Raad van de
Europese Unie

Brussel, 14 september 2017
(OR. en)

12183/17

Interinstitutioneel dossier:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

VOORSTEL

van:	de heer Jordi AYET PUIGARNAU, directeur, namens de secretaris-generaal van de Europese Commissie
aan:	de heer Jeppe TRANHOLM-MIKKELSEN, secretaris-generaal van de Raad van de Europese Unie
Nr. Comdoc.:	COM(2017) 477 final
Betreft:	Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")

Hierbij gaat voor de delegaties document COM(2017) 477 final.

Bijlage: COM(2017) 477 final

EUROPESE
COMMISSIE

Brussel, 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")

(Voor de EER relevante tekst)

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

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

De Europese Unie heeft een aantal maatregelen getroffen om de weerbaarheid en haar paraatheid inzake cyberbeveiliging te verhogen. De eerste, in 2013 vastgestelde, EU-strategie inzake cyberbeveiliging[1] omvat strategische doelstellingen en concrete maatregelen voor het tot stand brengen van veerkracht, voor het terugdringen van cybercriminaliteit alsmede voor de ontwikkeling van cyberdefensiebeleid- en capaciteit, van industriële en technologische voorzieningen en van een coherent internationaal cyberbeveiligingsbeleid voor de EU. Er hebben op dat gebied sindsdien belangrijke ontwikkelingen plaatsgevonden, waaronder met name het tweede mandaat voor het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa)[2] en de vaststelling van de **richtlijn inzake de beveiliging van netwerk- en informatiesystemen**[3] ("de NIS-richtlijn"), die de basis vormen voor het onderhavige voorstel.

Verder heeft **de Europese Commissie in 2016 een mededeling vastgesteld over het versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche**[4], waarin verdere maatregelen werden aangekondigd om nauwere samenwerking betere uitwisseling van informatie en kennis tot stand te brengen, en om weerbaarheid en paraatheid van de EU te verbeteren, waarbij ook rekening werd gehouden met het vooruitzicht op grootschalige incidenten en een eventuele pan-Europese cyberveiligheidscrisis. In dat kader heeft de Commissie aangekondigd sneller dan voorzien over te gaan tot de **evaluatie** en **herziening** van Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad inzake Enisa en tot intrekking van Verordening (EG) nr. 460/2004 ("de Enisa-verordening"). Dit evaluatieproces kan leiden tot een mogelijke hervorming van het Agentschap en versterking van haar vermogens en capaciteiten om de lidstaten op duurzame wijze te ondersteunen. Het Agentschap zou daardoor een meer operationele en centrale rol krijgen met betrekking tot de totstandbrenging van weerbaarheid op het gebied van cyberbeveiliging; tevens zouden in het nieuwe mandaat van het Agentschap haar nieuwe verantwoordelijkheden op grond van de NIS-richtlijn worden opgenomen.

De NIS-richtlijn is een eerste essentiële stap op weg naar het bevorderen van een cultuur van risicobeheersing doordat er beveiligingseisen worden ingevoerd die wettelijke verplichtingen zijn voor de belangrijkste economische actoren, en met name voor verleners van essentiële diensten en leveranciers van bepaalde belangrijke digitale diensten. Beveiligingseisen worden beschouwd als essentieel element voor de waarborging van de voordelen van de voortschrijdende digitalisering van de samenleving en het steeds aantal genetwerkte apparaten

---

1 Gezamenlijke mededeling van de Europese Commissie en de Europese Dienst voor extern optreden: "Strategie inzake cyberbeveiliging van de Europese Unie: Een open, veilige en beveiligde cyberspace" – JOIN(2013) 1 final.

2 Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad inzake het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en tot intrekking van Verordening (EG) nr. 460/2004.

3 Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

4 Mededeling van de Commissie "Versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche", COM(2016) 0410 final.

wordt steeds groter ("internet der dingen"); in de mededeling van 2016 werd daarom ook geopperd een kader voor de beveiligingscertificering van ICT-producten en -diensten tot stand te brengen om het vertrouwen en de beveiliging in de digitale eengemaakte markt te versterken. De certificering van ICT voor cyberbeveiliging wordt in het bijzonder relevant vanwege het toegenomen gebruik van technologieën en die een hoog cyberbeveiligingsniveau vergen, zoals genetwerkte en zelfrijdende auto's, elektronische gezondheidszorg en besturingssystemen voor industriële automatisatie (IACS).

