uddannelseskapaciteter. | gennemførelse. ***Eftersom menneskelige fejl udgør en af de mest oplagte risici med hensyn til cybersikkerheden,*** bør ***agenturet*** også tilbyde uddannelse og uddannelsesmateriale til offentlige organer og i ***videst muligt omfang*** "uddanne underviserne" med sigte på at bistå medlemsstaterne ***og EU's institutioner og agenturer*** med at udvikle deres egne uddannelseskapaciteter. ***Agenturet bør også tjene som et kontaktpunkt for medlemsstaterne og EU's institutioner, der bør kunne anmode agenturet om assistance inden for rammerne af de beføjelser og roller, der tillægges dette.*** |

**Ændringsforslag 19**

**Forslag til forordning**
**Betragtning 18**

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

**Ændringsforslag 20**

**Forslag til forordning**
**Betragtning 19**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (19) Agenturet bør bidrage til en respons på EU-niveau i tilfælde af væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser. Denne funktion bør omfatte indsamling af | (19) Agenturet bør bidrage til en respons på EU-niveau i tilfælde af væsentlige grænseoverskridende cybersikkerhedshændelser og -kriser. Denne funktion bør omfatte ***indkaldelse af*** |

| | |
|---|---|
| relevante oplysninger og etablering af kontakt mellem CSIRT-netværket og tekniske kredse samt de beslutningstagere, der er ansvarlige for krisestyringen. Derudover kunne agenturet støtte håndteringen af hændelser fra et teknisk synspunkt ved at fremme udveksling af relevante tekniske løsninger mellem medlemsstaterne og ved at komme med input til kommunikation med offentligheden. Agenturet bør støtte processen ved at afprøve metoderne for et sådant samarbejde gennem årlige cybersikkerhedsøvelser. | ***medlemsstaternes myndigheder til møde og bistand ved koordineringen af deres respons,*** 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***, f.eks.*** ved at fremme udveksling af relevante tekniske løsninger mellem medlemsstaterne og ved at komme med input til kommunikation med offentligheden. Agenturet bør støtte processen ved at afprøve metoderne for et sådant samarbejde gennem årlige cybersikkerhedsøvelser. ***Agenturet bør respektere medlemsstaternes beføjelser med hensyn til cybersikkerhed, navnlig hvad angår beføjelser vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område.*** |

**Ændringsforslag 21**

**Forslag til forordning**
**Betragtning 25**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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 ***og oplysninger, der er relevante for den offentlige sikkerhed***. |

**Ændringsforslag 22**

**Forslag til forordning**
**Betragtning 26**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|

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

**Ændringsforslag 23**

**Forslag til forordning**
**Betragtning 27**

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

| | |
|---|---|
| | ***oplysninger om cybersikkerhedsrisici og potentielle løsninger bør medlemsstaterne have lettere ved at styrke deres kapacitet og koordinere praksis og derved øge deres samlede modstandsdygtighed over for cyberangreb.*** |

**Ændringsforslag 24**

**Forslag til forordning**
**Betragtning 28**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (28) Agenturet bør bidrage til at bevidstgøre offentligheden ***om risiciene i forbindelse med cybersikkerhed*** og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere og ***organisationer***. Agenturet bør også bidrage til at fremme bedste praksis og løsninger på enkeltpersons- og ***organisationsniveauet*** ved at indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og ved at sammenstille rapporter med henblik på at yde vejledning til virksomheder og borgere samt forbedre det generelle niveau af beredskab og modstandsdygtighed. Agenturet bør herudover i samarbejde med medlemsstaterne og ***Unionens*** institutioner, organer, kontorer og agenturer tilrettelægge jævnlige informations- og oplysningskampagner for slutbrugere med sigte på at fremme en mere sikker individuel adfærd på nettet og øge bevidstheden om de potentielle farer på Internettet, herunder cyberkriminalitet, såsom phishing-angreb, botnet, økonomisk svig og banksvindel, samt fremme af ***grundlæggende autentificerings-*** og databeskyttelsesrådgivning. Agenturet bør spille en central rolle i bestræbelserne på at højne slutbrugernes oplysningsniveau om udstyrs sikkerhed. | (28) Agenturet bør bidrage til at bevidstgøre offentligheden***, herunder gennem uddannelsesfremme, om cybersikkerhedrisici*** og give vejledning om god praksis for individuelle brugere, der er målrettet mod borgere***,*** ***organisationer*** og ***virksomheder***. Agenturet bør også bidrage til at fremme bedste praksis ***inden for cyberhygiejne, som omfatter en række former for praksis, der bør gennemføres regelmæssigt for at beskytte brugere*** og ***virksomheder på nettet, og til at fremme*** løsninger på enkeltpersons-***, organisations-*** og ***virksomhedsniveauet*** ved at indsamle og analysere offentligt tilgængelige oplysninger om væsentlige hændelser og ved at sammenstille ***og offentliggøre*** rapporter ***og vejledninger*** med henblik på at yde vejledning til virksomheder og borgere samt forbedre det generelle niveau af beredskab og modstandsdygtighed. ***ENISA bør desuden stræbe efter at give forbrugere relevante oplysninger om gældende certificeringsordninger, f.eks. ved at give vejledning og anbefalinger vedrørende online- og offlinemarkedspladser.*** Agenturet bør herudover i ***tråd med handlingsplanen for digital uddannelse og i*** samarbejde med medlemsstaterne og ***EU's*** institutioner, organer, kontorer og agenturer tilrettelægge jævnlige informations- og oplysningskampagner for slutbrugere med |

| | |
|---|---|
| | sigte på at fremme en mere sikker individuel adfærd på nettet og ***digitale færdigheder samt*** øge bevidstheden om de potentielle farer på internettet, herunder cyberkriminalitet, såsom phishing-angreb, botnet, økonomisk svig og banksvindel, samt fremme af ***multifaktorautentificering, patching, kryptering, anonymiserings-*** og databeskyttelsesrådgivning. Agenturet bør spille en central rolle i bestræbelserne på at højne slutbrugernes oplysningsniveau om udstyrs sikkerhed ***og fremme indbygget sikkerhed, indbygget privatlivsbeskyttelse samt hændelser og løsninger på dem på EU-plan. I forbindelse med forfølgelsen af dette mål er det nødvendigt, at agenturet udnytter forhåndenværende bedste praksis og erfaring, navnlig hos akademiske institutioner og IT-sikkerhedsforskere, bedst muligt. Eftersom individuelle fejl og uopmærksomhed udgør en hovedusikkerhedsfaktor på cybersikkerhedsområdet, bør agenturet tildeles tilstrækkelige ressourcer til at udøve denne funktion bedst muligt.*** |

**Ændringsforslag 25**

**Forslag til forordning**
**Betragtning 28 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(28a) Agenturet bør skabe øget opmærksomhed i offentligheden om risikoen for databedrageri og -tyveri, der i alvorlig grad kan påvirke borgernes grundlæggende rettigheder, udgøre en trussel mod retsstatsprincippet og true stabiliteten i demokratiske samfund, herunder demokratiske processer i medlemsstaterne.*** |

**Ændringsforslag 26**

**Forslag til forordning**
**Betragtning 30**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (30) For at sikre, at det når sine mål fuldt ud, bør agenturet etablere kontakt med de relevante institutioner, agenturer og organer, herunder CERT-EU, Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol, Det Europæiske Forsvarsagentur (EDA), Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-Systemer (eu-LISA), Det Europæiske Luftfartssikkerhedsagentur (EASA) og ethvert andet EU-agentur, der er involveret i cybersikkerhed. Det bør også samarbejde med myndigheder med ansvar for databeskyttelse for at udveksle knowhow og bedste praksis og yde rådgivning om cybersikkerhedsaspekter, der kan have betydning for deres arbejde. Repræsentanter for de retshåndhævende myndigheder på nationalt og EU-plan og myndigheder, der har ansvar for databeskyttelse, bør kunne være repræsenteret i ***agenturets stående*** gruppe ***af interessenter***. I sine kontakter med retshåndhævende myndigheder vedrørende aspekter af net- og informationssikkerhed, der kan have indflydelse på disse myndigheders arbejde, bør agenturet respektere de eksisterende informationskanaler og etablerede netværk. | (30) For at sikre, at det når sine mål fuldt ud, bør agenturet etablere kontakt med de relevante institutioner, ***EU's tilsynsmyndigheder og andre kompetente myndigheder,*** agenturer og organer, herunder CERT-EU, Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol, Det Europæiske Forsvarsagentur (EDA), Det Europæiske ***GNSS-Agentur (GSA), Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC), Det Europæiske*** Agentur for den Operationelle Forvaltning af Store IT-Systemer (eu-LISA), ***Den Europæiske Centralbank (ECB), Den Europæiske Banktilsynsmyndighed (EBA), Det Europæiske Databeskyttelsesråd,*** Det Europæiske Luftfartssikkerhedsagentur (EASA) og ethvert andet EU-agentur, der er involveret i cybersikkerhed. Det bør også samarbejde med ***europæiske standardiseringsorganisationer, relevante interessenter og*** 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 ***ENISA-rådgivningsgruppen***. 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. ***Der bør etableres partnerskaber med akademiske institutioner, som tager forskningsinitiativer på relevante områder, mens bidrag fra*** |

| | |
|---|---|
| | ***forbrugerorganisationer og andre organisationer bør sikres passende kanaler og altid bør analyseres.*** |

**Ændringsforslag 27**

**Forslag til forordning**
**Betragtning 31**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (31) Agenturet bør som medlem, der også fungerer som CSIRT-netværkets sekretariat, støtte medlemsstaternes CSIRT'er og CERT-EU i det operationelle samarbejde oven i alle CSIRT-netværkets relevante opgaver som defineret i NIS-direktivet. Agenturet bør endvidere fremme og støtte samarbejdet mellem de relevante CSIRT'er i tilfælde af hændelser, angreb på eller afbrydelser af net eller infrastruktur, der styres eller beskyttes af CSIRT'erne, og som berører eller vil kunne berøre mindst to CERT'er, under behørig hensyntagen til CSIRT-netværkets standardprocedurer. | (31) Agenturet bør som medlem, der også fungerer som CSIRT-netværkets sekretariat, støtte medlemsstaternes CSIRT'er og CERT-EU i det operationelle samarbejde oven i alle CSIRT-netværkets relevante opgaver som defineret i NIS-direktivet. Agenturet bør endvidere fremme og støtte samarbejdet mellem de relevante CSIRT'er i tilfælde af hændelser, angreb på eller afbrydelser af net eller infrastruktur, der styres eller beskyttes af CSIRT'erne, og som berører eller vil kunne berøre mindst to CERT'er, under behørig hensyntagen til CSIRT-netværkets standardprocedurer. ***Agenturet kan på Kommissionens eller en medlemsstats anmodning regelmæssigt gennemføre IT-sikkerhedsrevision af kritiske infrastrukturer på tværs af grænserne med det formål at identificere mulige cybersikkerhedsrisici og foreslå forbedringer til at styrke deres modstandsdygtighed.*** |

**Ændringsforslag 28**

**Forslag til forordning**
**Betragtning 33**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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, | (33) Agenturet bør videreudvikle og opretholde sin ekspertise inden for cybersikkerhedscertificering med sigte på at understøtte EU's politik på dette område. Agenturet bør ***bygge på eksisterende former for god praksis og*** fremme |

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.

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.

**Ændringsforslag 29**

**Forslag til forordning**
**Betragtning 35**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (35) Agenturet bør tilskynde medlemsstaterne og tjenesteudbydere til at hæve deres generelle sikkerhedsstandarder, så alle internetbrugere kan tage de nødvendige skridt til at sikre deres egen personlige cybersikkerhed. Navnlig bør tjenesteudbydere og produktproducenter tilbagekalde eller genbruge produkter og tjenester, som ikke overholder ***cybersikkerhedsstandarderne***. I samarbejde med de kompetente myndigheder kan ENISA formidle oplysninger om cybersikkerhedsniveauet for produkter og tjenester, som udbydes i det indre marked, og udstede advarsler til udbydere og producenter og pålægge dem at forbedre sikkerheden, herunder cybersikkerheden, af deres produkter og ***tjenester***. | (35) Agenturet bør tilskynde medlemsstaterne***, producenter*** og tjenesteudbydere til at hæve deres generelle sikkerhedsstandarder ***for deres IKT-produkter, -processer, -tjenester og -systemer, der bør overholde grundlæggende sikkerhedsforpligtelser i overensstemmelse med princippet om indbygget sikkerhed og sikkerhed gennem standardindstillinger***, så alle internetbrugere kan ***sikres og anspores til at*** 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 ***de grundlæggende cybersikkerhedsforpligtelser, mens importører og distributører bør sikre sig, at de IKT-produkter, -processer, -tjenester og -systemer, de introducerer på EU-markedet, opfylder de gældende krav og ikke udgør en risiko for europæiske forbrugere***. 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***, processer, tjenester*** og ***systemer. Agenturet bør samarbejde med interessenter omkring udviklingen af en EU-dækkende tilgang til ansvarlig offentliggørelse af sårbarheder og bør fremme bedste praksis på dette område.*** |

**Ændringsforslag 30**

**Forslag til forordning**
**Betragtning 36**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (36) Agenturet bør tage fuldt hensyn til igangværende forsknings-, udviklings- og teknologivurderingsaktiviteter, navnlig aktiviteter, der gennemføres som led i de forskellige EU-forskningsinitiativer, for at rådgive Unionen og, hvor det er relevant, medlemsstaterne, hvis de anmoder herom, om forskningsbehov inden for net- og informationssikkerhed, herunder navnlig cybersikkerhed. | (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, organer, kontorer og agenturer samt, hvor det er relevant, medlemsstaterne, hvis de anmoder herom, om forskningsbehov inden for net- og informationssikkerhed, herunder navnlig cybersikkerhed. ***Mere specifikt bør der etableres et samarbejde med Det Europæiske Forskningsråd (EFR) og Det Europæiske Institut for Innovation og Teknologi (EIT), og der bør indgå sikkerhedsforskning i det niende forskningsrammeprogram (RP9) og Horisont 2020.*** |

**Ændringsforslag 31**

**Forslag til forordning**
**Betragtning 36 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(36 a) Standarder er et frivilligt, markedsdrevet redskab, der fastsætter tekniske krav og retningslinjer som et resultat af en åben, gennemsigtig og inklusiv proces. Agenturet bør regelmæssigt høre og opretholde et tæt samarbejde med*** |

| | |
|---|---|
| | ***standardiseringsorganisationerne, navnlig i forbindelse med udarbejdelsen af de europæiske cybersikkerhedscertificeringsordninger.*** |

**Ændringsforslag 32**

**Forslag til forordning**
**Betragtning 37**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (37) Cybersikkerhedsproblemer er af global karakter. Der er behov for et tættere internationalt samarbejde for at forbedre cybersikkerhedsstandarderne, herunder definitionen af fælles adfærdsnormer, og informationsudveksling, hvilket vil fremme hurtigere internationalt samarbejde om samt en fælles global tilgang til net- og informationssikkerhedsspørgsmål. Agenturet bør derfor støtte et fortsat EU-engagement og samarbejde med tredjelande og internationale organisationer, ved, hvor det er relevant, at yde den nødvendige ekspertise og analyse til Unionens relevante institutioner, organer, kontorer og agenturer. | (37) Cybersikkerhedsproblemer er af global karakter. Der er behov for et tættere internationalt samarbejde for at forbedre cybersikkerhedsstandarderne, herunder definitionen af fælles adfærdsnormer ***og adfærdskodekser***, ***anvendelse af internationale standarder*** 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, organer, kontorer og agenturer. |

**Ændringsforslag 33**

**Forslag til forordning**
**Betragtning 40**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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 | (40) For at sikre, at agenturet fungerer effektivt, bør medlemsstaterne og Kommissionen ***samt interessenter, der er relevante for opnåelsen af agenturets mål,*** 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 |

| | |
|---|---|
| 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. | 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. ***I lyset af agenturets stærkt tekniske og videnskabelige opgaver bør medlemmerne af bestyrelsen besidde tilstrækkelig erfaring og et højt ekspertiseniveau for så vidt angår emner, der falder inden for agenturets arbejdsområde.*** |

**Ændringsforslag 34**

**Forslag til forordning**
**Betragtning 41**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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. ***Som følge af den høje markedsværdi af de kvalifikationer, som kræves til agenturets arbejde, er det nødvendigt at sikre, at den løn og de sociale forhold, der tilbydes alle agenturets medarbejdere, er konkurrencedygtige, og sikre, at de bedste fagfolk kan vælge at arbejde der.*** |

*Begrundelse*

*For at have et tilstrækkeligt ekspertiseniveau er det nødvendigt, at ENISA er en*

*konkurrencedygtig arbejdsgiver på et stærkt konkurrencepræget marked.*

**Ændringsforslag 35**

**Forslag til forordning**
**Betragtning 42**

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

**Ændringsforslag 36**

**Forslag til forordning**
**Betragtning 44**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (44) Agenturet bør have en ***ENISA-rådgivningsgruppe*** som et rådgivende organ, der kan sikre en løbende dialog med den private sektor, forbrugerorganisationerne***, den akademiske verden*** og andre relevante interessenter. ***ENISA-rådgivningsgruppen***, 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. ***I betragtning af betydningen af certificeringskravene for at sikre tilliden til tingenes internet vil Kommissionen specifikt overveje at indføre gennemførelsesforanstaltninger, der sikrer harmonisering af sikkerhedsstandarderne for IoT-apparater på tværs af EU.*** |

**Ændringsforslag 37**

**Forslag til forordning**
**Betragtning 44 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(44 a) Agenturet bør have en interessentcertificeringsgruppe som et rådgivende organ, der kan sikre en løbende dialog med den private sektor, forbrugerorganisationer, den akademiske verden og andre relevante interessenter. Interessentcertificeringsgruppen, der nedsættes af den administrerende direktør, bør være sammensat af et*** |

| | |
|---|---|
| | ***generelt rådgivende udvalg, som yder input til, hvilke IKT-produkter og -tjenester der skal indgå i fremtidige europæiske IT-sikkerhedscertificeringsordninger, og et ad hoc-udvalg, der leverer input til forslaget om og udarbejdelsen og vedtagelsen af de foreslåede europæiske cybersikkerhedsordninger.*** |

**Ændringsforslag 38**

**Forslag til forordning**
**Betragtning 46**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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. ***For at sikre, at agenturet har tilstrækkelig kapacitet til at opfylde alle sine voksende opgaver og mål, er det af helt afgørende betydning, at det tildeles tilstrækkelige midler.*** 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 ***samt for at sikre udgifternes lønsomhed***. |