Deze beleidsmaatregelen en aankondigingen zijn verder versterkt in de **conclusies van de Raad** van 2016 , waarin het volgende werd erkend: "cyberdreigingen en -kwetsbaarheden blijven evolueren en worden groter, wat noopt tot een permanente nauwere samenwerking, vooral bij de behandeling van grootschalige grensoverschrijdende cyberincidenten". In de conclusies wordt bevestigd dat de Enisa-verordening mede de kern vormt van een EU-kader voor cyberbeveiliging[5] en wordt de Commissie opgeroepen om verdere stappen te nemen om de kwestie certificering op Europees niveau aan te pakken.

Om een certificeringsstelsel tot stand te brengen, moet een passend governancestelsel op EU-niveau worden opgezet, waarbij onder meer gebruik wordt gemaakt van gedegen expertise die door een onafhankelijk EU-agentschap wordt verstrekt. In dat kader wordt het Enisa in het onderhavige voorstel aangewezen als op EU-niveau voor kwesties inzake cyberbeveiliging bevoegd orgaan dat het meest in aanmerking komt om deze rol op zich te nemen en de werkzaamheden op het gebied van certificering van de desbetreffende nationale bevoegde instanties met elkaar in verbinding te brengen en te coördineren.

In haar mededeling over de **tussentijdse evaluatie van de strategie voor de digitale eengemaakte markt van mei 2017** heeft de Commissie verder gepreciseerd dat zij het mandaat van het Enisa tegen september 2017 zou herzien teneinde de rol van het Enisa in het veranderde ecosysteem op het gebied van cyberbeveiliging vast te stellen en maatregelen inzake cyberbeveiligingsnormen, -certificering en -etikettering te ontwikkelen om op ICT gebaseerde systemen, met inbegrip van gekoppelde objecten, cyberveiliger te maken[6]. In de **conclusies van de Europese Raad** van juni 2017[7] wordt het toegejuicht dat de Commissie de strategie voor cyberbeveiliging in september wil herzien en voor het eind van 2017 met verdere gerichte maatregelen wil komen.

De voorgestelde verordening voorziet in een uitgebreide reeks maatregelen die voortbouwen op voorgaande acties en draagt bij tot de verwezenlijking van specifieke doelstellingen die elkaar versterken:

- verhogen van de **vermogens en paraatheid** van de lidstaten en het bedrijfsleven;
- verbeteren van de **samenwerking en coördinatie** tussen de lidstaten en de EU-instellingen. -agentschappen en -organen;
- versterken van de **vermogens op EU-niveau ter aanvulling op maatregelen van de lidstaten**, met name in het geval van grensoverschrijdende cybercrises;
- versterken van het **bewustzijn** van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties;

---

5 Conclusies van de Raad over het versterken van het Europese cyberbeveiligingssysteem en het bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche - 15 november 2016.

6 Mededeling van de Commissie over de tussentijdse evaluatie van de uitvoering van de strategie voor de digitale interne markt - COM(2017) 228 final.

7 Bijeenkomst van de Europese Raad (22 en 23 juni 2017) – Conclusies EUCO 8/17.

- verbeteren van de algehele **transparantie van de zekerheid inzake cyberbeveiliging**[8] van ICT-producten en -diensten teneinde het vertrouwen in de digitale eengemaakte markt en in digitale innovatie te versterken; en
- voorkomen van de **versnippering van certificeringsregelingen** in de EU en de daarmee samenhangende beveiligingseisen en evaluatiecriteria in alle lidstaten en sectoren.

Het volgende gedeelte van de toelichting omvat een gedetailleerde motivering van het initiatief wat betreft de voorgestelde acties voor het Enisa en de cyberbeveiligingscertificering.

[8] Transparantie van de zekerheid inzake cyberbeveiliging houdt in dat de gebruikers worden voorzien van voldoende informatie over cyberbeveiligingseigenschappen, waardoor zij in staat zijn het beveiligingsniveau van elk ICT-product, -dienst of -proces objectief te bepalen.

Enisa

Het Enisa fungeert als expertisecentrum voor de verbetering van netwerk- en informatiebeveiliging in de Unie en voor de ondersteuning van de capaciteitsopbouw in de lidstaten.

Het Enisa is opgericht in 2004[9] om een bijdrage te leveren aan de algemene doelstelling van het waarborgen van een hoog niveau van netwerk- en informatiebeveiliging in de EU. In 2013 is in Verordening (EU) nr. 526/2013 het nieuwe mandaat voor het Agentschap vastgesteld voor een periode van zeven jaar, tot 2020. De kantoren van het Agentschap zijn gevestigd in Griekenland: de administratieve zetel bevindt zich in Heraklion (Kreta) en de kernactiviteiten in Athene.

Het Enisa is een klein agentschap met een klein budget en vergeleken met alle andere EU-agentschappen een klein personeelsbestand. Het heeft een tijdelijk mandaat.

Het Enisa ondersteunt de Europese instellingen, de lidstaten en het bedrijfsleven **bij het aanpakken van, reageren op en met name het voorkomen van problemen inzake netwerk- en informatiebeveiliging**. Daartoe wordt op vijf in de strategie van het Enisa[10] vastgestelde gebieden een reeks activiteiten ontplooid:

- deskundigheid: verstrekken van informatie en expertise inzake belangrijke kwesties op het gebied van netwerk- en informatiebeveiliging;
- beleid: ondersteunen van beleidsvorming en -uitvoering in de Unie;
- capaciteit: ondersteunen van capaciteitsopbouw in de gehele Unie (bijv. door middel van opleidingen, aanbevelingen, voorlichtingsactiviteiten);
- gemeenschap: bevorderen van de netwerk- en informatiebeveiligingsgemeenschap (bijv. door ondersteuning van de computercrisisteams (Computer Emergency Response Teams – CERT's) en coördinatie van pan-Europese cyberoefeningen);
- overleg tot stand brengen (bijv. overleg met de belanghebbenden en internationale betrekkingen).

In het kader van de onderhandelingen over de NIS-richtlijn hebben de EU-medewetgevers besloten om bij de uitvoering van deze richtlijn een belangrijke rol aan het Enisa toe te kennen. In het bijzonder verzorgt het Agentschap het secretariaat voor het CSIRT-netwerk (dat is opgericht ter bevordering van snelle en doeltreffende operationele samenwerking tussen de lidstaten inzake specifieke cyberbeveiligingsincidenten en van de uitwisseling van informatie over risico's) en ondersteunt het de samenwerkingsgroep bij de uitvoering van zijn taken. Daarnaast moet het Enisa op grond van de richtlijn de lidstaten en de Commissie bijstaan door expertise en advies te verstrekken en door de uitwisseling van beste praktijken te faciliteren.

Overeenkomstig de Enisa-verordening heeft de Commissie een evaluatie van het Agentschap verricht, waarbij een onafhankelijke studie en een openbare raadpleging zijn uitgevoerd. Bij

[9] Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (PB L 77 van 13.3.2004, blz. 1).

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

de evaluatie is een beoordeling gemaakt van de relevantie, de impact, de doeltreffendheid, de efficiëntie, de samenhang en de EU-meerwaarde van het Agentschap wat betreft de prestaties, de governance, de interne organisatiestructuur en de werkmethoden in de periode 2013-2016.

Bij de openbare raadpleging gaf het merendeel van de respondenten[11] (74 %) een positieve beoordeling. De meerderheid van de respondenten was bovendien van mening dat het Enisa zijn verschillende doelstellingen bereikt (ten minste 63 % voor elk van de doelstellingen). De diensten en producten van Enisa worden regelmatig (maandelijks of vaker) gebruikt door bijna de helft van de respondenten (46 %); daarbij worden deze op prijs gesteld omdat ze afkomstig zijn van een instantie op EU-niveau (83 %) en vanwege de kwaliteit (62 %).

Een grote meerderheid (88 %) van de respondenten was echter van mening dat de huidige, op EU-niveau beschikbare instrumenten en mechanismen onvoldoende of slechts gedeeltelijk adequaat zijn voor de aanpak van de huidige uitdagingen inzake cyberbeveiliging. Een grote meerderheid van de respondenten (98 %) gaf aan dat een EU-orgaan in deze behoeften zou moeten voorzoen, waarbij 99 % van de respondenten van mening was dat het Enisa daarvoor de juiste organisatie is. Daarnaast vond 67,5 % van de respondenten dat het Enisa een rol kan spelen bij de vaststelling van een geharmoniseerd kader voor de beveiligingscertificering van IT-producten en -diensten.

In de algehele evaluatie (gebaseerd op niet alleen de openbare raadpleging, maar ook op een aantal individuele vraaggesprekken, aanvullende doelgerichte enquêtes en workshops) werden de volgende conclusies getrokken:

- De doelstellingen van het Enisa zijn nog steeds relevant. In een klimaat van snelle technologische ontwikkelingen en veranderende dreigingen, en gezien de toenemende mondiale risico's op het gebied van cyberbeveiliging, is het duidelijk dat in de EU hoogwaardige technische expertise inzake kwesties betreffende cyberbeveiliging moeten worden bevorderd en versterkt. De capaciteit in de lidstaten moet worden opgebouwd, zodat dreigingen juist worden ingeschat en er adequaat op wordt gereageerd, en de belanghebbenden moeten over de grenzen van thematische gebieden en instellingen heen samenwerken.
- Hoewel het Agentschap slechts over een klein budget beschikt, heeft het in operationeel opzicht efficiënt van zijn middelen gebruikgemaakt en zijn taken uitgevoerd. Door de twee locaties zijn er echter ook extra administratieve kosten ontstaan.
- Wat betreft doeltreffendheid heeft het Enisa zijn doelstellingen gedeeltelijk bereikt. Het Agentschap heeft met succes bijgedragen tot het verbeteren van de netwerk- en informatiebeveiliging in Europa door capaciteitsopbouw in 28 lidstaten aan te bieden[12], te zorgen voor nauwere samenwerking tussen de lidstaten en de