**Ændringsforslag 39**

**Forslag til forordning**
**Betragtning 47**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (47) Overensstemmelsesvurdering er den proces, hvorved det fastslås, om nærmere bestemte krav til et produkt, en proces, en tjeneste, et system, en person eller et organ er opfyldt. I forbindelse med denne forordning bør certificering betragtes som en form for overensstemmelsesvurdering for så vidt angår cybersikkerhedsegenskaberne for et produkt, en proces, en tjeneste, et system eller en kombination af disse ("IKT-produkter og -tjenester"), der foretages af en uafhængig tredjepart, ***som ikke*** er produktproducenten eller tjenesteudbyderen. Certificering kan ikke i sig selv garantere, at certificerede IKT-produkter og -tjenester er cybersikre. Det er snarere en procedure og en teknisk metode til at attestere, at IKT-produkter og -tjenester er blevet prøvet og at de opfylder visse krav til cybersikkerhed, som er fastsat andetsteds, f.eks. i tekniske standarder. | (47) Overensstemmelsesvurdering er den proces, hvorved det fastslås, om nærmere bestemte krav til et produkt, en proces, en tjeneste, et system, en person eller et organ er opfyldt. I forbindelse med denne forordning bør certificering betragtes som en form for overensstemmelsesvurdering for så vidt angår cybersikkerhedsegenskaberne for et produkt, en proces, en tjeneste, et system eller en kombination af disse ("IKT-produkter***, -processer*** og -tjenester"), der foretages af en uafhængig tredjepart ***eller***, ***hvor det*** er ***tilladt, ved selvevaluering af*** produktproducenten eller tjenesteudbyderen. ***Selvevaluering kan som specificeret i denne forordning foretages af produktfabrikanter, SMV'er eller tjenesteydere og, hvis det er relevant, som fastsat af og i overensstemmelse med den nye lovgivningsramme. Selvevaluering kan endvidere foretages af produktproducenten eller operatøren, hvis sandsynligheden for, at der foreligger en risiko for en cybersikkerhedshændelse og/eller en risiko for, at en sådan hændelse vil volde samfundet eller et stort udsnit heraf væsentlig skade, ikke forventes at være høj eller væsentlig under hensyntagen til producentens eller tjenesteudbyderens påtænkte anvendelse af det pågældende produkt eller den pågældende tjeneste.*** Certificering kan ikke i sig selv garantere, at ***omfattede*** IKT-produkter***, -processer*** og -tjenester er cybersikre***, hvilket skal meddeles forbrugere og virksomheder på behørig vis***. Det er snarere en procedure og en teknisk metode til at attestere, at IKT-produkter***, -processer*** og -tjenester er blevet prøvet og at de opfylder visse krav til cybersikkerhed, som er fastsat andetsteds, f.eks. i tekniske standarder. ***Sådanne tekniske standarder inkluderer en angivelse af, hvorvidt et IKT-produkt,*** |

| | |
|---|---|
| | ***en IKT-proces og en IKT-tjeneste er i stand til at udføre dets eller dens almindelige opgaver uden at være tilsluttet internettet.*** |

**Ændringsforslag 40**

**Forslag til forordning**
**Betragtning 48**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (48) ***Europæisk cybersikkerhedscertificering*** spiller en ***afgørende*** rolle for at øge tilliden til og sikkerheden af IKT-produkter***, -processer*** 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 ***højt*** 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. |

**Ændringsforslag 41**

**Forslag til forordning**
**Betragtning 49**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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 | (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. | interoperable. Udbuddet af ***IKT-produkter, -processer*** 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. |

**Ændringsforslag 42**

**Forslag til forordning**
**Betragtning 50**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (50) I øjeblikket anvendes cybersikkerhedscertificering af IKT-produkter og -tjenester kun i begrænset omfang. Hvis den findes, er det som regel på medlemsstatsniveau eller inden for rammerne af en brancheordning. En attest udstedt af en national cybersikkerhedsmyndighed anerkendes i princippet ikke i andre medlemsstater. Virksomhederne kan således være nødt til at certificere deres produkter og tjenester i | (50) I øjeblikket anvendes cybersikkerhedscertificering af IKT-produkter***, -processer*** 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***, processer*** og |

| | |
|---|---|
| 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. | tjenester i flere medlemsstater, hvor de driver virksomhed, f.eks. hvis de vil deltage i nationale offentlige udbud***, hvorved deres omkostninger øges***. Desuden er der, selv om der laves nye ordninger, tilsyneladende ikke nogen sammenhængende og holistisk tilgang til horisontale cybersikkerhedsspørgsmål, f.eks. inden for tingenes Internet. De bestående ordninger har væsentlige mangler og forskelle med hensyn til produktdækning, ***risikobaserede tillidsniveauer***, materielle kriterier og den faktiske udnyttelse. ***Gensidig anerkendelse og tillid blandt medlemsstaterne er et hovedelement i denne sammenhæng. ENISA har en vigtig rolle at spille med hensyn til at bistå medlemsstaterne med at udvikle en solid institutionel struktur og ekspertise til beskyttelse mod potentielle cyberangreb. En fremgangsmåde, hvor man ser på hver enkelt sag, er påkrævet for at sikre, at tjenester, processer og produkter er genstand for passende certificeringsordninger. Desuden er der behov for en risikobaseret tilgang med henblik på effektiv identifikation og afbødning af risici, samtidig med at det må erkendes, at en udifferentieret universalløsning ikke er mulig.*** |

**Ændringsforslag 43**

**Forslag til forordning**
**Betragtning 52**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (52) På denne baggrund er det nødvendigt at etablere en europæisk ramme for cybersikkerhedscertificering, som fastlægger de vigtigste horisontale krav til kommende europæiske cybersikkerhedscertificeringsordninger, og som giver mulighed for anerkendelse og brug af attester for IKT-produkter og -tjenester i alle medlemsstater. Den europæiske ramme har et dobbelt formål: | (52) På denne baggrund er det nødvendigt at ***vedtage en fælles tilgang og*** etablere en europæisk ramme for cybersikkerhedscertificering, som fastlægger de vigtigste horisontale krav til kommende europæiske cybersikkerhedscertificeringsordninger, og som giver mulighed for anerkendelse og brug af attester for IKT-produkter***, -processer*** og -tjenester i alle |

| | |
|---|---|
| På den ene side bør den bidrage til at øge tilliden til IKT-produkter og -tjenester, der er certificeret i henhold til sådanne ordninger. På den anden side bør den hindre udbredelsen af modstridende eller overlappende nationale cybersikkerhedscertificeringer og dermed mindske omkostningerne for virksomheder, der opererer på det digitale indre marked. Ordningerne bør være ikke-diskriminerende og baseret på internationale eller europæiske standarder, medmindre sådanne standarder er ineffektive eller uhensigtsmæssige til at opfylde ***EU's*** legitime mål i denne henseende. | medlemsstater. ***I denne forbindelse er det afgørende at bygge videre på eksisterende nationale og internationale ordninger samt på ordninger for gensidig anerkendelse, navnlig SOG-IS, og at der muliggøres en smidig overgang fra de eksisterende ordninger til ordninger under den nye europæiske ramme.*** Den europæiske ramme har et dobbelt formål: På den ene side bør den bidrage til at øge tilliden til IKT-produkter***, -processer*** 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. ***Når en europæisk cybersikkerhedscertificering har erstattet en national ordning, bør attester udstedt under den europæiske ordning godtages som værende gyldige i de tilfælde, hvor en certificering i henhold til den nationale ordning har været påkrævet.*** Ordningerne bør ***bygge på princippet om indbygget sikkerhed og på principperne i forordning (EU) 2016/679. De bør desuden*** være ikke-diskriminerende og baseret på internationale eller europæiske standarder, medmindre sådanne standarder er ineffektive eller uhensigtsmæssige til at opfylde ***EU's*** legitime mål i denne henseende. |

**Ændringsforslag 44**

**Forslag til forordning**
**Betragtning 52 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(52a) Den europæiske ramme for cybersikkerhedscertificering bør etableres på en ensartet måde i alle medlemsstater med henblik på at undgå "certificeringsshopping" som følge af forskelle mellem medlemsstaterne med*** |

| | |
|---|---|
| | ***hensyn til omkostninger eller krav af forskellig strenghed.*** |

**Ændringsforslag 45**

**Forslag til forordning**
**Betragtning 52 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(52b) Certificeringsordninger bør bygge på, hvad der allerede findes på nationalt og internationalt plan, idet der drages lære af nuværende stærke sider, og svagheder vurderes og korrigeres.*** |

**Ændringsforslag 46**

**Forslag til forordning**
**Betragtning 52 c (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(52c) Industrien har brug for fleksible cybersikkerhedsløsninger for at kunne foregribe ondsindede angreb og trusler, hvorfor det bør sikres, at enhver certificeringsordning ikke forældes for hurtigt.*** |

**Ændringsforslag 47**

**Forslag til forordning**
**Betragtning 53**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (53) Kommissionen bør have beføjelse til at vedtage europæiske cybersikkerhedscertificeringsordninger for specifikke grupper af IKT-produkter og ***-tjenester***. Ordningerne bør gennemføres og overvåges af nationale certificeringstilsynsmyndigheder, og attester udstedt i henhold til disse ordninger bør være gyldige og anerkendes i hele Unionen. Certificeringsordninger, som | (53) Kommissionen bør have beføjelse til at vedtage europæiske cybersikkerhedscertificeringsordninger for specifikke grupper af IKT-produkter***, -processer*** og ***tjenester***. Ordningerne bør gennemføres og overvåges af nationale certificeringstilsynsmyndigheder, og attester udstedt i henhold til disse ordninger bør være gyldige og anerkendes i hele Unionen. Certificeringsordninger, som |

| | |
|---|---|
| er branchedrevne eller drives af andre private organisationer, bør ikke være omfattet af forordningen. Sådanne organer kan dog foreslå Kommissionen at betragte sådanne ordninger som grundlaget for at godkende dem som en europæisk ordning. | 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. ***Agenturet bør identificere og vurdere de ordninger, der allerede anvendes af industrien eller private organisationer, med henblik på at vælge den bedste praksis, som kan indgå i en europæisk ordning. Industriaktører kan foretage en selvevaluering af deres produkter eller tjenester forud for certificering, hvorved de antyder, at deres produkt eller tjeneste er rede til at påbegynde certificeringsprocessen, hvis det er påkrævet eller nødvendigt.*** |

**Ændringsforslag 48**

**Forslag til forordning**
**Betragtning 53 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(53 a) Agenturet og Kommissionen bør udnytte allerede eksisterende certificeringsordninger på europæisk og/eller internationalt plan bedst muligt. ENISA bør være i stand til at vurdere, hvilke af de allerede anvendte ordninger der er egnede til formålet og kan indføres i EU-lovgivningen i samarbejde med EU-standardiseringsorganer og så vidt muligt anerkendes internationalt. Eksisterende god praksis bør indsamles og deles blandt medlemsstaterne.*** |

**Ændringsforslag 49**

**Forslag til forordning**
**Betragtning 54**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (54) Bestemmelserne i denne forordning bør ikke berøre EU-lovgivning om | (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. | specifikke regler for certificering af IKT-produkter***, -processer*** 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. |

**Ændringsforslag 50**

**Forslag til forordning**
**Betragtning 55**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (55) Målet med europæiske cybersikkerhedscertificeringsordninger er at sikre, at de IKT-produkter og ***-tjenester***, der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastsatte krav. Kravene vedrører evnen til, på et givet ***tillidsniveau***, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, processer, tjenester og systemer i denne forordnings betydning. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-produkter og ***-tjenester*** i denne forordning. IKT-produkter og ***-tjenester*** og de | (55) Målet med europæiske cybersikkerhedscertificeringsordninger er at sikre, at de IKT-produkter***, -tjenester*** og ***-processer,*** der er certificeret i overensstemmelse med en sådan ordning, opfylder de fastsatte krav. Kravene vedrører evnen til, på et givet ***risikoniveau***, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, processer, tjenester og systemer i denne forordnings betydning. Det er ikke muligt at fastsætte detaljerede cybersikkerhedskrav for alle IKT-produkter***, -tjenester*** og ***-processer*** i denne |

| | |
|---|---|
| tilhørende cybersikkerhedsbehov er så forskellige, at det er meget vanskeligt at komme med generelle cybersikkerhedskrav, der gælder for alting. Det er således nødvendigt at have en bred og generel opfattelse af cybersikkerhed med henblik på certificering, som suppleres af en række specifikke cybersikkerhedsmål, som skal tages i betragtning ved udformningen af europæiske cybersikkerhedscertificeringsordninger. De metoder, der skal anvendes til at nå disse mål for specifikke IKT-produkter og ***-tjenester*** bør så præciseres yderligere i den enkelte certificeringsordning, der vedtages af Kommissionen, f.eks. i form af henvisninger til standarder eller tekniske specifikationer. | forordning. IKT-produkter***, -tjenester*** og ***-processer*** og de tilhørende cybersikkerhedsbehov er så forskellige, at det er meget vanskeligt at komme med generelle cybersikkerhedskrav, der gælder for alting. Det er således nødvendigt at have en bred og generel opfattelse af cybersikkerhed med henblik på certificering, som suppleres af en række specifikke cybersikkerhedsmål, som skal tages i betragtning ved udformningen af europæiske cybersikkerhedscertificeringsordninger. De metoder, der skal anvendes til at nå disse mål for specifikke IKT-produkter***, -tjenester*** og ***-processer*** bør så præciseres yderligere i den enkelte certificeringsordning, der vedtages af Kommissionen, f.eks. i form af henvisninger til standarder eller tekniske specifikationer. ***Alle aktører i en given forsyningskæde bør tilskyndes til at udvikle og indføre principper for sikkerhedsstandarder, tekniske normer og principper for indbygget sikkerhed på alle stadier af produktets, tjenestens eller processens livscyklus. Alle europæiske cybersikkerhedscertificeringsordninger bør udformes, så de opfylder dette mål.*** |

**Ændringsforslag 51**

**Forslag til forordning**
**Betragtning 56**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (56) Kommissionen bør have beføjelse til at anmode ENISA om at udarbejde forslag til ordninger for specifikke IKT-produkter eller -tjenester. ***Kommissionen bør*** på grundlag af ***den af ENISA foreslåede ordning*** have beføjelse til at vedtage ***den*** europæiske ***cybersikkerhedscertificeringsordning*** ved hjælp af ***gennemførelsesretsakter***. Under hensyntagen til de generelle formål og sikkerhedsmål, der er fastsat i denne | (56) Kommissionen bør have beføjelse til at anmode ENISA om at udarbejde forslag til ordninger for specifikke IKT-produkter***, -processer*** eller -tjenester ***på grundlag af velbegrundede årsager, nemlig eksisterende nationale cybersikkerhedscertificeringsordninger, der fragmenterer det indre marked, et aktuelt eller forventet behov for at støtte EU's lovgivning eller udtalelsen fra medlemsstaternes certificeringsgruppe*** |

| | |
|---|---|
| forordning, bør europæiske cybersikkerhedscertificeringsordninger***, der vedtages af Kommissionen,*** angive et minimumssæt af elementer vedrørende den enkelte ordnings genstand, omfang og funktion. Det bør bl.a. omfatte cybersikkerhedscertificeringens omfang og genstand, herunder de omfattede kategorier af IKT-produkter og -tjenester, nærmere specifikation af cybersikkerhedskravene, f.eks. med henvisning til standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder og det påtænkte tillidsniveau (dvs. grundlæggende, betydeligt eller højt). | ***eller interessentcertificeringsgruppen. Efter at have vurderet de foreslåede certificeringsordninger, som ENISA har foreslået*** på grundlag af ***Kommissionens anmodning, bør Kommissionen derpå*** have beføjelse til at vedtage ***de*** europæiske ***cybersikkerhedscertificeringsordninger*** ved hjælp af ***delegerede retsakter***. Under hensyntagen til de generelle formål og sikkerhedsmål, der er fastsat i denne forordning, bør ***disse*** europæiske cybersikkerhedscertificeringsordninger angive et minimumssæt af elementer vedrørende den enkelte ordnings genstand, omfang og funktion. Det bør bl.a. omfatte cybersikkerhedscertificeringens omfang og genstand, herunder de omfattede kategorier af IKT-produkter og -tjenester, nærmere specifikation af cybersikkerhedskravene, f.eks. med henvisning til standarder eller tekniske specifikationer, de specifikke evalueringskriterier og -metoder og det påtænkte tillidsniveau (dvs. grundlæggende, betydeligt eller højt). |

**Ændringsforslag 52**

**Forslag til forordning**
**Betragtning 56 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(56 a) Agenturet bør være referencepunktet for oplysninger om europæiske cybersikkerhedsordninger. Den bør have et websted med alle relevante oplysninger, herunder oplysninger om certificeringer, der er trukket tilbage eller udløbet, samt oplysninger om, hvilke nationale certificeringer der er omfattet. Agenturet bør sikre, at en passende del af indholdet på dets websted er forståeligt for almindelige forbrugere.*** |

**Ændringsforslag 53**

**Forslag til forordning**
**Betragtning 56 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(56 b) Fastlæggelse af tillidsniveauer for attester er nødvendigt for at give slutbrugeren en indikation af den forventede type cybertrusler, som cybersikkerhedsforanstaltningerne i produktet, processen eller tjenesten har til hensigt at forhindre. Cybertrusler skal defineres under hensyntagen til den forventede risiko og ophavsmandens eller ophavsmændenes muligheder for angrebet i forbindelse med den forventede anvendelse af det pågældende IKT-produkt, -proces eller -tjeneste. Tillidsniveauet "grundlæggende" henviser til evnen til at modstå angreb, der kan undgås med grundlæggende cybersikkerhedsforanstaltninger, og som let kan kontrolleres ved at gennemgå den tekniske dokumentation. Tillidsniveauet "betydeligt" henviser til evnen til med begrænsede ressourcerat modstå kendte typer af angreb, som foretages af en rimeligt avanceret angriber. Tillidsniveauet "højt" henviser til evnen til at modstå ukendte sårbarheder og avancerede angreb fra en angriber, der anvender de nyeste teknikker, men som kræver betydelige ressourcer, såsom finansierede tværfaglige teams.*** |

**Ændringsforslag 54**

**Forslag til forordning**
**Betragtning 56 c (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(56 c)Med henblik på at undgå opsplitning af det indre marked som følge af nationale cybersikkerhedsordninger, sikre støtte til fremtidig lovgivning og øge tilliden og sikkerheden bør beføjelsen til at vedtage retsakter delegeres til*** |

| | |
|---|---|
| | ***Kommissionen i overensstemmelse med artikel 290 i traktaten om Den Europæiske Unions funktionsmåde for så vidt angår fastsættelsen af prioriteterne for den europæiske cybersikkerhedscertificering, vedtagelsen af det rullende program og vedtagelsen af europæiske certificeringsordninger. Det er særlig vigtigt, at Kommissionen gennemfører de relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016. For at sikre lige deltagelse i forberedelsen af delegerede retsakter er det navnlig vigtigt, at Europa-Parlamentet og Rådet modtager alle dokumenter på samme tid som medlemsstaternes eksperter, og at deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.*** |

**Ændringsforslag 55**

**Forslag til forordning**
**Betragtning 56 d (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(56d) Blandt de evalueringsmetoder og vurderingsprocedurer, som vedrører de enkelte europæiske cybersikkerhedscertificeringsordninger, bør etisk hacking, som har til formål at lokalisere svagheder og sårbarheder i enheder og informationssystemer ved at forudsige ondsindede hackeres intentioner og færdigheder, fremmes på EU-plan.*** |

**Ændringsforslag 56**

**Forslag til forordning**

**Betragtning 57**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (57) At få foretaget en europæisk cybersikkerhedscertificering bør fortsat være frivilligt, medmindre andet er fastsat i EU-lovgivningen eller den nationale lovgivning. Med sigte på at nå denne forordnings mål og undgå fragmentering af det indre marked bør nationale cybersikkerhedscertificeringsordninger eller -procedurer for IKT-produkter og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, dog ophøre med at have virkning fra det tidspunkt, der fastsættes af Kommissionen i ***gennemførelsesretsakten***. Medlemsstaterne bør desuden ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der allerede er omfattet af en bestående europæisk cybersikkerhedscertificeringsordning. | (57) At få foretaget en europæisk cybersikkerhedscertificering bør fortsat være frivilligt, medmindre andet er fastsat i EU-lovgivningen eller den nationale lovgivning. Med sigte på at nå denne forordnings mål og undgå fragmentering af det indre marked bør nationale cybersikkerhedscertificeringsordninger eller -procedurer for IKT-produkter***, -processer*** og -tjenester, der er omfattet af en europæisk cybersikkerhedscertificeringsordning, dog ophøre med at have virkning fra det tidspunkt, der fastsættes af Kommissionen i ***den delegerede retsakt***. Medlemsstaterne bør desuden ikke indføre nye nationale cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der allerede er omfattet af en bestående europæisk cybersikkerhedscertificeringsordning. ***Nærværende forordning bør dog ikke berøre nationale ordninger, som medlemsstaterne fortsat suverænt kan forvalte for så vidt angår IKT-produkter, -processer og -tjenester, der anvendes i nationalt øjemed.*** |

**Ændringsforslag 57**

**Forslag til forordning**
**Betragtning 57 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(57 a) Der indføres pligt til at udstede en produkterklæring, der indeholder strukturerede oplysninger om certificeringen af produktet, processen eller tjenesten, med henblik på at forsyne forbrugeren med yderligere oplysninger og gøre det muligt for denne at foretage et velbegrundet valg.*** |

**Ændringsforslag 58**

**Forslag til forordning**
**Betragtning 57 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(57b) Når ENISA og andre relevante organer foreslår nye europæiske cybersikkerhedsordninger, bør de tage behørigt hensyn til forslagets konkurrencedynamik og specielt sikre sig, at certificeringsordninger inden for sektorer, der rummer mange små og mellemstore virksomheder, såsom inden for softwareudvikling, ikke udgør en hindring for markedsadgang for nye virksomheder og for innovation.*** |

**Ændringsforslag 59**

**Forslag til forordning**
**Betragtning 57 c (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(57c) Europæiske cybersikkerhedsordninger vil bidrage til at harmonisere og samle cybersikkerhedspraksisser i Unionen. De må dog ikke ende med at udgøre minimumsniveauet for cybersikkerhed. Udformningen af europæiske cybersikkerhedsordninger bør også tage hensyn til og tillade udvikling af nye innovative løsninger på cybersikkerhedsområdet.*** |

**Ændringsforslag 60**

**Forslag til forordning**
**Betragtning 58**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (58) Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenterne af IKT- | (58) Når en europæisk cybersikkerhedscertificeringsordning er vedtaget, kan producenterne af IKT- |

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

produkter og udbydere af ***IKT-processer eller -tjenester*** indgive en ansøgning om certificering af deres produkter eller tjenester til et overensstemmelsesvurderingsorgan efter eget valg ***overalt i Unionen***.
Overensstemmelsesvurderingsorganer bør akkrediteres af et akkrediteringsorgan, hvis de opfylder visse nærmere fastsatte krav i denne forordning. Akkreditering udstedes for en periode på højst fem år og kan forlænges på samme betingelser, såfremt overensstemmelsesvurderingsorganet opfylder kravene. Akkrediteringsorganer tilbagekalder akkrediteringen af et overensstemmelsesvurderingsorgan, hvis betingelserne for akkrediteringen ikke eller ikke længere er opfyldt, eller hvis foranstaltninger truffet af et overensstemmelsesvurderingsorgan er i modstrid med denne forordning. ***Agenturet bør foretage revisioner for at sikre en tilsvarende grad af kvalitet og omhu hos overensstemmelsesvurderingsorganerne med henblik på at undgå tilsynsarbitrage. Resultaterne bør meddeles agenturet, Kommissionen og Europa-Parlamentet og bør gøres offentligt tilgængelige.***

**Ændringsforslag 61**

**Forslag til forordning**
**Betragtning 58 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(58 a) Den obligatoriske anvendelse af europæisk cybersikkerhedscertificering bør begrænses til tilfælde, hvor risikoanalyser berettiger omkostningerne for industrien, borgerne og forbrugerne. Hændelser, som afbryder vigtige tjenester, kan hindre gennemførelsen af økonomiske aktiviteter, medføre betydelige finansielle tab, underminere brugernes tillid og forårsage stor skade på Unionens økonomi. Den obligatoriske brug af europæisk*** |

| | |
|---|---|
| | ***cybersikkerhedscertificering, som kræves af operatører af væsentlige tjenester, bør begrænses til de elementer, der er afgørende for, at de fungerer, og bør ikke udvides til at omfatte generelle produkter, processer og tjenester, da dette ville medføre en urimelig omkostning for industrien og forbrugerne. Kommissionen bør samarbejde med den samarbejdsgruppe, der er nedsat i medfør af artikel 11 i direktiv (EU) 2016/1148, med henblik på at fastlægge en liste over de kategorier af produkter, processer og tjenester, der specifikt er bestemt til brug for operatører af væsentlige tjenester, og hvis fejlfunktion i tilfælde af en hændelse kan have en betydelig forstyrrende virkning på den væsentlige tjeneste. Denne liste bør udarbejdes gradvist og ajourføres, når det er nødvendigt. Kun de produkter, processer og tjenester, der er opført på listen, bør være obligatoriske for operatører af væsentlige tjenester.*** |

**Ændringsforslag 62**

**Forslag til forordning**
**Betragtning 58 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(58 b) Eksistensen af krydshenvisninger i national lovgivning, som henviser til en national standard, der er ophørt med at have retsvirkning som følge af ikrafttrædelsen af en europæisk certificeringsordning, kan være en potentiel kilde til forvirring hos producenter og slutbrugere. For at undgå, at producenter fortsætter med at gennemføre specifikationer svarende til nationale attester, der ikke længere er gældende, bør medlemsstaterne i overensstemmelse med sine forpligtelser i henhold til traktaterne tilpasse deres nationale lovgivning, således at de afspejler vedtagelsen af en europæisk certificeringsordning.*** |

**Ændringsforslag 63**

**Forslag til forordning**
**Betragtning 59**

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

***overensstemmelse med de krav, der er fastsat i denne forordning, herunder den europæiske cybersikkerhedscertificeringsgruppes regler og kravene i den tilsvarende europæiske cybersikkerhedscertificeringsordning. Et effektivt samarbejde mellem de nationale certificeringstilsynsmyndigheder er afgørende for at opnå en korrekt gennemførelse af europæiske cybersikkerhedscertificeringsordninger og tekniske spørgsmål vedrørende IKT-produkters og -tjenesters cybersikkerhed. Kommissionen bør lette denne udveksling af oplysninger ved at stille et generelt understøttende elektronisk informationssystem til rådighed, f.eks. informations- og kommunikationssystemet for markedsovervågning (ICSMS) og det hurtige varslingssystem for farlige nonfoodprodukter (RAPEX), som allerede anvendes af markedsovervågningsmyndighederne i medfør af forordning (EF) nr. 765/2008.***

**Ændringsforslag 64**

**Forslag til forordning**
**Betragtning 60**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (60) Med henblik på at sikre en ensartet anvendelse af den europæiske ramme for cybersikkerhedscertificering bør der oprettes en ***europæisk cybersikkerhedscertificeringsgruppe ("gruppen")***, som består af medlemsstaternes nationale certificeringstilsynsmyndigheder. ***Gruppens*** vigtigste opgaver bør være at rådgive og bistå Kommissionens i dens arbejde med at sikre en konsekvent gennemførelse og anvendelse af den europæiske ramme for cybersikkerhedscertificering, at bistå og | (60) Med henblik på at sikre en ensartet anvendelse af den europæiske ramme for cybersikkerhedscertificering bør der oprettes en ***certificeringsgruppe for medlemsstaterne***, som består af medlemsstaternes nationale certificeringstilsynsmyndigheder. ***De*** vigtigste opgaver ***for medlemsstaternes certificeringsgruppe*** 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 |

| | |
|---|---|
| arbejde tæt sammen med agenturet ved udarbejdelsen af forslag til cybersikkerhedscertificeringsordninger, at anbefale, at Kommissionen anmoder agenturet om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning og at vedtage udtalelser rettet til Kommissionen vedrørende vedligehold og revision af bestående europæiske cybersikkerhedscertificeringsordninger. | udarbejdelsen af forslag til cybersikkerhedscertificeringsordninger, at anbefale, at Kommissionen anmoder agenturet om at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning og at vedtage udtalelser rettet til Kommissionen vedrørende vedligehold og revision af bestående europæiske cybersikkerhedscertificeringsordninger. |

**Ændringsforslag 65**

**Forslag til forordning**
**Betragtning 60 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(60 a) For at sikre et ensartet kompetenceniveau i overensstemmelsesvurderingsorganerne samt lette og fremme gensidig anerkendelse og den generelle accept af attester og overensstemmelsesvurderinger fra overensstemmelsesvurderingsorganer er det nødvendigt, at de nationale certificeringsorganer har et konsekvent og gennemsigtigt peerevalueringssystem og regelmæssigt lader sig underkaste sådanne evalueringer.*** |

**Ændringsforslag 66**

**Forslag til forordning**
**Betragtning 60 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(60 b) Det er nødvendigt, at de nationale certificeringstilsynsmyndigheder arbejder effektivt sammen, således at peerevalueringerne kan gennemføres korrekt, og der kan opnås akkreditering på tværs af grænserne. Af hensyn til systemets gennemsigtighed er det derfor*** |

| | |
|---|---|
| | ***nødvendigt, at de nationale certificeringstilsynsmyndigheder forpligtes til gensidig udveksling af oplysninger og til at sende relevante oplysninger til de nationale myndigheder og til Kommissionen. Desuden bør ajourførte og nøjagtige oplysninger om, hvilke akkrediteringstjenester de nationale akkrediteringsorganer tilbyder, offentliggøres og dermed gøres tilgængelige, især for overensstemmelsesvurderingsorganer.*** |

**Ændringsforslag 67**

**Forslag til forordning**
**Betragtning 61**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (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. | (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***, -processer*** og -tjenester. |

**Ændringsforslag 68**

**Forslag til forordning**
**Betragtning 63**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (63) Med sigte på at fastsætte de nærmere kriterier for akkrediteringen af overensstemmelsesvurderingsorganer bør Kommissionen tillægges beføjelser til at vedtage retsakter i henhold til artikel 290 i traktaten om Den Europæiske Unions Funktionsmåde. Kommissionen bør under sit forberedende arbejde gennemføre | (63) Med sigte på at fastsætte de nærmere kriterier for akkrediteringen af overensstemmelsesvurderingsorganer bør Kommissionen tillægges beføjelser til at vedtage retsakter i henhold til artikel 290 i traktaten om Den Europæiske Unions Funktionsmåde. Kommissionen bør under sit forberedende arbejde gennemføre |

| | |
|---|---|
| relevante høringer, herunder på ekspertniveau. Disse høringer bør gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016. For at sikre lige deltagelse i forberedelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter. | relevante høringer, herunder på ekspertniveau ***og, hvor det er hensigtsmæssigt, med relevante interessenter***. Disse høringer bør gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016. For at sikre lige deltagelse i forberedelsen af delegerede retsakter bør Europa-Parlamentet og Rådet navnlig modtage alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter bør have systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter. |

**Ændringsforslag 69**

**Forslag til forordning**
**Betragtning 65**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (65) ***Undersøgelsesproceduren bør anvendes til at vedtage gennemførelsesretsakter*** om de europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, om agenturets metoder i forbindelse med gennemførelsen af undersøgelser, samt om vilkår, formater og procedurer for de nationale certificeringstilsynsmyndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer til Kommissionen. | (65) ***Der kan desuden eventuelt vedtages delegerede retsakter*** om de europæiske cybersikkerhedscertificeringsordninger for IKT-produkter***, -processer*** og -tjenester, om agenturets metoder i forbindelse med gennemførelsen af undersøgelser, samt om vilkår, formater og procedurer for de nationale certificeringstilsynsmyndigheders anmeldelse af akkrediterede overensstemmelsesvurderingsorganer til Kommissionen. |

**Ændringsforslag 70**

**Forslag til forordning**
**Betragtning 66**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| (66) Der bør foretages en uafhængig evaluering af agenturets arbejde. | (66) Der bør foretages en ***kontinuerlig og*** uafhængig evaluering af agenturets |

| | |
|---|---|
| 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***. | arbejde. Evalueringen bør tage stilling til, om agenturets mål nås, om arbejdsmetoderne er effektive, og om dets opgaver er relevante***, navnlig dets koordinerende rolle over for medlemsstaterne og deres nationale myndigheder***. ***I tilfælde af en revision*** bør ***Kommissionen*** vurdere ***muligheden for at lade agenturet fungere som en kvikskranke*** for ***medlemsstaterne og for EU's institutioner og organer***. |

**Ændringsforslag 71**

**Forslag til forordning**
**Betragtning 66 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(66 a) Evalueringen bør også vurdere virkningen, effektiviteten og efficiensen af den europæiske ramme for cybersikkerhedscertificering. I forbindelse med en revision vil Kommissionen kunne evaluere agenturets rolle i forbindelse med vurderingen af tredjelandes produkter og tjenester, der indføres på EU-markedet, og muligheden for at sortliste virksomheder, der ikke overholder EU-reglerne.*** |

**Ændringsforslag 72**

**Forslag til forordning**
**Betragtning 66 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***(66 b) Evalueringen bør omfatte en analyse af cybersikkerheden for de produkter og tjenester, der sælges i Unionen. I tilfælde af en revision bør Kommissionen vurdere, hvorvidt væsentlige cybersikkerhedskrav bør indføres som en forudsætning for adgang til det indre marked.*** |

**Ændringsforslag 73**

**Forslag til forordning**
**Artikel 1 – stk. 1 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| a) at fastsætte målene, opgaverne og de organisatoriske aspekter for ENISA, ***"EU's*** Agentur for ***cybersikkerhed"*** (i det følgende benævnt "agenturet") ***og*** | a) at fastsætte målene, opgaverne og de organisatoriske aspekter for ENISA, ***"Den Europæiske Unions*** Agentur for ***Net- og Informationssikkerhed"*** (i det følgende benævnt "agenturet") og |

**Ændringsforslag 74**

**Forslag til forordning**
**Artikel 1 – stk. 1 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) at fastlægge en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at sikre et tilstrækkeligt cybersikkerhedsniveau af IKT-produkter og -tjenester i Unionen***. Denne ramme anvendes uden at det berører*** specifikke bestemmelser vedrørende frivillig ***eller*** obligatorisk certificering i ***andre af Unionens retsakter***. | b) at fastlægge en ramme for etablering af europæiske cybersikkerhedscertificeringsordninger, der har til formål at ***undgå en opsplitning af certificeringsordningerne i Unionen og*** sikre et tilstrækkeligt cybersikkerhedsniveau af IKT-produkter***, -processer*** og -tjenester i Unionen***, som finder anvendelse, jf. dog*** specifikke bestemmelser vedrørende frivillig ***og eventuelt*** obligatorisk certificering***, når det er fastsat*** i ***denne forordning eller i andre EU-retsakter***. |

**Ændringsforslag 75**

**Forslag til forordning**
**Artikel 1 – stk. 1 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Agenturet udfører sine opgaver, uden at det berører medlemsstaternes beføjelser vedrørende cybersikkerhed, navnlig hvad angår medlemsstaternes beføjelser med hensyn til offentlig sikkerhed, forsvar, national sikkerhed og strafferlovgivning.*** |

**Ændringsforslag 76**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1) "cybersikkerhed": alle aktiviteter, der er nødvendige for at beskytte net- og informationssystemer, deres brugere og berørte personer mod cybertrusler | *(Vedrører ikke den danske tekst)* |

**Ændringsforslag 77**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 2**

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

**Ændringsforslag 78**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 3**

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

**Ændringsforslag 79**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 4**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 4) "operatør af væsentlige tjenester": en | 4) "operatør af væsentlige tjenester": en |

| | |
|---|---|
| ***offentlig eller privat enhed*** som defineret i artikel 4, nr. 4), i direktiv (EU) 2016/1148 | ***operatør af væsentlige tjenester*** som defineret i artikel 4, nr. 4), i direktiv (EU) 2016/1148 |

**Ændringsforslag 80**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | 5) "udbyder af digitale tjenester": ***en*** udbyder ***af digitale tjenester*** som defineret i artikel 4, nr. 6), i direktiv (EU) 2016/1148 |

**Ændringsforslag 81**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 6**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 6) "hændelse": ***enhver begivenhed*** som defineret i artikel 4, nr. 7), i direktiv (EU) 2016/1148 | 6) "hændelse": ***en hændelse*** som defineret i artikel 4, nr. 7), i direktiv (EU) 2016/1148 |

**Ændringsforslag 82**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 7**

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

**Ændringsforslag 83**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 8**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 8) "cybertrussel": enhver potentiel omstændighed eller begivenhed, som kan have en negativ indvirkning på net- og informationssystemer, deres brugere og berørte personer | 8) "cybertrussel": enhver potentiel omstændighed eller begivenhed ***eller anden tilsigtet handling, herunder en automatisk kommando***, som kan ***skade, afbryde eller på anden måde*** have en negativ indvirkning på net- og informationssystemer, deres brugere og berørte personer |

**Ændringsforslag 84**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 8 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***8 a) "cyberhygiejne": enkle rutineforanstaltninger, som kan minimere risikoen for cybertrusler, når brugere og virksomheder regelmæssigt anvender og gennemfører sådanne*** |

**Ændringsforslag 85**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 9**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 9) "europæisk cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er fastlagt på EU-plan, og som finder anvendelse på certificeringen af informations- og kommunikationsteknologiske (IKT-) produkter og ***tjenester***, der er omfattet af den pågældende ordning | 9) "europæisk cybersikkerhedscertificeringsordning": et sammenhængende sæt regler, tekniske krav, standarder og procedurer, der er fastlagt på EU-plan, og som ***i overensstemmelse med de internationale og europæiske standarder og IKT-specifikationer, der er identificeret af agenturet,*** finder anvendelse på certificeringen af informations- og kommunikationsteknologiske (IKT-)produkter***, -processer*** og ***-tjenester***, der er omfattet af den pågældende ordning |

**Ændringsforslag 86**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 10**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 10) "europæisk cybersikkerhedsattest": et dokument udstedt af et overensstemmelsesvurderingsorgan, som attesterer at et givet IKT-produkt eller en given ***IKT-tjeneste*** opfylder de specifikke krav i en europæisk cybersikkerhedscertificeringsordning | 10) "europæisk cybersikkerhedsattest": et dokument udstedt af et overensstemmelsesvurderingsorgan, som attesterer at et givet IKT-produkt***, en given IKT-tjeneste*** eller en given ***IKT-proces*** opfylder de specifikke krav i en europæisk cybersikkerhedscertificeringsordning |

**Ændringsforslag 87**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 11 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***11 a) "IKT-proces": et sæt af aktiviteter, der udføres for at udforme, udvikle, opretholde og levere et IKT-produkt eller en IKT-tjeneste*** |

**Ændringsforslag 88**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 11 b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***11 b) "forbrugerelektronik": anordning bestående af hardware og software, der behandler personlige data eller opretter forbindelse til internettet til brug for applikationer i boligen og anordninger til styring af boligen, kontorudstyr, routerudstyr og anordninger, der opretter forbindelse til et netværk, såsom intelligente tv-apparater, legetøj og spillekonsoller, virtuelle eller personlige assistenter, opkoblede streaminganordninger, kropsbåren elektronik, stemmestyrede systemer og*** |

| | |
|---|---|
| | ***systemer til virtuel virkelighed*** |

**Ændringsforslag 89**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 16**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 16) ***"standard"***: en standard som defineret i artikel 2, nr. 1***)***, i forordning (EU) nr. 1025/2012***.*** | 16) ***"standard, teknisk specifikation og IKT-teknisk specifikation"***: en standard***, teknisk specifikation og IKT-teknisk specifikation*** som defineret i artikel 2, nr. 1***, 4 og 5***, i forordning (EU) nr. 1025/2012 |

**Ændringsforslag 90**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 16 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***16 a) "national certificeringstilsynsmyndighed": et organ, der udpeges af hver medlemsstat i overensstemmelse med denne forordnings artikel 50*** |

**Ændringsforslag 91**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 16 b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***16 b) "selvevaluering": den overensstemmelseserklæring, hvormed producenten erklærer, at specifikke krav i en certificeringsordning for så vidt angår produkter, processer og tjenester er opfyldt*** |

**Ændringsforslag 92**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 16 c (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***16 c) "sikkerhed gennem standardindstillinger": en situation, hvor et produkt, en software eller en proces kan etableres på en måde, der sikrer en højere grad af sikkerhed, og den første bruger bør modtage standardkonfigurationen med de mest sikre indstillinger. Hvis en risiko- og brugeranalyse fra sag til sag fører til den konklusion, at en sådan indstilling ikke er mulig, bør brugerne tilskyndes til at vælge den mest sikre indstilling*** |

**Ændringsforslag 93**

**Forslag til forordning**
**Artikel 2 – stk. 1 – nr. 16 d (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***16 d) "operatør af væsentlige tjenester": en operatør af væsentlige tjenester som defineret i artikel 4, nr. 4), i direktiv (EU) 2016/1148*** |

**Ændringsforslag 94**

**Forslag til forordning**
**Artikel 3 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. Agenturet udfører de opgaver, det tillægges ved nærværende forordning, med det formål at bidrage til et højt ***cybersikkerhedsniveau*** i Unionen. | 1. Agenturet udfører de opgaver, det tillægges ved nærværende forordning, ***og skal styrkes*** med det formål at bidrage til ***at opnå*** et højt ***niveau af generel cybersikkerhed med henblik på at forebygge cyberangreb*** i Unionen***, mindske opsplitningen af det indre marked og forbedre dets funktion samt sikre sammenhæng ved at tage hensyn til medlemsstaternes samarbejdsresultater*** |

***under NIS-direktivet***.

**Ændringsforslag 95**

**Forslag til forordning**
**Artikel 4 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 1. Agenturet fungerer som et ***teoretisk og praktisk*** 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. |

**Ændringsforslag 96**

**Forslag til forordning**
**Artikel 4 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2. Agenturet bistår Unionens institutioner, agenturer og organer samt medlemsstaterne med udvikling og gennemførelse af politikker vedrørende cybersikkerhed. | 2. Agenturet bistår EU's institutioner, agenturer og organer samt medlemsstaterne med udvikling og gennemførelse af politikker vedrørende cybersikkerhed ***samt styrkelse af bevidstheden blandt borgere og virksomheder***. |

**Ændringsforslag 97**

**Forslag til forordning**
**Artikel 4 – stk. 3**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 3. Agenturet støtter kapacitetsopbygning og beredskab i ***hele Unionen*** ved at bistå ***Unionen,*** medlemsstaterne og offentlige og private interessenter med at øge beskyttelsen af deres net- og informationssystemer, | 3. Agenturet støtter kapacitetsopbygning og beredskab i ***EU's institutioner, agenturer og organer*** ved at bistå medlemsstaterne og offentlige og private interessenter med ***det formål*** at øge beskyttelsen af deres net- og |

| | |
|---|---|
| udvikle ***færdigheder*** og ***kompetencer inden for*** cybersikkerhed og ***opnå cybermodstandsdygtighed***. | informationssystemer, udvikle ***og forbedre cyberrobusthed*** og ***indsatskapaciteter, øge kendskabet til*** cybersikkerhed og ***udvikle færdigheder og kompetencer inden for cybersikkerhed***. |

**Ændringsforslag 98**

**Forslag til forordning**
**Artikel 4 – stk. 4**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 4. Agenturet fremmer samarbejde og ***koordinering*** på EU-plan mellem medlemsstaterne, Unionens institutioner, agenturer og organer og relevante interessenter, herunder den private sektor, for så vidt angår cybersikkerhedsanliggender. | 4. Agenturet fremmer samarbejde***,*** ***koordinering*** og ***informationsdeling*** på EU-plan mellem medlemsstaterne, EU's institutioner, agenturer og organer og relevante interessenter, herunder den private sektor, for så vidt angår cybersikkerhedsanliggender. |

**Ændringsforslag 99**

**Forslag til forordning**
**Artikel 4 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 5. Agenturet ***øger*** cybersikkerhedskapaciteten på EU-plan for at supplere medlemsstaternes indsats for at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser. | 5. Agenturet ***bidrager til at øge*** cybersikkerhedskapaciteten på EU-plan for at supplere medlemsstaternes indsats for at forebygge og reagere på cybertrusler, herunder navnlig i tilfælde af grænseoverskridende hændelser***, og med henblik på udførelsen af dets opgave med at bistå EU's institutioner med at udforme politikker vedrørende cybersikkerhed***. |

**Ændringsforslag 100**

**Forslag til forordning**
**Artikel 4 – stk. 6**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 6. Agenturet fremmer brugen af | 6. Agenturet fremmer brugen af |

| | |
|---|---|
| certificering, herunder ved at bidrage til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau, jf. afsnit III, for at øge gennemsigtigheden af IKT-produkters og ***-tjenesters*** cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked. | certificering ***med henblik på at undgå opsplitning af det indre marked og forbedre dets funktionsevne***, herunder ved at bidrage til etablering og vedligeholdelse af en ramme for cybersikkerhedscertificering på EU-niveau, jf. afsnit III, for at øge gennemsigtigheden af IKT-produkters***, -tjenesters*** og ***-processers*** cybersikkerhedstillidsniveau og dermed styrke tilliden til det digitale indre marked ***samt øge kompatibiliteten mellem de eksisterende nationale og internationale certificeringsordninger***. |

**Ændringsforslag 101**

**Forslag til forordning**
**Artikel 4 – stk. 7**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 7. Agenturet fremmer et højt niveau for oplysning ***af*** borgere og virksomheder vedrørende cybersikkerhed. | 7. Agenturet fremmer ***og støtter projekter, der bidrager til*** et højt niveau for oplysning***, cyberhygiejne og cyberfærdigheder blandt*** borgere og virksomheder vedrørende cybersikkerhed. |

**Ændringsforslag 102**

**Forslag til forordning**
**Artikel 5 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | 1. bistå og rådgive, navnlig ved at levere uafhængige udtalelser og ***analyse af relevante aktiviteter i cyberspace og*** forberedende arbejde, ved udvikling og revision af Unionens politik og lovgivning på cybersikkerhedsområdet samt sektorspecifik politik og lovgivningsinitiativer, som involverer cybersikkerhedsanliggender |

**Ændringsforslag 103**

**Forslag til forordning**
**Artikel 5 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | 2. bistå medlemsstaterne med en konsekvent gennemførelse af Unionens politikker og lovgivning om cybersikkerhed, navnlig i forbindelse med direktiv (EU) 2016/1148, ***direktiv ... om en europæisk kodeks for elektronisk kommunikation, forordning (EU) 2016/679 og direktiv 2002/58/EF,*** herunder ved hjælp af udtalelser, retningslinjer, råd og bedste praksis om emner som ***udvikling af sikker software og sikre systemer,*** risikostyring, indberetning af hændelser og informationsudveksling, ***tekniske og organisatoriske foranstaltninger, navnlig udvikling af koordinerede programmer for offentliggørelse af sårbarheder,*** samt lette udvekslingen af bedste praksis mellem de kompetente myndigheder i denne henseende |

**Ændringsforslag 104**

**Forslag til forordning**
**Artikel 5 – stk. 2 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***2 a. udvikle og fremme politikker, der skal understøtte den generelle tilgængelighed eller integritet af den offentligt tilgængelige kerne af det åbne internet, som giver internettet dets kernefunktioner som en helhed, og som er medvirkende til den normale drift, herunder, men ikke begrænset til, sikkerheden og stabiliteten af centrale protokoller (især DNS, BGP, og IPv6), driften af domænenavnssystemet (herunder med alle topniveaudomæner), og driften af rodzonen*** |

**Ændringsforslag 105**

**Forslag til forordning**
**Artikel 5 – stk. 4 – nr. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | 2) fremme af et højere sikkerhedsniveau i elektronisk kommunikation, ***dataopbevaring og databehandling,*** herunder gennem rådgivning og bistand samt ved at fremme udvekslingen af bedste praksis mellem de kompetente myndigheder |

**Ændringsforslag 106**

**Forslag til forordning**
**Artikel 5 – stk. 5 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***5 a. bistå medlemsstaterne med at gennemføre Unionens politikker og lovgivning om databeskyttelse på en konsekvent måde, navnlig forordning (EU) 2016/679, og bistå Det Europæiske Databeskyttelsesråd (EDPB) i forbindelse med udarbejdelsen af retningslinjer vedrørende gennemførelsen af forordning (EU) 2016/679 til cybersikkerhedsformål. EDPB hører agenturet, hver gang det udsender en udtalelse vedrørende gennemførelsen af GDPR og cybersikkerhed, navnlig vedrørende, men ikke begrænset til, konsekvensanalyser vedrørende beskyttelsen af privatlivets fred, anmeldelse af brud på datasikkerheden, sikkerhedsprocedurer, sikkerhedskrav og indbygget sikkerhed*** |

**Ændringsforslag 107**

**Forslag til forordning**
**Artikel 6 – stk. 1 – litra a a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***a a) medlemsstaterne og EU's institutioner med at udarbejde og gennemføre politikker for koordineret offentliggørelse af sårbarheder samt revisionsprocedurer for offentliggørelse af sårbarheder i den offentlige sektor, idet det sikres, at sådanne procedurer og konstateringer er gennemsigtige og underkastes uafhængigt tilsyn*** |

**Ændringsforslag 108**

**Forslag til forordning**
**Artikel 6 – stk. 1 – litra a b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***a b) Agenturet letter oprettelsen og lanceringen af et langsigtet europæisk IT-sikkerhedsprojekt for yderligere at fremme cybersikkerhedsforskning i EU og medlemsstaterne i samarbejde med Det Europæiske Forskningsråd (EFR) og Det Europæiske Institut for Innovation og Teknologi (EIT) og med henblik på Unionens forskningsprogrammer.*** |

**Ændringsforslag 109**

**Forslag til forordning**
**Artikel 6 – stk. 1 – litra g**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| g) medlemsstaterne ved at tilrettelægge årlige cybersikkerhedsøvelser i stor skala på EU-plan som omhandlet i artikel 7, stk. 6, og ved at fremsætte politikanbefalinger baseret på vurderingen af øvelserne og de indhøstede erfaringer fra dem | g) medlemsstaterne ved at tilrettelægge ***regelmæssige og som minimum*** årlige cybersikkerhedsøvelser i stor skala på EU-plan som omhandlet i artikel 7, stk. 6, og ved at fremsætte politikanbefalinger ***og udveksle bedste praksis*** baseret på vurderingen af øvelserne og de indhøstede erfaringer fra dem |

**Ændringsforslag 110**

**Forslag til forordning**
**Artikel 6 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2. Agenturet fremmer etableringen af centre for informationsudveksling og analyse (ISAC'er), herunder navnlig i de sektorer, der er nævnt i bilag II i direktiv (EU) 2016/1148, ved at stille bedste praksis og vejledning om tilgængelige værktøjer og ***procedurer*** til rådighed samt ved at vejlede om håndtering af lovgivningsmæssige spørgsmål relateret til informationsudveksling. | 2. Agenturet fremmer etableringen af centre for informationsudveksling og analyse (ISAC'er), herunder navnlig i de sektorer, der er nævnt i bilag II i direktiv (EU) 2016/1148, ved at stille bedste praksis og vejledning om tilgængelige værktøjer***, procedurer*** og ***principper for cyberhygiejne*** til rådighed samt ved at vejlede om håndtering af lovgivningsmæssige spørgsmål relateret til informationsudveksling. |

**Ændringsforslag 111**

**Forslag til forordning**
**Artikel 7 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. Agenturet understøtter det operationelle samarbejde mellem ***de kompetente offentlige*** organer og mellem interessenter. | 1. Agenturet understøtter det operationelle samarbejde mellem ***medlemsstaterne, EU's institutioner, agenturer og*** organer og mellem interessenter ***med henblik på at sikre samarbejde ved at analysere og vurdere de eksisterende nationale ordninger, ved at udvikle og gennemføre en plan og ved hjælp af passende instrumenter med henblik på at opnå det højeste niveau af cybersikkerhedscertificering i EU og medlemsstaterne***. |

**Ændringsforslag 112**

**Forslag til forordning**
**Artikel 7 – stk. 4 – afsnit 1 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) levere – på deres anmodning – | b) levere – på deres anmodning – |

| | |
|---|---|
| teknisk bistand i tilfælde af hændelser, der har en betydelig eller væsentlig virkning | teknisk bistand i ***form af informationsudveksling og ekspertise i*** tilfælde af hændelser, der har en betydelig eller væsentlig virkning |

**Ændringsforslag 113**

**Forslag til forordning**
**Artikel 7 – stk. 4 – afsnit 1 – litra b a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***b a) hvis en situation kræver omgående handling, eller en hændelse medfører en væsentlig afbrydelse, kan en medlemsstat anmode om bistand fra eksperter fra agenturet for at vurdere situationen. Anmodningen skal indeholde en beskrivelse af situationen, de mulige mål og de påtænkte behov.*** |

**Ændringsforslag 114**

**Forslag til forordning**
**Artikel 7 – stk. 5 – afsnit 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| På anmodning af ***to*** eller flere berørte medlemsstater og alene med det formål at levere rådgivning om forebyggelse af fremtidige hændelser skal agenturet yde støtte til eller foretage en efterfølgende teknisk undersøgelse efter underretning fra de berørte virksomheder om hændelser, der har en betydelig eller væsentlig virkning, i henhold til direktiv (EU) 2016/1148. Agenturet skal også foretage en sådan undersøgelse efter en behørigt begrundet anmodning fra Kommissionen og efter aftale med de berørte medlemsstater i tilfælde, hvor flere end ***to medlemsstater*** berøres af sådanne hændelser. | På anmodning af ***en*** eller flere berørte medlemsstater og alene med det formål at levere ***bistand enten i form af*** rådgivning om forebyggelse af fremtidige ***hændelser eller i form af bistand ved håndtering af aktuelle større*** hændelser skal agenturet yde støtte til eller foretage en efterfølgende teknisk undersøgelse efter underretning fra de berørte virksomheder om hændelser, der har en betydelig eller væsentlig virkning, i henhold til direktiv (EU) 2016/1148. Agenturet ***udfører ovennævnte aktiviteter ved at modtage relevante oplysninger fra de berørte medlemsstater og ved at benytte sine egne ressourcer til trusselsanalyser samt ressourcer om håndtering af hændelser. Agenturet*** skal også foretage en sådan undersøgelse efter en behørigt begrundet anmodning fra Kommissionen |

og efter aftale med de berørte medlemsstater i tilfælde, hvor mere end ***én medlemsstat*** berøres af sådanne hændelser. ***I den forbindelse skal ENISA sørge for ikke at offentliggøre de foranstaltninger, som medlemsstaterne træffer for at beskytte deres centrale statslige funktioner, navnlig dem vedrørende den nationale sikkerhed.***

**Ændringsforslag 115**

**Forslag til forordning**
**Artikel 7 – stk. 6**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 6. Agenturet tilrettelægger ***årlige*** cybersikkerhedsøvelser på EU-niveau og på deres anmodning ***støtte*** medlemsstaterne og EU's institutioner, agenturer og organer i at tilrettelægge øvelser. Årlige øvelser på EU-plan skal omfatte tekniske, operationelle og strategiske elementer og bidrage til at forberede den ***samordnede*** indsats på EU-plan mod væsentlige grænseoverskridende cybersikkerhedshændelser. Agenturet bidrager også til og hjælper med at tilrettelægge, hvor det er relevant, sektorspecifikke cybersikkerhedsøvelser sammen med relevante ISAC'er og give ISAC'er mulighed for også at deltage i cybersikkerhedsøvelser på EU-plan. | 6. Agenturet tilrettelægger ***regelmæssige og under alle omstændigheder mindst én gang om året*** cybersikkerhedsøvelser på EU-niveau og ***støtter*** på deres anmodning medlemsstaterne og EU's institutioner, agenturer og organer i at tilrettelægge øvelser. Årlige øvelser på EU-plan skal omfatte tekniske, operationelle og strategiske elementer og bidrage til at forberede den ***koordinerede*** indsats på EU-plan mod væsentlige grænseoverskridende cybersikkerhedshændelser. Agenturet bidrager også til og hjælper med at tilrettelægge, hvor det er relevant, sektorspecifikke cybersikkerhedsøvelser sammen med relevante ISAC'er og give ISAC'er mulighed for også at deltage i cybersikkerhedsøvelser på EU-plan. |

**Ændringsforslag 116**

**Forslag til forordning**
**Artikel 7 – stk. 7**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 7. Agenturet udarbejder regelmæssigt en teknisk EU-cybersikkerhedsrapport om hændelser og trusler, der skal være baseret | 7. Agenturet udarbejder regelmæssigt en ***tilbundsgående*** teknisk EU-cybersikkerhedsrapport om hændelser og |

| | |
|---|---|
| på offentligt tilgængelige oplysninger, agenturets egen analyse og rapporter, som deles af bl.a. medlemsstaternes CSIRT'er (på frivillig basis) eller NIS-direktivets centrale kontaktpunkter (jf. artikel 14, stk. 5, i NIS-direktivet), Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol og CERT-EU. | trusler, der skal være baseret på offentligt tilgængelige oplysninger, agenturets egen analyse og rapporter, som deles af bl.a. medlemsstaternes CSIRT'er (på frivillig basis) eller NIS-direktivets centrale kontaktpunkter (jf. artikel 14, stk. 5, i NIS-direktivet), Det Europæiske Center til Bekæmpelse af Cyberkriminalitet (EC3) hos Europol og CERT-EU. ***Den administrerende direktør forelægger Europa-Parlamentet de offentlige resultater.*** |

**Ændringsforslag 117**

**Forslag til forordning**
**Artikel 7 – stk. 7 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***7 a. Agenturet bidrager til cybersamarbejdet med NATO's cyberforsvarscenter og NATO's akademi for kommunikation og information (NCI), når det er hensigtsmæssigt og efter forudgående godkendelse fra Kommissionen.*** |

**Ændringsforslag 118**

**Forslag til forordning**
**Artikel 7 – stk. 8 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| a) ***sammenstille*** rapporter fra nationale kilder med henblik på at bidrage til at skabe en fælles situationsforståelse | a) ***udarbejde analyser og sammenstille*** rapporter fra nationale kilder med henblik på at bidrage til at skabe en fælles situationsforståelse |

**Ændringsforslag 119**

**Forslag til forordning**
**Artikel 7 – stk. 8 – litra c**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| c) understøtte den tekniske håndtering af en hændelse eller en krise, herunder ved at fremme ***delingen*** af tekniske løsninger mellem medlemsstaterne | c) understøtte den tekniske håndtering af en hændelse eller en krise, ***baseret på egen uafhængig ekspertise og egne ressourcer,*** herunder ved at fremme ***den frivillige deling*** af tekniske løsninger mellem medlemsstaterne |

**Ændringsforslag 120**

**Forslag til forordning**
**Artikel 7 – stk. 8 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***8 a. Agenturet sørger for, at der arrangeres drøftelser, når der er behov for det, og bistår medlemsstaternes myndigheder med at koordinere deres indsats i overensstemmelse med nærhedsprincippet og proportionalitetsprincippet.*** |

**Ændringsforslag 121**

**Forslag til forordning**
**Artikel 7 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 7a*** |
| | ***Agenturets tekniske kapacitet*** |
| | ***1. Med henblik på at opfylde målene i artikel 7 og i overensstemmelse med agenturets arbejdsprogram skal agenturet bl.a. udvikle følgende tekniske kapacitet og færdigheder:*** |
| | ***a) evnen til at indsamle oplysninger om cybersikkerhedstrusler fra åbne kilder, og*** |
| | ***b) evnen til at fjernanvende teknisk udstyr, redskaber og ekspertise.*** |
| | ***2. Med henblik på at opfylde den tekniske kapacitet, der er omhandlet i denne*** |

| | |
|---|---|
| | ***artikels stk. 1, og for at udvikle de relevante færdigheder, skal agenturet:*** |
| | ***a) sikre, at dets ansættelsesprocedurer afspejler de mange forskellige tekniske færdigheder, der kræves, og*** |
| | ***b) samarbejde med CERT-EU og Europol i overensstemmelse med artikel 7, stk. 2, i denne forordning.*** |

**Ændringsforslag 122**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – indledning**

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

**Ændringsforslag 123**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – led -1 (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***-1) løbende fastlægge standarder, tekniske specifikationer og tekniske IKT-specifikationer*** |

**Ændringsforslag 124**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – nr. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1) ***forberede*** forslag til europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og ***-tjenester*** i henhold til denne forordnings artikel 44 | 1) ***i samarbejde med erhvervets aktører og standardiseringsorganisationer gennem en formaliseret, standardiseret og gennemsigtig proces at identificere og*** |

| | |
|---|---|
| | ***forberede*** forslag til europæiske cybersikkerhedscertificeringsordninger for IKT-produkter***, -tjenester*** og ***-processer*** i henhold til denne forordnings artikel 44 |

**Ændringsforslag 125**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – nr. 1 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***1 a) i samarbejde med den europæiske cybersikkerhedsgruppe, jf. artikel 53 i denne forordning, udføre vurderinger af procedurerne for udstedelse af europæiske cybersikkerhedsattester, der er indført af de i artikel 51 i denne forordning omhandlede overensstemmelsesvurderingsorganer, med henblik på at sikre, at overensstemmelsesvurderingsorganerne anvender denne forordning på en ensartet måde, når de udsteder attester*** |

**Ændringsforslag 126**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – nr. 1 b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***1 b) udføre efterfølgende uafhængige periodiske kontroller med hensyn til, hvorvidt certificerede IKT-produkter og tjenester er i overensstemmelse med europæiske cybersikkerhedscertificeringsordninger*** |

**Ændringsforslag 127**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – nr. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2) bistå Kommissionen med at varetage sekretariatsfunktionen for ***den europæiske cybersikkerhedscertificeringsgruppe*** i henhold til denne forordnings artikel 53 | 2) bistå Kommissionen med at varetage sekretariatsfunktionen for ***medlemsstaternes certificeringsgruppe*** i henhold til denne forordnings artikel 53 |

**Ændringsforslag 128**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra a – nr. 3**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 3) samle og offentliggøre retningslinjer og udvikle god praksis vedrørende cybersikkerhedskrav til IKT-produkter og -tjenester i samarbejde med nationale certificeringstilsynsmyndigheder og branchen | 3) samle og offentliggøre retningslinjer og udvikle god praksis***, herunder om principper for cyberhygiejne,*** vedrørende cybersikkerhedskrav til IKT-produkter***, -processer*** og -tjenester i samarbejde med nationale certificeringstilsynsmyndigheder og branchen ***i en formaliseret, standardiseret og gennemsigtig proces*** |

**Ændringsforslag 129**

**Forslag til forordning**
**Artikel 8 – stk. 1 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) fremme indførelse og udbredelse af europæiske og internationale standarder for risikostyring og sikkerhed af IKT-produkter og -tjenester og i samarbejde med medlemsstaterne udarbejde vejledning og retningslinjer om de tekniske områder vedrørende sikkerhedskrav for operatører af væsentlige tjenester og udbydere af digitale tjenester samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, i henhold til artikel 19, stk. 2, i direktiv (EU) 2016/1148 | b) fremme indførelse og udbredelse af europæiske og internationale standarder for risikostyring og sikkerhed af IKT-produkter***, -processer*** og -tjenester og i samarbejde med medlemsstaterne ***og industrien*** 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 ***og dele disse oplysninger blandt medlemsstaterne*** |

**Ændringsforslag 130**

**Forslag til forordning**
**Artikel 9 – stk. 1 – litra c**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| c) i samarbejde med eksperter fra medlemsstaterne levere rådgivning, vejledning og bedste praksis for sikkerheden af net- og informationssystemer, navnlig for sikkerheden af internetinfrastruktur og de infrastrukturer, der understøtter sektorerne nævnt i bilag II til direktiv (EU) 2016/1148 | c) i samarbejde med eksperter fra medlemsstaterne ***og relevante interessenter fra industrien*** levere rådgivning, vejledning og bedste praksis for sikkerheden af net- og informationssystemer, navnlig for sikkerheden af internetinfrastruktur og de infrastrukturer, der understøtter sektorerne nævnt i bilag II til direktiv (EU) 2016/1148 |

**Ændringsforslag 131**

**Forslag til forordning**
**Artikel 9 – stk. 1 – litra e**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| e) ***højne*** offentlighedens oplysningsniveau om risiciene i forbindelse med cybersikkerhed og give vejledning om god praksis for ***individuelle*** brugere, der er målrettet mod borgere og organisationer | e) ***løbende højne*** offentlighedens oplysningsniveau om risiciene i forbindelse med cybersikkerhed og give vejledning ***og gennemføre kurser*** om god praksis for brugere, der er målrettet mod borgere og organisationer***, og fremme indførelsen af stærke, forebyggende IT-sikkerhedsforanstaltninger og pålidelig beskyttelse af data og personoplysninger*** |

**Ændringsforslag 132**

**Forslag til forordning**
**Artikel 9 – stk. 1 – litra g**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| g) i samarbejde med medlemsstaterne og Unionens institutioner, organer, kontorer og agenturer tilrettelægge jævnlige ***informations- og oplysningskampagner*** for at ***øge cybersikkerheden og dens synlighed i*** | g) i samarbejde med medlemsstaterne og EU's institutioner, organer, kontorer og agenturer tilrettelægge jævnlige ***kommunikationskampagner*** for at ***fremme en bred offentlig debat*** |

***Unionen***.

**Ændringsforslag 133**

**Forslag til forordning**
**Artikel 9 – stk. 1 – litra g a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***g a) støtte tættere koordinering og udveksling af bedste praksis mellem medlemsstaterne om uddannelse i cybersikkerhed, cyberfærdigheder, cyberhygiejne og bevidstgørelse herom*** |

**Ændringsforslag 134**

**Forslag til forordning**
**Artikel 10 – stk. 1 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | a) ***sikre forudgående høring af relevante brugergrupper og rådgive*** Unionen og medlemsstaterne om forskningsbehov på ***cybersikkerheds-, databeskyttelses- og privatlivsbeskyttelsesområdet*** 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 |

**Ændringsforslag 135**

**Forslag til forordning**
**Artikel 10 – stk. 1 – litra b a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***b a) forestå egne forskningsaktiviteter på områder, der endnu ikke er omfattet af eksisterende EU-forskningsprogrammer, hvor der er en klar europæisk merværdi*** |

**Ændringsforslag 136**

**Forslag til forordning**
**Artikel 11 – stk. 1 – litra c a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***c a) i samarbejde med medlemsstaternes certificeringsgruppe, der er nedsat i henhold til artikel 53, rådgive og støtte Kommissionen om forhold vedrørende aftaler om gensidig anerkendelse af cybersikkerhedsattester med tredjelande*** |

**Ændringsforslag 137**

**Forslag til forordning**
**Artikel 12 – stk. 1 – litra d**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| d) en ***stående gruppe af interessenter***, der varetager de funktioner, der er fastsat i artikel 20***.*** | d) en ***ENISA-rådgivningsgruppe***, der varetager de funktioner, der er fastsat i artikel 20 |

**Ændringsforslag 138**

**Forslag til forordning**
**Artikel 14 – stk. 1 – litra e**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 a***genturet*** har opfyldt sine resultatindikatorer. Årsberetningen offentliggøres | 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***, beskrive omkostningseffektiviteten*** og ***vurdere***, ***hvor virkningsfuldt agenturet har været, og*** i hvilket omfang ***det*** har opfyldt sine resultatindikatorer. Årsberetningen offentliggøres |

**Ændringsforslag 139**

**Forslag til forordning**
**Artikel 14 – stk. 1 – litra m**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| m) udnævne den administrerende direktør og, hvis relevant, forlænge den administrerende direktørs ansættelsesperiode eller afskedige vedkommende i overensstemmelse med denne forordnings artikel 33 | m) udnævne den administrerende direktør ***gennem udvælgelse baseret på faglige kriterier*** og, hvis relevant, forlænge den administrerende direktørs ansættelsesperiode eller afskedige vedkommende i overensstemmelse med denne forordnings artikel 33 |

**Ændringsforslag 140**

**Forslag til forordning**
**Artikel 14 – stk. 1 – litra o**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | o) træffe alle afgørelser vedrørende etablering af agenturets organisatoriske struktur og om nødvendigt ændring heraf under hensyntagen til agenturets aktivitetsbehov ***som anført i denne forordning*** og under hensyntagen til forsvarlig budgetforvaltning |

**Ændringsforslag 141**

**Forslag til forordning**
**Artikel 16 – stk. 4**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 4. Medlemmerne af ***den stående gruppe af interessenter*** kan efter invitation fra formanden deltage i bestyrelsens møder uden stemmeret. | 4. Medlemmerne af ***ENISA-rådgivningsgruppen*** kan efter invitation fra formanden deltage i bestyrelsens møder uden stemmeret. |

**Ændringsforslag 142**

**Forslag til forordning**

**Artikel 18 – stk. 3**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 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. ***Ved udpegelserne tilstræbes det at opnå en ligelig kønsmæssig repræsentation i forretningsudvalget.*** |

*Begrundelse*

*Udpegelserne til forretningsudvalget skal også sigte mod ligelig repræsentation af kønnene i lighed med bestemmelserne for bestyrelsen i artikel 13, stk. 3.*

**Ændringsforslag 143**

**Forslag til forordning**
**Artikel 19 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 2. Den administrerende direktør aflægger ***årligt*** 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. |

**Ændringsforslag 144**

**Forslag til forordning**
**Artikel 19 – stk. 5 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***5a. Den administrerende direktør har også ret til at fungere som særlig institutionel rådgiver om politikken for cybersikkerhed for Europa-Kommissionens formand med et mandat fastlagt i Kommissionens beslutning*** |

**Ændringsforslag 145**

**Forslag til forordning**
**Artikel 20 – overskrift**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| ***Den stående gruppe af interessenter*** | ***ENISA-rådgivningsgruppe*** |
| | *(Dette ændringsforslag gælder for hele teksten. Hvis det vedtages, skal ændringerne foretages alle relevante steder).* |

**Ændringsforslag 146**

**Forslag til forordning**
**Artikel 20 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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, 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. | 1. På forslag af den administrerende direktør nedsætter bestyrelsen ***på*** en ***gennemsigtig måde en ENISA-rådgivningsgruppe*** bestående af anerkendte ***sikkerhedseksperter***, der repræsenterer de relevante interessenter***,*** såsom IKT-industrien, ***herunder SMV'er, operatører af væsentlige tjenester i henhold til NIS-direktivet,*** udbydere af elektroniske kommunikationsnet og -tjenester til offentligheden, forbrugergrupper, akademiske eksperter i cybersikkerhed***, europæiske standardiseringsorganisationer, EU-agenturer*** 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. ***Bestyrelsen sikrer en passende balance mellem de forskellige interessentgrupper.*** |

**Ændringsforslag 147**

**Forslag til forordning**
**Artikel 20 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 2. Procedurerne for ***ENISA-rådgivningsgruppen***, 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. |

**Ændringsforslag 148**

**Forslag til forordning**
**Artikel 20 – stk. 3**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 3. ***Den stående gruppe af interessenter*** ledes af den administrerende direktør eller af en person udpeget af den administrerende direktør fra sag til sag. | 3. ***ENISA-rådgivningsgruppen*** ledes af den administrerende direktør eller af en person udpeget af den administrerende direktør fra sag til sag. |

**Ændringsforslag 149**

**Forslag til forordning**
**Artikel 20 – stk. 4**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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*** | 4. Embedsperioden for medlemmerne af ***ENISA-rådgivningsgruppen*** er to et halvt år. Medlemmer af bestyrelsen kan ikke være medlemmer af ***ENISA-rådgivningsgruppen***. Eksperter fra Kommissionen og medlemsstaterne har ret til at være til stede på møderne og deltage i arbejdet i ***ENISA-rådgivningsgruppen***. Repræsentanter for andre organer, som den administrerende direktør skønner er relevante, og som ikke er medlemmer af ***ENISA-rådgivningsgruppen***, kan indbydes |

| | |
|---|---|
| ***interessenter***, kan indbydes til at være til stede ***på møderne*** og deltage i ***arbejdet i den stående gruppe af interessenter***. | til at være til stede ***på ENISA-rådgivningsgruppens møder*** og deltage i ***dens arbejde***. |

**Ændringsforslag 150**

**Forslag til forordning**
**Artikel 20 – stk. 4 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***4 a. ENISA-rådgivningsgruppen vil regelmæssigt orientere om sin planlægning i løbet af året og opstille målene for sit arbejdsprogram, der skal offentliggøres hver sjette måned for at sikre gennemsigtighed.*** |

**Ændringsforslag 151**

**Forslag til forordning**
**Artikel 20 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 5. ***ENISA-rådgivningsgruppen*** rådgiver agenturet med hensyn til udførelsen af dets aktiviteter***, bortset fra anvendelsen af afsnit III i denne forordning***. Den rådgiver navnlig den administrerende direktør om udarbejdelsen af forslag til agenturets arbejdsprogram samt om varetagelse af kommunikation med de relevante interessenter om spørgsmål, der vedrører arbejdsprogrammet. |

**Ændringsforslag 152**

**Forslag til forordning**
**Artikel 20 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 20a*** |

***Interessentcertificeringsgruppe***

***1. Den administrerende direktør opretter en interessentcertificeringsgruppe bestående af et generelt rådgivende udvalg, der yder generel rådgivning om anvendelsen af afsnit III i denne forordning, og nedsætter ad hoc-udvalg om forslaget, udarbejdelsen og vedtagelsen af hver enkel foreslåede ordning. Medlemmerne af denne gruppe udvælges blandt af anerkendte sikkerhedseksperter, der repræsenterer relevante interessenter, såsom IKT-industrien, herunder SMV'er, operatører af væsentlige tjenester i henhold til NIS-direktivet, udbydere af elektroniske kommunikationsnet og -tjenester til offentligheden, forbrugergrupper, akademiske eksperter i cybersikkerhed, europæiske standardiseringsorganisationer 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 interessentcertificeringsgruppen, især hvad angår gruppens antal, sammensætning og den administrerende direktørs udpegelse af dens medlemmer, skal fastlægges i agenturets interne forretningsgange, følge bedste praksis for at sikre en retfærdig repræsentation og lige rettigheder for alle interessenter og skal offentliggøres.***

***3. Medlemmer af bestyrelsen kan ikke være medlemmer af interessentcertificeringsgruppen. Medlemmer af ENISA-rådgivningsgruppen kan også være medlemmer af interessentcertificeringsgruppen. Eksperter fra Kommissionen og medlemsstaterne har ret til, efter invitation, at være til stede på møderne i interessentcertificeringsgruppen.***

***Repræsentanter for andre organer, som den administrerende direktør skønner er relevante, kan indbydes til at være til stede på møderne i interessentcertificeringsgruppen og deltage i dens arbejde.***

***4. Interessentcertificeringsgruppen rådgiver agenturet med hensyn til udførelsen af dets aktiviteter vedrørende afsnit III i denne forordning. Den kan navnlig foreslå Kommissionen at udarbejde et forslag til en europæisk cybersikkerhedscertificeringsordning, jf. artikel 44 i denne forordning, og deltage i de i artikel 43-48 og artikel 53 i denne forordning omhandlede procedurer vedrørende godkendelse af sådanne ordninger.***

**Ændringsforslag 153**

**Forslag til forordning**
**Artikel 21 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 21 a*** |
| | ***Anmodninger til agenturet*** |
| | ***1. Agenturet etablerer og forvalter en kvikskranke, igennem hvilken anmodninger om rådgivning og bistand, som er omfattet af agenturets mål og arbejdsopgaver, skal indgives. Disse anmodninger skal ledsages af en redegørelse for det spørgsmål, der skal behandles. Agenturet udarbejder en oversigt over de potentielle ressourcemæssige konsekvenser og følger anmodningerne op inden for en rimelig frist. Afviser agenturet en anmodning, skal det begrunde afvisningen.*** |
| | ***2. Anmodninger i henhold til stk. 1 kan fremsættes af:*** |
| | ***a) Europa-Parlamentet*** |
| | ***b) Rådet*** |

| | |
|---|---|
| | ***c) Kommissionen og*** |
| | ***d) ethvert kompetent organ udpeget af en medlemsstat såsom en national tilsynsmyndighed som defineret i artikel 2 i direktiv 2002/21/EF.*** |
| | ***3. Bestemmelser for anvendelsen af stk. 1 og 2 i praksis, navnlig vedrørende forelæggelse, prioritering, opfølgning og orientering, fastsættes af bestyrelsen i agenturets interne forretningsgange.*** |

**Ændringsforslag 154**

**Forslag til forordning**
**Artikel 24 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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). | 2. Medlemmerne af bestyrelsen, den administrerende direktør, medlemmerne af ***ENISA-rådgivningsgruppen***, 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). |

**Ændringsforslag 155**

**Forslag til forordning**
**Artikel 26 – stk. 1 – afsnit 1 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Det foreløbige udkast til overslag skal være baseret på de mål og forventede resultater, der er fastlagt i det samlede programmeringsdokument, jf. artikel 21, stk. 1, i denne forordning, og skal tage hensyn til de finansielle ressourcer, der er nødvendige for at nå disse mål og forventede resultater i overensstemmelse*** |

| | |
|---|---|
| | ***med princippet om resultatorienteret budgetlægning.*** |

**Ændringsforslag 156**

**Forslag til forordning**
**Artikel 30 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | *(Vedrører ikke den danske tekst)* |

**Ændringsforslag 157**

**Forslag til forordning**
**Artikel 36 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 5. De ansattes personlige ansvar over for agenturet fastsættes i de ansættelsesvilkår, der gælder for agenturets personale. | 5. De ansattes personlige ansvar over for agenturet fastsættes i de ansættelsesvilkår, der gælder for agenturets personale. ***Der skal sikres en effektiv rekruttering af medarbejdere.*** |

**Ændringsforslag 158**

**Forslag til forordning**
**Artikel 37 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2. De oversættelsesopgaver, der er påkrævet i forbindelse med agenturets virksomhed, udføres af Oversættelsescentret for Den Europæiske Unions Organer. | 2. De oversættelsesopgaver, der er påkrævet i forbindelse med agenturets virksomhed, udføres af Oversættelsescentret for Den Europæiske Unions Organer ***eller andre oversættelsestjenesteydere i henhold til udbudsbestemmelserne og inden for de grænser, der er fastsat i de relevante finansielle regler***. |

**Ændringsforslag 159**

**Forslag til forordning**
**Artikel 39 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 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. ***I det omfang der samarbejdes med NATO, kan dette omfatte fælles cybersikkerhedsøvelser og fælles koordinering af cybersikkerhedshændelser.*** Disse ordninger må ikke skabe retlige forpligtelser for Unionen og dens medlemsstater. |

*Begrundelse*

*Eftersom cyberhændelser er grænseoverskridende, bør ENISA handle sammen med cybersikkerhedsaktører i Europa som NATO, når det er hensigtsmæssigt at gøre dette. Dette er særligt vigtigt, eftersom NATO kan have cyberkapacitet, som ENISA ikke har, og omvendt. I en situation, hvor cyberangreb i stigende grad rettes mod stater som sådan, er det særdeles vigtigt for Europas sikkerhed, at ENISA samarbejde med internationale organisationer som NATO på internationalt niveau.*

**Ændringsforslag 160**

**Forslag til forordning**
**Artikel 41 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2. Agenturets værtsmedlemsstat sikrer de bedst mulige betingelser for, at agenturet kan fungere efter hensigten, herunder stedets tilgængelighed, tilbud om tilstrækkelige uddannelsesfaciliteter for personalets børn, tilstrækkelig adgang til arbejdsmarkedet, social sikring og lægebehandling for såvel børn som | 2. Agenturets værtsmedlemsstat sikrer de bedst mulige betingelser for, at agenturet kan fungere efter hensigten, herunder ***ét hjemsted for hele agenturet,*** stedets tilgængelighed, tilbud om tilstrækkelige uddannelsesfaciliteter for personalets børn, tilstrækkelig adgang til arbejdsmarkedet, social sikring og |

| | |
|---|---|
| ægtefæller. | lægebehandling for såvel børn som ægtefæller. |

*Begrundelse*

*Agenturets nuværende struktur med dets administrative sæde i Heraklion og det centrale operationelle hovedsæde i Athen har vist sig at være ineffektiv og dyr. Hele ENISA's personale bør derfor arbejde i samme by. I betragtning af de kriterier, der er nævnt i dette stykke, bør dette sted være Athen.*

**Ændringsforslag 161**

**Forslag til forordning**
**Artikel 43 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| En europæisk cybersikkerhedscertificeringsordning skal attestere, at IKT-produkter og -tjenester***,*** ***der er certificeret i overensstemmelse med en sådan ordning***, ***opfylder de fastlagte krav*** for så vidt angår deres evne til, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, processer***,*** tjenester og ***systemer***. | En europæisk cybersikkerhedscertificeringsordning skal attestere, at ***de omfattede*** IKT-produkter***, -processer*** og -tjenester ***ikke har nogen kendte svagheder på certificeringstidspunktet og opfylder specifikke krav***, ***som kan henvise til europæiske og internationale standarder, teknisk specifikation og IKT-teknisk specifikation,*** for så vidt angår deres evne til ***i hele deres livscyklus***, på et givet tillidsniveau, at modstå handlinger, der sigter mod at kompromittere tilgængeligheden, autenticiteten, integriteten og fortroligheden af data, der opbevares, overføres eller behandles, eller de dermed forbundne funktioner eller tjenester, der tilbydes i eller er tilgængelige via disse produkter, processer ***og*** tjenester samt ***opfylde de specifikke sikkerhedsmål***. |

**Ændringsforslag 162**

**Forslag til forordning**
**Artikel 44 – stk. -1 (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***-1. Kommissionen vedtager delegerede retsakter i overensstemmelse med artikel*** |

***55a med henblik på at supplere denne forordning med et rullende EU-arbejdsprogram for europæiske cybersikkerhedscertificeringsordninger. Disse delegerede retsakter skal identificere fælles foranstaltninger, der skal gennemføres på EU-plan, og strategiske prioriteter. Det rullende EU-arbejdsprogram skal navnlig omfatte en prioriteret liste over identificerede IKT-produkter, -processer og -tjenester, der er egnede til at blive genstand for en europæisk cybersikkerhedscertificeringsordning, samt en analyse af, om der er et tilsvarende niveau af kvalitet, viden og ekspertise mellem overensstemmelsesvurderingsorganerne og de nationale tilsynsmyndigheder, og om nødvendigt et forslag til foranstaltninger for at opnå et sådant tilsvarende niveau.***

***Det indledende rullende EU-arbejdsprogram udarbejdes senest [six months after entry into force of this Regulation] og ajourføres efter behov, men under alle omstændigheder hvert andet år derefter. Det rullende EU-arbejdsprogram gøres offentligt tilgængeligt.***

***Inden Kommissionen vedtager eller ajourfører det rullende arbejdsprogram, hører den medlemsstaternes certificeringsgruppe, agenturet og interessentcertificeringsgruppen ved en åben, gennemsigtig og inklusiv høring.***

**Ændringsforslag 163**

**Forslag til forordning**
**Artikel 44 – stk. -1 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***-1a. Kommissionen anmoder, når det er berettiget, agenturet om at udarbejde et forslag til en europæisk*** |

| | |
|---|---|
| | ***cybersikkerhedscertificeringsordning. Anmodningen skal være baseret på det rullende EU-arbejdsprogram.*** |

**Ændringsforslag 164**

**Forslag til forordning**
**Artikel 44 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. ***På anmodning fra Kommissionen skal ENISA udarbejde*** et forslag til en europæisk cybersikkerhedscertificeringsordning, ***som opfylder kravene i denne forordnings*** artikel 45, ***46 og 47. Medlemsstaterne eller den europæiske cybersikkerhedscertificeringsgruppe ("gruppen")***, ***der er nedsat ved artikel 53,*** kan ***foreslå*** Kommissionen***, at der udarbejdes et forslag til en europæisk cybersikkerhedscertificeringsordning***. | 1. ***Anmodningen om*** et forslag til en europæisk cybersikkerhedscertificeringsordning ***skal indeholde anvendelsesområdet***, ***de relevante sikkerhedsmålsætninger, der er omhandlet i*** artikel 45, ***de relevante elementer, der er omhandlet i artikel 47***, ***og en frist for, hvornår den specifikke ordning*** kan ***blive få gyldighed.*** Kommissionen ***kan under udarbejdelsen af anmodningen høre agenturet, medlemsstaternes certificeringsgruppe og interessentcertificeringsgruppen***. |

**Ændringsforslag 165**

**Forslag til forordning**
**Artikel 44 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2. ***Under udarbejdelsen af forslaget til den*** i stk. 1 ***omhandlede ordning skal ENISA høre*** alle relevante interessenter og ***samarbejde*** tæt med ***gruppen***. ***Gruppen*** yder ***ENISA*** den bistand og ekspertrådgivning, som ***ENISA*** har behov for i forbindelse med udarbejdelsen af forslaget til en ordning, herunder også udtalelser om nødvendigt. | 2. ***Agenturet hører under udarbejdelsen af de*** i stk. **-**1 ***(ny) foreslåede ordninger*** alle relevante interessenter ***i form af en formel, åben, gennemsigtig*** og ***inklusiv høringsproces og samarbejder*** tæt med ***medlemsstaternes certificeringsgruppe, interessentcertificeringsgruppen, ad hoc-udvalg i overensstemmelse med denne forordnings artikel 20a samt de europæiske standardiseringsorganer***. ***Disse*** yder ***agenturet*** den bistand og ekspertrådgivning, som ***agenturet*** har behov for i forbindelse med udarbejdelsen af forslaget til en ordning, herunder også |

udtalelser om nødvendigt.

**Ændringsforslag 166**

**Forslag til forordning**
**Artikel 44 – stk. 3**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 3. ***ENISA*** fremsender forslaget til en europæisk cybersikkerhedscertificeringsordning udarbejdet i henhold til stk. 2 til Kommissionen. | 3. ***Agenturet*** fremsender forslaget til en europæisk cybersikkerhedscertificeringsordning udarbejdet i henhold til ***denne artikels*** stk. ***1 og*** 2 til Kommissionen. |

**Ændringsforslag 167**

**Forslag til forordning**
**Artikel 44 – stk. 4**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 4. Kommissionen kan på grundlag af den af ***ENISA*** foreslåede ordning vedtage ***gennemførelsesretsakter*** i overensstemmelse med artikel 55***, stk. 1, vedrørende*** europæiske cybersikkerhedscertificeringsordninger for IKT-produkter og -tjenester, der opfylder kravene i denne forordnings artikel 45, 46 og 47. | 4. Kommissionen kan på grundlag af den af ***agenturet*** foreslåede ordning vedtage ***delegerede retsakter*** i overensstemmelse med artikel 55***a med henblik på at supplere denne forordning med*** europæiske cybersikkerhedscertificeringsordninger for IKT-produkter***, -processer*** og -tjenester, der opfylder kravene i denne forordnings artikel 45, 46 og 47. |

**Ændringsforslag 168**

**Forslag til forordning**
**Artikel 44 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 5. ***ENISA*** skal drive en dedikeret hjemmeside, der giver oplysninger om og offentlig omtale af de europæiske cybersikkerhedscertificeringsordninger. | 5. ***Agenturet*** skal drive en dedikeret hjemmeside, der giver oplysninger om og offentlig omtale af de europæiske cybersikkerhedscertificeringsordninger***, herunder oplysninger om certificeringer, der er trukket tilbage eller udløbet, samt*** |

| | |
|---|---|
| | ***hvilke nationale certificeringer der er omfattet***. |
| | ***Når en europæisk cybersikkerhedscertificeringsordning opfylder de krav, som den havde til hensigt at dække i overensstemmelse med den relevante EU-harmoniseringslovgivning, offentliggør Kommissionen straks en henvisning hertil i Den Europæiske Unions Tidende og via andre kanaler i overensstemmelse med de vilkår, der er fastsat i den tilsvarende retsakt i henhold til Unionens harmoniseringslovgivning.*** |

**Ændringsforslag 169**

**Forslag til forordning**
**Artikel 44 – stk. 5 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***5 a. Agenturet reviderer efter den struktur, der er fastlagt i denne forordning, de vedtagne ordninger efter udløbet af deres gyldighedsperiode i overensstemmelse med artikel 47, stk. 1, litra ac), eller efter anmodning fra Kommissionen, idet der tages hensyn til feedback fra relevante interessenter.*** |

**Ændringsforslag 170**

**Forslag til forordning**
**Artikel 45 – stk. 1 – indledning**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| En europæisk cybersikkerhedscertificeringsordning skal være udformet således at den***, alt efter relevans,*** tager hensyn til følgende sikkerhedsmål: | En europæisk cybersikkerhedscertificeringsordning skal være udformet således**,** at den tager hensyn til følgende sikkerhedsmål ***og sikrer***: |

**Ændringsforslag 171**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| a) ***beskyttelse af data, som lagres***, ***overføres eller på anden måde behandles***, ***mod utilsigtet eller uautoriseret lagring, behandling***, ***adgang eller videregivelse*** | a) ***fortroligheden***, ***integriteten***, ***disponibiliteten og privatlivets fred for tjenester***, ***funktioner og data*** |

**Ændringsforslag 172**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) ***beskyttelse af data***, ***som lagres, overføres eller på anden måde behandles, mod utilsigtet*** eller ***uautoriseret ødelæggelse, utilsigtet tab eller ændring*** | b) ***at tjenester***, ***funktioner og data kun kan tilgås og anvendes af bemyndigede personer og/***eller ***godkendte systemer og programmer*** |

**Ændringsforslag 173**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra c**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| c) ***sikring af, at autoriserede personer, programmer eller maskiner udelukkende kan få adgang til data, tjenester eller funktioner, som de har adgangsret til*** | c) ***at der er indført en procedure til at indkredse og dokumentere al afhængighed og alle kendte sårbarheder i IKT-produkter, -processer og -tjenester*** |

**Ændringsforslag 174**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra d**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| d) ***registrering af***, ***hvilke data, funktioner eller tjenester, der er blevet videregivet, på hvilket tidspunkt og til*** | d) ***at IKT-produkter***, ***-processer og -tjenester ikke indeholder kendte sårbarheder*** |

***hvem***

**Ændringsforslag 175**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra e**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| e) ***sikring af, at det*** er ***muligt at kontrollere, hvilke data, tjenester og funktioner, der er tilgået eller anvendt***, ***på hvilket tidspunkt*** og ***af hvem*** | e) ***at der*** er ***indført en procedure til at reagere på nyligt opdagede sårbarheder i IKT-produkter***, ***-processer*** og ***-tjenester*** |

**Ændringsforslag 176**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra f**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| f) ***genetablering af tilgængelighed af og adgang til data***, ***tjenester*** og ***funktioner hurtigt i tilfælde af fysiske eller tekniske hændelser*** | f) ***at IKT-produkter***, ***-processer*** og ***tjenester er sikre som følge af standardindstillinger og indbygget sikkerhed*** |

**Ændringsforslag 177**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra g**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| g) ***sikring af, at*** IKT-produkter og -tjenester er forsynet med ajourført software og ikke indeholder kendte svagheder og har mekanismer til sikker opdatering af software. | g) ***at*** IKT-produkter og -tjenester er forsynet med ajourført software og ikke indeholder kendte svagheder og har mekanismer til sikker opdatering af software. |

**Ændringsforslag 178**

**Forslag til forordning**
**Artikel 45 – stk. 1 – litra g a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***g a) at andre risici, der er forbundet med cyberhændelser, såsom risici for liv, sundhed, miljø og andre væsentlige juridiske interesser, minimeres.*** |

**Ændringsforslag 179**

**Forslag til forordning**
**Artikel 46 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. En europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende tillidsniveauer: grundlæggende, betydeligt og/eller højt for IKT-produkter og -tjenester, der er certificeret under ordningen. | 1. En europæisk cybersikkerhedscertificeringsordning kan angive et eller flere af følgende ***risikobaserede*** tillidsniveauer ***afhængigt af sammenhængen og den påtænkte anvendelse af IKT-produkter, -processer og -tjenester***: grundlæggende, betydeligt og/eller højt for IKT-produkter***, -processer*** og -tjenester, der er certificeret under ordningen. |

**Ændringsforslag 180**

**Forslag til forordning**
**Artikel 46 – stk. 2 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| a) tillidsniveauet "grundlæggende" ***henviser*** til en ***attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en begrænset grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for*** et IKT-produkt ***eller*** en ***IKT-tjeneste,*** og ***som er karakteriseret ved henvisning*** til ***tekniske specifikationer, standarder*** og ***hertil knyttede procedurer, herunder tekniske kontroller***, ***hvis formål er at mindske risikoen*** for ***cybersikkerhedshændelser*** | a) tillidsniveauet "grundlæggende" ***svarer*** til en ***lav risiko med hensyn til den kombinerede sandsynlighed og skade i forbindelse med*** et IKT-produkt***,*** en ***proces*** og ***en tjeneste under hensyntagen*** til ***deres tilsigtede anvendelse*** og ***kontekst. Tillidsniveauet "grundlæggende" skaber tillid til***, ***at de kendte grundlæggende risici*** for ***cyberhændelser kan modstås.*** |

**Ændringsforslag 181**

**Forslag til forordning**
**Artikel 46 – stk. 2 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) tillidsniveauet "betydeligt" ***henviser*** til en ***attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en betydelig grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for et IKT-produkt eller en IKT-tjeneste***, ***og som er karakteriseret ved henvisning til tekniske specifikationer***, ***standarder*** og ***hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er*** at ***mindske risikoen for cybersikkerhedshændelser betydeligt*** | b) tillidsniveauet "betydeligt" ***svarer*** til en ***større risiko med hensyn til den kombinerede sandsynlighed og skade i forbindelse med et IKT-produkt, en proces og en tjeneste. Sikringsniveauet "betydelig" giver sikkerhed for***, ***at kendte risici for cyberhændelser kan forebygges***, og ***at der også er kapacitet til*** at ***modstå cyberangreb med begrænsede ressourcer.*** |

**Ændringsforslag 182**

**Forslag til forordning**
**Artikel 46 – stk. 2 – litra c**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| c) tillidsniveauet "højt" ***henviser*** til en ***attest, der udstedes som led i en europæisk cybersikkerhedscertificeringsordning, som giver en større grad af tillid til de påberåbte eller påståede cybersikkerhedsegenskaber for et IKT-produkt eller en IKT-tjeneste end attester med niveauet "betydelig"***, og ***som er karakteriseret ved henvisning*** til ***tekniske specifikationer, standarder og hertil knyttede procedurer, herunder tekniske kontroller, hvis formål er at forhindre cybersikkerhedshændelser***. | c) tillidsniveauet "højt" ***svarer*** til en ***stor risiko med hensyn til den kombinerede sandsynlighed og skade i forbindelse med et IKT-produkt, en proces og en tjeneste. tillidsniveauet "højt" giver sikkerhed for, at kendte risici for cyberhændelser kan forebygges***, og ***at der også er kapacitet*** til ***at modstå de nyeste cyberangreb, men at dette kræver betydelige ressourcer***. |

**Ændringsforslag 183**

**Forslag til forordning**
**Artikel 46 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 46 a*** |
| | ***Vurdering af tillidsniveauer for europæiske cybersikkerhedscertificeringsordninger*** |
| | ***1. For så vidt angår tillidsniveauet "grundlæggende" kan producenten eller udbyderen af IKT-produkter, -processer og -tjenester på eget ansvar foretage en selvevaluering af overensstemmelse.*** |
| | ***2. For så vidt angår tillidsniveauet "betydeligt" skal vurderingen være baseret på mindst en kontrol af, at de sikkerhedsmæssige funktioner i produktet, processen eller tjenesten stemmer overens med den tekniske dokumentation herfor.*** |
| | ***3. For så vidt angår tillidsniveauet "højt" skal vurderingsmetoden som minimum være baseret på en effektiv kontrol, der vurderer sikkerhedsfunktionernes modstandsdygtighed over for angribere med betydelige ressourcer.*** |

**Ændringsforslag 184**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| a) certificeringens genstand og omfang, herunder typer eller kategorier af IKT-produkter og -tjenester, der er omfattet | a) certificeringens genstand og omfang, herunder typer eller kategorier af IKT-produkter***, -processer*** og -tjenester, der er omfattet |

**Ændringsforslag 185**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra a a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***a a) krav til anvendelsesområde og cybersikkerhed, og dette anvendelsesområde og disse krav skal, når det er relevant, afspejle de nationale cybersikkerhedscertificeringer, som de erstatter, eller som er fastsat i retsakter*** |

**Ændringsforslag 186**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra a b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***a b) certificeringsordningens gyldighed*** |

**Ændringsforslag 187**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) detaljeret specifikation af cybersikkerhedskravene, som de specifikke IKT-produkter og -tjenester ***evalueres*** i forhold til, f.eks. ved at henvise til europæiske eller internationale standarder eller ***tekniske*** specifikationer | b) detaljeret specifikation af cybersikkerhedskravene, som de specifikke IKT-produkter***, -processer*** og -tjenester ***er evalueret*** i forhold til, f.eks. ved at henvise til europæiske eller internationale standarder***, tekniske specifikationer*** eller ***IKT-tekniske*** specifikationer***, defineret på en sådan måde, at certificeringen kan indbygges i eller baseres på producentens systematiske sikkerhedsprocesser, der følges i det pågældende produkts eller tjenestes udvikling og livscyklus*** |

**Ændringsforslag 188**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra b a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***b a) oplysninger om kendte cybertrusler, der ikke er omfattet af certificeringen, og vejledning til håndteringen af sådanne*** |

**Ændringsforslag 189**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra c**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| c) hvor det er relevant, et eller flere tillidsniveauer | c) hvor det er relevant, et eller flere tillidsniveauer***, der bl.a. tager højde for en risikobaseret tilgang*** |

**Ændringsforslag 190**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra c a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***c a) en angivelse af, hvorvidt selvevalueringen af overensstemmelse er tilladt i henhold til ordningen, og den gældende procedure for overensstemmelsesvurdering eller selverklæring om overensstemmelse eller begge*** |

**Ændringsforslag 191**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra d**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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 | d) de specifikke evalueringskriterier***, former for overensstemmelsesvurdering*** og ***metoder***, der er anvendt, for at påvise, at de specifikke mål omhandlet i artikel 45 er nået |

**Ændringsforslag 192**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra e**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| e) oplysninger til videresendelse til overensstemmelsesvurderingsorganer fra en ansøger, som er nødvendige med henblik på certificering | *(Vedrører ikke den danske tekst)* |

**Ændringsforslag 193**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra f**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| f) ***hvis ordningen fastsætter mærker eller etiketter, omstændighederne under hvilke disse mærker eller etiketter kan anvendes*** | f) ***oplysninger om cybersikkerhed i henhold til denne forordnings artikel 47a*** |

**Ændringsforslag 194**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra g**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| g) ***hvis overvågningen er en del af ordningen, reglerne*** for overvågning af overensstemmelsen med attesternes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav | g) ***reglerne*** for overvågning af overensstemmelsen med attesternes krav, herunder mekanismer til at dokumentere den fortsatte overholdelse af de angivne cybersikkerhedskrav |

**Ændringsforslag 195**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra h**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| h) betingelserne for udstedelse, | h) betingelserne for udstedelse, |

| | |
|---|---|
| bibeholdelse, forlængelse, udvidelse og indskrænkning af certificeringens omfang | bibeholdelse, forlængelse, ***revision,*** udvidelse og indskrænkning af certificeringens omfang ***samt certificeringens gyldighed*** |

**Ændringsforslag 196**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra h a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***h a) regler, der tager sigte på at håndtere sårbarheder, der kan opstå, efter certificeringen er udstedt, ved at iværksætte en dynamisk og vedvarende organisatorisk proces, der såvel involverer udbydere og brugere*** |

**Ændringsforslag 197**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra i**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| i) regler om følgerne af certificerede IKT-produkters og -tjenesters manglende overholdelse af certificeringskravene | i) regler om følgerne af ***selvevaluerede og*** certificerede IKT-produkters og -tjenesters manglende overholdelse af certificeringskravene |

**Ændringsforslag 198**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra j**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| j) regler om, hvordan ***hidtil uopdagede*** cybersikkerhedssårbarheder i IKT-produkter og -tjenester skal indberettes og håndteres | j) regler om, hvordan cybersikkerhedssårbarheder i IKT-produkter og -tjenester***, som ikke er offentligt kendt,*** skal indberettes og håndteres***, når de er blevet opdaget*** |

**Ændringsforslag 199**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra l**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| l) angivelse af nationale cybersikkerhedscertificeringsordninger, som dækker samme typer eller kategori af IKT-produkter og -tjenester | l) angivelse af nationale ***eller internationale*** cybersikkerhedscertificeringsordninger, som dækker samme typer eller kategori af IKT-produkter***, -processer*** og -tjenester***, -sikkerhedskrav samt evalueringskriterier og -metoder*** |

**Ændringsforslag 200**

**Forslag til forordning**
**Artikel 47 – stk. 1 – litra m a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***m a) betingelserne for gensidig anerkendelse af certificeringsordninger med tredjelande*** |

**Ændringsforslag 201**

**Forslag til forordning**
**Artikel 47 – stk. 1 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***1 a. vedligeholdelsesprocesser med opdateringer må ikke medføre, at certificeringen er ugyldig, medmindre sådanne opdateringer har betydelige negative følger for IKT-produktets, -processens eller -tjenesteydelsens sikkerhed.*** |

**Ændringsforslag 202**

**Forslag til forordning**
**Artikel 47 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
| --- | --- |
| | ***Artikel 47 a*** |
| | ***Oplysninger om cybersikkerhed for certificerede produkter, processer og tjenester*** |
| | ***1. Producenter og udbydere af IKT-produkter, -processer og -tjenester, der er omfattet af en certificeringsordning i henhold til denne forordning, giver slutbrugeren et dokument i elektronisk form eller i papirform, der mindst indeholder følgende oplysninger: tillidsniveauet for certificeringen for så vidt angår den planlagte anvendelse af IKT-produktet, -processen og -tjenesten, en beskrivelse af de risici, som certificeringen har til formål at skabe tillid til bekæmpelse af, anbefalinger om, hvordan brugere kan fremme cybersikkerheden for produktet, processen eller tjenesten yderligere, regelmæssigheden af og perioden for støtte efter eventuelle ajourføringer samt, hvor det er relevant, oplysninger om, hvordan brugerne kan bevare de vigtigste egenskaber ved produktet, processen eller tjenesten i tilfælde af et angreb.*** |
| | ***2. Det i denne artikels stk. 1 omhandlede dokument skal være tilgængeligt i hele produktets, processens eller tjenestens livscyklus, indtil dette produkt eller denne proces eller tjeneste ikke længere findes på markedet, og som minimum i en periode på fem år.*** |
| | ***3. Kommissionen vedtager gennemførelsesretsakter, der fastsætter en model for dette dokument. Kommissionen kan anmode agenturet om at udarbejde et forslag til en model for dokumentet. Denne gennemførelsesretsakt vedtages efter den i artikel 55 i denne forordning omhandlede undersøgelsesprocedure.*** |

**Ændringsforslag 203**

**Forslag til forordning**
**Artikel 48 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. IKT-produkter og -tjenester, der er certificeret i henhold til en europæisk cybersikkerhedscertificeringsordning, som er vedtaget i medfør af artikel 44, skal antages at overholde kravene i en sådan ordning. | 1. IKT-produkter***, -processer*** 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. |

**Ændringsforslag 204**

**Forslag til forordning**
**Artikel 48 – stk. 4 – indledning**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 4. Som en undtagelse fra stk. 3 ***kan det*** i behørigt begrundede tilfælde fastsættes i en europæisk cybersikkerhedscertificeringsordning, at en europæisk cybersikkerhedsattest, der fremgår af denne ordning, kun kan udstedes af et offentligt organ. Et sådant offentligt organ skal være ***en*** af ***følgende:*** | 4. Som en undtagelse fra stk. 3 ***og kun*** i behørigt begrundede tilfælde***, såsom af hensyn til den nationale sikkerhed, kan det*** fastsættes i en europæisk cybersikkerhedscertificeringsordning, at en europæisk cybersikkerhedsattest, der fremgår af denne ordning, kun kan udstedes af et offentligt organ. Et sådant offentligt organ skal være ***et organ, der er akkrediteret som et overensstemmelsesvurderingsorgan i medfør*** af ***artikel 51, stk. 1, i denne forordning. Den fysiske eller juridiske person, der indgiver sine IKT-produkter, -processer eller -tjenester til certificeringsmekanismen, skal stille alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, til rådighed for det i artikel 51 omhandlede overensstemmelsesvurderingsorgan.*** |

**Ændringsforslag 205**

**Forslag til forordning**
**Artikel 48 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 5. Den fysiske eller juridiske person, der indgiver sine IKT-produkter ***og -tjenester*** til certificeringsmekanismen, skal fremlægge alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, for det i artikel 51 omhandlede overensstemmelsesvurderingsorgan. | 5. Den fysiske eller juridiske person, der indgiver sine IKT-produkter***, -tjenester eller -processer*** til certificeringsmekanismen, skal fremlægge alle oplysninger, der er nødvendige for at gennemføre certificeringsproceduren, for det i artikel 51 omhandlede overensstemmelsesvurderingsorgan***, herunder oplysninger om kendte sikkerhedssårbarheder. Indgivelsen kan ske til et hvilket som helst overensstemmelsesvurderingsorgan som omhandlet i artikel 51.*** |

**Ændringsforslag 206**

**Forslag til forordning**
**Artikel 48 – stk. 6**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 6. Attester udstedes for en ***periode på højst tre år og kan forlænges på samme betingelser***, såfremt de relevante krav fortsat er opfyldt. | 6. Attester udstedes for ***et maksimalt tidsrum, som fastlægges i det konkrete tilfælde af hver enkelt ordning under hensyntagen til*** en ***rimelig livscyklus, som under alle omstændigheder ikke må overstige fem år***, såfremt de relevante krav fortsat er opfyldt. |

*Begrundelse*

*Dette sikrer fleksibilitet med hensyn til at tilpasse gyldighedsperioden til den påtænkte anvendelse.*

**Ændringsforslag 207**

**Forslag til forordning**
**Artikel 48 – stk. 7**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 7. En europæisk cybersikkerhedsattest udstedt i henhold til denne artikel skal anerkendes i alle medlemsstater. | 7. En europæisk cybersikkerhedsattest udstedt i henhold til denne artikel skal anerkendes i alle medlemsstater ***til opfyldelse af lokale cybersikkerhedskrav i forbindelse med IKT-produkter og -*** |

| | |
|---|---|
| | ***processer samt forbrugerelektronik omfattet af den pågældende attest, idet der tages hensyn til det specifikke tillidsniveau, der er omhandlet i artikel 46, og der skal ikke være nogen forskelsbehandling mellem disse attester baseret enten på oprindelsesmedlemsstaten eller det udstedende overensstemmelsesvurderingsorgan, jf. artikel 51***. |

*Begrundelse*

*For at undgå opsplitning i forbindelse med anerkendelsen og/eller overensstemmelsen af europæiske cybersikkerhedscertificeringsordninger er det nødvendigt, at det i artiklen fremhæves, at der ikke sker forskelsbehandling med hensyn til stedet for udstedelse af en attest.*

**Ændringsforslag 208**

**Forslag til forordning**
**Artikel 48 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 48 a*** |
| | ***Certificeringsordninger for operatører af væsentlige tjenester*** |
| | ***1. Når de europæiske cybersikkerhedscertificeringsordninger er blevet vedtaget i henhold til denne artikels stk. 2, skal operatører af væsentlige tjenester for at opfylde sikkerhedskravene i henhold til artikel 14 i direktiv (EU) 2016/1148 anvende de produkter, processer og tjenester, der er omfattet af disse certificeringsordninger.*** |
| | ***2. Senest [et år efter denne forordnings ikrafttræden] vedtager Kommissionen efter høring af samarbejdsgruppen, jf. artikel 11 i direktiv (EU) 2016/1148, delegerede retsakter i overensstemmelse med artikel 55a med henblik på at supplere denne forordning ved at opføre de kategorier af produkter, processer og tjenester, der*** |

***opfylder begge følgende kriterier:***

***a) de er beregnet til at blive anvendt af operatører af væsentlige tjenester, og***

***b) deres funktionssvigt ville have en væsentlig forstyrrende virkning på leveringen af den væsentlige tjenesteydelse.***

***3. Kommissionen vedtager delegerede retsakter i overensstemmelse med artikel 55a med henblik på at ændre denne forordning ved om nødvendigt at ajourføre listen over de i denne artikel, stk. 3, omhandlede kategorier af produkter, processer og tjenester.***

***4. Kommissionen anmoder agenturet om at udarbejde et udkast til en europæisk cybersikkerhedsordning i henhold til denne forordnings artikel 44, stk. (-1), for så vidt angår listen over de kategorier af produkter, processer og tjenester, der er omhandlet i denne artikels stk. 2 og 3, så snart denne liste er vedtaget eller ajourført. Attester, der er udstedt i henhold til sådanne europæiske cybersikkerhedscertificeringsordninger, skal have et tillidsniveau, der er højt.***

**Ændringsforslag 209**

**Forslag til forordning**
**Artikel 48 b (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 48 b*** |
| | ***Formelle indsigelser mod europæiske cybersikkerhedscertificeringsordninger*** |
| | ***1. Hvis en medlemsstat mener, at en europæisk cybersikkerhedscertificeringsordning ikke fuldt ud opfylder de krav, som det er hensigten, at den skal opfylde, og som er fastsat i den relevante EU-lovgivning, underretter den Kommissionen herom med en detaljeret forklaring. Kommissionen træffer efter høring af det*** |

***udvalg, der er nedsat i henhold til den relevante EU-harmoniseringslovgivning, hvis det er relevant, eller efter andre former for høring af sektoreksperter, afgørelse om:***

***a) at offentliggøre eller ikke at offentliggøre henvisningerne til den pågældende europæiske cybersikkerhedsordning i Den Europæiske Unions Tidende eller at offentliggøre henvisningerne med begrænsninger***

***b) at opretholde, opretholde med begrænsninger eller tilbagetrække henvisningerne til den pågældende europæiske cybersikkerhedsordning i Den Europæiske Unions Tidende.***

***2. Kommissionen offentliggør på sit websted oplysninger om den europæiske cybersikkerhedsordning, som har været genstand for den i stk. 1 i denne artikel omhandlede afgørelse.***

***3. Kommissionen underretter agenturet om sin afgørelse som omhandlet i stk. 1 og anmoder om nødvendigt om ændring af den pågældende europæiske cybersikkerhedsordning.***

***4. Den i denne artikel, stk. 1, litra a), omhandlede afgørelse vedtages efter rådgivningsproceduren i artikel 55, stk. 2, i denne forordning.***

***5. Den i denne artikel, stk. 1, litra b), omhandlede afgørelse vedtages efter undersøgelsessproceduren i artikel 55, stk. 2a (nyt), i denne forordning.***

**Ændringsforslag 210**

**Forslag til forordning**
**Artikel 49 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. Nationale cybersikkerhedscertificeringsordninger og | 1. Nationale cybersikkerhedscertificeringsordninger og |

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

**Ændringsforslag 211**

**Forslag til forordning**
**Artikel 49 – stk. 2**

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

**Ændringsforslag 212**

**Forslag til forordning**
**Artikel 49 – stk. 3 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***3 a. Medlemsstaterne underretter Kommissionen om enhver anmodning om at udarbejde nationale cybersikkerhedscertificeringsordninger og angiver grundene til at indføre dem.*** |

**Ændringsforslag 213**

**Forslag til forordning**
**Artikel 49 – stk. 3 b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***3 b. Medlemsstaterne fremsender på anmodning udkast til nationale cybersikkerhedscertificeringsordninger til andre medlemsstater, agenturet eller Kommissionen, som minimum i elektronisk form.*** |

**Ændringsforslag 214**

**Forslag til forordning**
**Artikel 49 – stk. 3 c (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***3 c. Medlemsstaterne besvarer og tager med forbehold for direktiv (EU) 2015/1535 inden for en frist på tre måneder behørigt hensyn til enhver bemærkning fra enhver anden medlemsstat, agenturet eller Kommissionen for så vidt angår ethvert udkast, jf. denne artikels stk. 3b.*** |

**Ændringsforslag 215**

**Forslag til forordning**
**Artikel 49 – stk. 3 d (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***3 d. Hvis bemærkninger, som er modtaget i henhold til denne artikels stk. 3c viser, at et udkast til en national cybersikkerhedscertificeringsordning med sandsynlighed vil have en negativ indvirkning på det indre markeds funktion, konsulterer den modtagende medlemsstat agenturet og Kommissionen, idet den tager størst mulig hensyn til disses bemærkninger, inden den vedtager udkastet til ordning.*** |

**Ændringsforslag 216**

**Forslag til forordning**
**Artikel 50 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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, efficient og sikker måde. | 5. Med henblik på en effektiv gennemførelse af forordningen er det hensigtsmæssigt, at disse myndigheder deltager i ***medlemsstaternes*** cybersikkerhedscertificeringsgruppe, der er oprettet i henhold til artikel 53, på en aktiv, effektiv, virkningsfuld og sikker måde. |

**Ændringsforslag 217**

**Forslag til forordning**
**Artikel 50 – stk. 6 – litra a**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| a) overvåge og håndhæve anvendelsen af bestemmelserne i dette afsnit på nationalt niveau og ***føre tilsyn med, at de attester, der er udstedt af overensstemmelsesvurderingsorganer***, som ***er etableret på deres respektive område, er*** i ***overensstemmelse med de krav***, ***der er fastsat i dette afsnit og i den tilsvarende europæiske cybersikkerhedscertificeringsordning*** | a) overvåge og håndhæve anvendelsen af bestemmelserne i dette afsnit på nationalt niveau og ***verificere overholdelsen i overensstemmelse med de regler***, som ***den europæiske cybersikkerhedscertificeringsgruppe har vedtaget*** i ***henhold til artikel 53***, ***stk. 3, litra da), af:*** |
| | ***i) de attester, der er udstedt af overensstemmelsesvurderingsorganer, som er etableret på deres respektive område, med de krav, der er fastsat i dette afsnit og i den tilsvarende europæiske cybersikkerhedscertificeringsordning og*** |
| | ***ii) selverklæringer om overensstemmelse, som er afgivet i henhold til en ordning for en IKT-proces, et IKT-produkt eller en IKT-tjeneste*** |

**Ændringsforslag 218**

**Forslag til forordning**

**Artikel 50 – stk. 6 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) overvåge ***og*** føre tilsyn med overensstemmelsesvurderingsorganers aktiviteter i forbindelse med denne forordning, herunder med hensyn til anmeldelsen af overensstemmelsesvurderingsorganer og de relaterede opgaver, der er fastsat i denne forordnings artikel 52 | b) overvåge***,*** føre tilsyn med ***og mindst hvert andet år vurdere*** overensstemmelsesvurderingsorganers aktiviteter i forbindelse med denne forordning, herunder med hensyn til anmeldelsen af overensstemmelsesvurderingsorganer og de relaterede opgaver, der er fastsat i denne forordnings artikel 52 |

**Ændringsforslag 219**

**Forslag til forordning**
**Artikel 50 – stk. 6 – litra b a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***b a) foretage revisioner for at sikre, at der gælder tilsvarende standarder i EU, og indberette resultaterne heraf til agenturet og gruppen*** |

*Begrundelse*

*Dette bidrager til at sikre anvendelsen af et ensartet niveau for tjenester og kvalitet i hele EU og bidrager til at forebygge muligheden for "certificeringsshopping".*

**Ændringsforslag 220**

**Forslag til forordning**
**Artikel 50 – stk. 6 – litra c**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| c) behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en rimelig frist | c) behandle klager fra fysiske eller juridiske personer i forbindelse med attester udstedt af overensstemmelsesvurderingsorganer, der er etableret på deres område, ***eller til selvevaluering af overensstemmelse,*** undersøge genstanden for klagen i relevant omfang og underrette klageren om forløbet og resultatet af undersøgelsen inden for en |

| | |
|---|---|
| | rimelig frist |

**Ændringsforslag 221**

**Forslag til forordning**
**Artikel 50 – stk. 6 – litra c a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***ca) rapportere om resultaterne af kontrollen, jf. litra a), og vurderingerne, jf. litra b), til agenturet og den europæiske cybersikkerhedscertificeringsgruppe*** |

**Ændringsforslag 222**

**Forslag til forordning**
**Artikel 50 – stk. 6 – litra d**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| d) samarbejde med andre nationale certificeringstilsynsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings eller specifikke cybersikkerhedscertificeringsordningers krav | d) samarbejde med andre nationale certificeringstilsynsmyndigheder eller andre offentlige myndigheder, ***såsom nationale databeskyttelsestilsynsmyndigheder,*** herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters***, -processers*** og -tjenesters manglende overholdelse af denne forordnings eller specifikke cybersikkerhedscertificeringsordningers krav |

**Ændringsforslag 223**

**Forslag til forordning**
**Artikel 50 – stk. 6 – litra d**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| d) samarbejde med andre nationale certificeringstilsynsmyndigheder eller andre offentlige myndigheder, herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters | d) samarbejde med andre nationale certificeringstilsynsmyndigheder eller andre offentlige myndigheder, ***såsom nationale databeskyttelsestilsynsmyndigheder,*** |

| | |
|---|---|
| manglende overholdelse af denne forordnings eller specifikke ***cybersikkerhedscertificeringsordningers*** krav | herunder ved at dele oplysninger om mulige tilfælde af IKT-produkters og -tjenesters manglende overholdelse af denne forordnings eller specifikke ***IT-sikkerhedscertificeringsordningers*** krav |

*Begrundelse*

*I overensstemmelse med udtalelsen fra EDPS.*

**Ændringsforslag 224**

**Forslag til forordning**
**Artikel 50 – stk. 7 – litra c a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***c a) at kunne inddrage akkrediteringen af overensstemmelsesvurderingsorganer, som ikke overholder bestemmelserne i denne forordning.*** |

**Ændringsforslag 225**

**Forslag til forordning**
**Artikel 50 – stk. 7 – litra e**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| e) at kunne tilbagekalde, i overensstemmelse med national ret, attester, som ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning | e) at kunne tilbagekalde, i overensstemmelse med national ret, attester, som ikke overholder bestemmelserne i denne forordning eller i en europæisk cybersikkerhedscertificeringsordning, ***og underrette de nationale akkrediteringsorganer herom*** |

**Ændringsforslag 226**

**Forslag til forordning**
**Artikel 50 – stk. 8**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 8. De nationale | 8. De nationale |

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

**Ændringsforslag 227**

**Forslag til forordning**
**Artikel 50 – stk. 8 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***8a. Alle nationale certificeringstilsynsmyndigheder og alle medlemmer af og ansatte i alle nationale certificeringstilsynsmyndigheder er i overensstemmelse med EU-retten eller medlemsstatslovgivningen såvel under embeds- og ansættelsesperioden som efter dens ophør underlagt tavshedspligt for så vidt angår alle fortrolige oplysninger, der er kommet til deres kendskab under udøvelsen af deres hverv eller deres beføjelser.*** |

**Ændringsforslag 228**

**Forslag til forordning**
**Artikel 50 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 50 a*** |
| | ***Peerevaluering*** |
| | ***1. Nationale certificeringstilsynsmyndigheder underkastes en peerevaluering i forbindelse med udøvelsen af enhver af de i artikel 50 omhandlede aktiviteter, som agenturet tilrettelægger*** |
| | ***2. Peerevalueringen foretages på grundlag af holdbare og gennemsigtige*** |

***evalueringskriterier og -procedurer, især med hensyn til strukturelle krav, krav til menneskelige ressourcer og procedurekrav, samt med hensyn til fortrolighed og klager. Det skal være muligt at appellere afgørelser truffet på baggrund af evalueringen.***

***3. Peerevalueringen omfatter vurderinger af de procedurer, der er indført af nationale certificeringstilsynsmyndigheder, navnlig procedurerne for at kontrollere, om attesterne er i overensstemmelse med kravene, procedurerne for overvågning af og tilsyn med overensstemmelsesvurderingsorganernes aktiviteter, personalets kompetencer, korrektheden af kontrolundersøgelserne og inspektionsmetoden samt rigtigheden af resultaterne. Ved peerevalueringen skal det ligeledes vurderes, hvorvidt de pågældende nationale certificeringstilsynsmyndigheder har tilstrækkelige ressourcer til, at de kan udføre deres opgaver i overensstemmelse med artikel 50, stk. 4.***

***4. Peerevaluering af en national certificeringstilsynsmyndighed udføres af to nationale certificeringstilsynsmyndigheder i andre medlemsstater og Kommissionen og udføres mindst én gang hvert femte år. Agenturet kan deltage i peerevalueringen og træffer afgørelse om dets deltagelse på baggrund af en risikovurderingsanalyse.***

***5. Kommissionen kan vedtage delegerede retsakter i overensstemmelse med artikel 55a med henblik på at supplere denne forordning ved at udarbejde en plan for peerevalueringen, som dækker en periode på mindst fem år, og som fastsætter kriterierne for sammensætningen af peerevalueringsholdet, den anvendte metode for peerevalueringen, tidsplanen, hyppighed samt de øvrige opgaver i forbindelse med peerevalueringen. Kommissionen tager behørigt hensyn til***

***overvejelserne fra medlemsstaternes certificeringsgruppe, når den vedtager de pågældende delegerede retsakter.***

***6. Resultatet af peerevalueringen undersøges af medlemsstaternes certificeringsgruppe. Agenturet udarbejder et sammendrag af resultatet og giver om nødvendigt vejledning og dokumenter om bedste praksis og offentliggør dem.***

**Ændringsforslag 229**

**Forslag til forordning**
**Artikel 51 – stk. 1 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***1a. Ved tillidsniveauet "højt" skal overensstemmelsesvurderingsorganet ud over at være akkrediteret også være anmeldt af den nationale certificeringstilsynsmyndighed med hensyn til dets kompetencer og ekspertise inden for cybersikkerhedsvurdering. Den nationale certificeringstilsynsmyndighed foretager regelmæssig revision af overensstemmelsesvurderingsorganernes kompetencer og ekspertise.*** |

*Begrundelse*

*Høje tillidsniveauer kræver effektivitetstest. Overensstemmelsesvurderingsorganer, som foretager effektivitetstest, skal regelmæssigt underkastes revision af deres kompetencer og ekspertise med henblik på især at sikre testenes kvalitet.*

**Ændringsforslag 230**

**Forslag til forordning**
**Artikel 51 – stk. 2 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***2 a. Der skal foretages revisioner for at sikre, at der gælder tilsvarende standarder i EU, og resultaterne heraf skal indberettes til agenturet og gruppen.*** |

**Ændringsforslag 231**

**Forslag til forordning**
**Artikel 51 – stk. 2 b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***2b. Hvis producenterne vælger en "selverklæring om overensstemmelse" i henhold til artikel 48, stk. 3, tager overensstemmelsesvurderingsorganerne yderligere skridt med henblik på at kontrollere de interne procedurer, som producenterne har fulgt, så det sikres, at deres produkter og/eller tjenester overholder kravene i den europæiske cybersikkerhedscertificeringsordning.*** |

**Ændringsforslag 232**

**Forslag til forordning**
**Artikel 52 – stk. 5**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 5. Kommissionen kan ved hjælp af ***delegerede retsakter*** fastlægge vilkår, formater og procedurer for anmeldelserne omhandlet i stk. 1. Disse ***delegerede retsakter*** vedtages efter undersøgelsesproceduren omhandlet i artikel 55, stk. 2. |

**Ændringsforslag 233**

**Forslag til forordning**
**Artikel 53 – overskrift**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| ***Den europæiske cybersikkerhedscertificeringsgruppe*** | ***Medlemsstaterne certificeringsgruppe***<br><br>***(Dette ændringsforslag gælder for hele teksten.*** *Hvis det vedtages, skal ændringerne foretages alle relevante* |

*steder).*

**Ændringsforslag 234**

**Forslag til forordning**
**Artikel 53 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. ***Den europæiske cybersikkerhedscertificeringsgruppe (gruppen")*** oprettes. | 1. ***Medlemsstaterne certificeringsgruppe*** oprettes. |

**Ændringsforslag 235**

**Forslag til forordning**
**Artikel 53 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 2. ***Gruppen*** sammensættes af nationale certificeringstilsynsmyndigheder ***Myndighederne repræsenteres ved lederne af eller andre højtstående repræsentanter for de nationale certificeringstilsynsmyndigheder.*** | 2. ***Medlemsstaterne certificeringsgruppe*** sammensættes af nationale certificeringstilsynsmyndigheder ***fra hver medlemsstat***. Myndighederne repræsenteres ved lederne af eller andre højtstående repræsentanter for de nationale certificeringstilsynsmyndigheder. ***Medlemmer af interessentcertificeringsgruppen kan indbydes til at deltage i gruppens møder og deltage i dens arbejde.*** |

**Ændringsforslag 236**

**Forslag til forordning**
**Artikel 53 – stk. 3 – indledning**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 3. ***Gruppen*** har følgende opgaver: | 3. ***Medlemsstaterne certificeringsgruppe*** har følgende opgaver: |

**Ændringsforslag 237**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra b**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| b) at bistå, rådgive og samarbejde med ***ENISA*** i forbindelse med udarbejdelse af forslag til ordninger i overensstemmelse med artikel 44 | b) at bistå, rådgive og samarbejde med ***agenturet*** i forbindelse med udarbejdelse af forslag til ordninger i overensstemmelse med artikel 44 |

**Ændringsforslag 238**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra d a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***d a) at vedtage henstillinger vedrørende fastsættelse af intervallerne for, hvornår de nationale certificeringstilsynsmyndigheders skal foretage kontrol af certificeringer og selvevalueringer af overensstemmelse og fastsætte kriterierne, omfanget og formålet med de pågældende kontroller, samt vedtage fælles regler og standarder for rapportering i henhold til artikel 50, stk. 6*** |

**Ændringsforslag 239**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra e**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| e) at undersøge de relevante udviklinger inden for cybersikkerhedscertificering og udveksle god praksis om cybersikkerhedscertificeringsordninger | e) at undersøge de relevante udviklinger inden for cybersikkerhedscertificering og udveksle ***oplysninger og*** god praksis om cybersikkerhedscertificeringsordninger |

**Ændringsforslag 240**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra f a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***f a) at lette tilpasningen af de europæiske cybersikkerhedsordninger til internationalt anerkendte standarder, herunder ved at revidere eksisterende europæiske cybersikkerhedsordninger og, hvor det er relevant, henstille til agenturet at samarbejde med relevante internationale standardiseringsorganisationer med henblik på at afhjælpe mangler eller huller i internationalt anerkendte standarder*** |

**Ændringsforslag 241**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra f b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***f b) at etablere en peerevalueringsproces. Denne proces skal især tage hensyn til den krævede tekniske ekspertise af nationale certificeringstilsynsmyndigheder i udførelsen af deres opgaver, som omhandlet i artikel 48 og 50, og om nødvendigt omfatte udvikling af dokumenter om retningslinjer og bedste praksis for at forbedre de nationale certificeringstilsynsmyndigheders overholdelse af denne forordning*** |

**Ændringsforslag 242**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra f c (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***f c) at føre tilsyn med overvågningen og vedligeholdelse af en attest*** |

**Ændringsforslag 243**

**Forslag til forordning**
**Artikel 53 – stk. 3 – litra f d (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***f d) at tage hensyn til resultaterne af høringer af interessenter i forbindelse med udarbejdelse af forslag til en ordning i overensstemmelse med artikel 44*** |

**Ændringsforslag 244**

**Forslag til forordning**
**Artikel 53 – stk. 4**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 4. Kommissionen varetager formandskabet og sekretariatsfunktionen for gruppen med bistand fra ***ENISA***, som fastsat i artikel 8, litra a). | 4. Kommissionen varetager formandskabet ***for medlemsstaternes certificeringsgruppe*** og sekretariatsfunktionen for gruppen med bistand fra ***agenturet***, som fastsat i artikel 8, litra a). |

**Ændringsforslag 245**

**Forslag til forordning**
**Artikel 53 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 53a*** |
| | ***Ret til effektive retsmidler over for en tilsynsmyndighed eller et overensstemmelsesvurderingsorgan*** |
| | ***1. Uden at det berører eventuelle andre administrative eller udenretslige midler har enhver fysisk eller juridisk person ret til effektive retsmidler:*** |
| | ***a) over for en afgørelse truffet af et overensstemmelsesvurderingsorgan eller en national certificeringstilsynsmyndighed vedrørende dem, herunder, hvis det er relevant, i*** |

| | |
|---|---|
| | ***forbindelse med udstedelse, ikkeudstedelse eller anerkendelse af en europæisk cybersikkerhedsattest, som denne person er indehaver af, og*** |
| | ***b) hvis en national certificeringstilsynsmyndighed ikke behandler en klage, som hører ind under dens kompetence.*** |
| | ***2. En sag mod et overensstemmelsesvurderingsorgan eller en national tilsynsmyndighed anlægges ved en domstol i den medlemsstat, hvor overensstemmelsesvurderingsorganet eller den nationale certificeringstilsynsmyndighed er etableret.*** |

**Ændringsforslag 246**

**Forslag til forordning**
**Artikel 55 – stk. 2 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***2 a. Når der henvises til dette stykke, anvendes artikel 5 i forordning (EU) nr. 182/2011.*** |

**Ændringsforslag 247**

**Forslag til forordning**
**Artikel 55 a (ny)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***Artikel 55 a*** |
| | ***Udøvelse af de delegerede beføjelser*** |
| | ***1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.*** |
| | ***2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 44 og 48a, tillægges Kommissionen for en ubegrænset periode fra [datoen for denne forordnings ikrafttræden].*** |

***3. Delegationen af beføjelser, jf. artikel 44 og 48a, kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.***

***4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale om bedre lovgivning af 13. april 2016.***

***5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.***

***6. En delegeret retsakt vedtaget i henhold til artikel 44 og artikel 48a træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.***

**Ændringsforslag 248**

**Forslag til forordning**
**Artikel 56 – stk. 1**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 1. Senest ***fem*** år efter den dato, der er omhandlet i artikel 58, og hvert ***femte*** år | 1. Senest ***to*** år efter den dato, der er omhandlet i artikel 58, og hvert ***andet*** 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. | 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. |

**Ændringsforslag 249**

**Forslag til forordning**
**Artikel 56 – stk. 2**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 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***, -processer*** og -tjenester i EU og forbedre det indre markeds funktion. |

**Ændringsforslag 250**

**Forslag til forordning**
**Artikel 56 – stk. 2 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***2 a. Evalueringen skal vurdere, om det er nødvendigt at indføre væsentlige cybersikkerhedskrav for at få adgang til det indre marked med henblik på at forhindre produkter, tjenester og processer, der kommer ind på EU-markedet, som ikke opfylder grundlæggende cybersikkerhedskrav.*** |

**Ændringsforslag 251**

**Forslag til forordning**
**Bilag -I (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***BILAG -I*** |
| | ***Ved lancering af EU-rammen for cybersikkerhedscertificering er det sandsynligt, at der vil være fokus på områder af umiddelbar interesse for at imødegå de udfordringer, der udgøres af nye teknologier. Området inden for Tingenes Internet (IoT) er af særlig interesse, da det spænder hen over både forbrugerbehov og industrielle behov. Der foreslås følgende prioritetsliste til vedtagelse inden for rammen for certificering:*** |
| | ***1) Certificering af cloud-tjenesteudbydere.*** |
| | ***2) Certificering af IoT-enheder, herunder:*** |
| | ***a. enheder på individuelt plan, såsom kropsbårne intelligente anordninger*** |
| | ***b. enheder på fællesskabsplan, såsom intelligente biler, intelligente hjem og sundhedsanordninger*** |
| | ***c. enheder på samfundsplan, såsom intelligente byer og intelligente net.*** |
| | ***3) Industri 4.0 med intelligente, sammenkoblede cyberfysiske systemer, som automatiserer alle faser af industrielle processer, lige fra design og produktion til drift, forsyningskæder og service/vedligeholdelse.*** |
| | ***4) Certificering af teknologier or produkter, der anvendes til hverdag, for eksempel netværksanordninger såsom internetroutere til privatboliger.*** |

**Ændringsforslag 252**

**Forslag til forordning**
**Bilag I – del 1 – nr. 5 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
| --- | --- |
| | ***5a. Hvis et overensstemmelsesvurderingsorgan ejes eller drives af en offentlig enhed eller institution, skal det sikres og dokumenteres, at det er uafhængigt, og at der ikke er interessekonflikter mellem certificeringstilsynsmyndigheden på den ene side og overensstemmelsesvurderingsorganet på den anden side.*** |

**Ændringsforslag 253**

**Forslag til forordning**
**Bilag I – del 1 – nr. 8**

| *Kommissionens forslag* | *Ændringsforslag* |
| --- | --- |
| 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. | 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. ***Eventuelle tildelinger af underentrepriser eller høringer af eksterne personer skal være veldokumenterede, må ikke involvere nogen mellemmænd og skal være underlagt en skriftlig aftale, der blandt andet omfatter tavshedspligt og interessekonflikter. Det pågældende overensstemmelsesvurderingsorgan skal påtage sig det fulde ansvar for de udførte opgaver.*** |

**Ændringsforslag 254**

**Forslag til forordning**
**Bilag I – del 1 – nr. 12**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 12. Der skal være sikkerhed for overensstemmelsesvurderingsorganernes, deres øverste ledelses og vurderingspersonalets uvildighed. | 12. Der skal være sikkerhed for overensstemmelsesvurderingsorganernes, deres øverste ledelses og vurderingspersonalets ***og underleverandørers*** uvildighed. |

**Ændringsforslag 255**

**Forslag til forordning**
**Bilag I – del 1 – nr. 15**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| 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. | 15. ***Overensstemmelsesvurderingsorganet og dets*** personale***, udvalg, datterselskaber, underleverandører og overensstemmelsesorganets eventuelle tilknyttede organer eller personalet i eksterne organer skal bevare fortroligheden og*** 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 ***i de tilfælde, hvor offentliggørelse er påkrævet i henhold til EU-retten eller medlemsstatens lovgivning, som sådanne personer er underlagt, og undtagen*** over for de kompetente myndigheder i den medlemsstat, hvor aktiviteterne udføres. ***Ejendomsrettigheder beskyttes. Overensstemmelsesvurderingsorganet skal have indført dokumenterede procedurer i henhold til bestemmelserne i nærværende afdeling 15.*** |

**Ændringsforslag 256**

**Forslag til forordning**
**Bilag I – del 1 – nr. 15 a (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|

| | |
|---|---|
| | ***15a. Med undtagelse af afdeling 15 forhindrer kravene i dette bilag på ingen måde, at der udveksles tekniske oplysninger og reguleringsmæssige retningslinjer mellem et overensstemmelsesvurderingsorgan og en person, der ansøger, eller overvejer at ansøge, om certificering.*** |

**Ændringsforslag 257**

**Forslag til forordning**
**Bilag I – afdeling 1 – nr. 15 b (nyt)**

| *Kommissionens forslag* | *Ændringsforslag* |
|---|---|
| | ***15b.***<br>***Overensstemmelsesvurderingsorganerne skal udøve deres virksomhed i overensstemmelse med et sæt sammenhængende, reelle og rimelige vilkår og betingelser, idet der tages hensyn til interesser hos små og mellemstore virksomheder som fastlagt i Kommissionens henstilling 2003/361/EF for så vidt angår gebyrer.*** |