[11] 90 belanghebbenden uit 19 lidstaten hebben op de raadpleging gereageerd (88 reacties en twee standpuntnota's), waaronder nationale autoriteiten uit 15 lidstaten en acht overkoepelende organisaties die een significant aantal Europese ondernemingen vertegenwoordigen.

[12] Aan de respondenten van de openbare raadpleging werd gevraagd wat zij als de belangrijkste prestaties van het Enisa in de periode 2013-2016 beschouwden. Respondenten uit alle groepen (in totaal 55, waarvan 13 van nationale overheidsinstanties, 20 uit de particuliere sector en 22 uit de categorie "overige") beschouwden het volgende als de belangrijkste prestaties van het Enisa: 1) de coördinatie van de Cyber Europe-oefeningen;; 2) het verlenen van ondersteuning aan de CERT's/CSIRT's door middel van opleidingen en workshops ter bevordering van de coördinatie en uitwisseling; 3) de publicaties van het Enisa (richtsnoeren en aanbevelingen, verslagen inzake het dreigingslandschap, strategieën inzake rapportage en crisisbeheersing enz.) die nuttig werden geacht voor het tot stand

belanghebbenden op het gebied van netwerk- en informatiebeveiliging, en te voorzien in expertise, gemeenschapsopbouw en ondersteuning van de ontwikkeling van beleid. Over het geheel genomen, heeft het Enisa zijn werkprogramma nauwkeurig uitgevoerd en gefungeerd als betrouwbare partner voor de betrokken belanghebbenden, en dat op een gebied waarvan slechts onlangs is erkend dat het van groot grensoverschrijdend belang is.

- Het Enisa is erin geslaagd enige resultaten te boeken op het omvangrijke gebied van de netwerk- en informatiebeveiliging, maar het is er niet volledig in geslaagd een sterke merknaam te vestigen en voldoende bekendheid te verwerven om te worden erkend als het expertisecentrum in Europa bij uitstek. Dat is het gevolg van het feit dat het Enisa een breed mandaat heeft, maar niet beschikt over voldoende middelen. Daarnaast heeft het Enisa als enige EU-agentschap een tijdelijk mandaat, waardoor het slechts in beperkte mate een langetermijnvisie kan ontwikkelen en de belanghebbenden op duurzame wijze kan ondersteunen. Hiermee wordt afgeweken van de NIS-richtlijn, waarin is bepaald dat aan het Enisa taken zonder einddatum worden toevertrouwd. Tot slot is uit de beoordeling gebleken dat deze beperkte doeltreffendheid gedeeltelijk te wijten is aan het feit dat meer gebruik wordt gemaakt van externe expertise dan van in-house expertise, en aan de moeilijkheden die worden ondervonden bij het aantrekken en behouden van gespecialiseerd personeel.
- Tot slot, maar daarom niet minder belangrijk, wordt in de evaluatie geconcludeerd dat de meerwaarde van het Enisa hoofdzakelijk voortvloeit uit het vermogen van het Agentschap om de samenwerking te versterken tussen in de eerste plaats de lidstaten, en met name met aanverwante gemeenschappen op het gebied van netwerk- en informatiebeveiliging (in he bijzonder tussen de CSIRT's). Op EU-niveau is er geen andere actor die een dergelijke breed bereik van belanghebbenden op het gebied van netwerk- en informatiebeveiliging ondersteunt. Het Enisa moet bij zijn activiteiten echter strenge prioriteiten stellen, waardoor zijn werkprogramma echter grotendeels wordt gestuurd door de behoeften van de lidstaten. Daardoor komt het niet afdoende tegemoet aan de behoeften van andere belanghebbenden, waaronder met name het bedrijfsleven. Daarnaast is het Agentschap erop gericht tegemoet te komen aan de behoeften van de belangrijkste belanghebbenden, waardoor het niet in staat is grotere impact tot stand te brengen. Zodoende varieert de meerwaarde die het Agentschap biedt naargelang van de uiteenlopende behoeften van de belanghebbenden, en van de mate waarin het Agentschap in staat was erop te reageren (bijv. grote tegenover kleine lidstaten, lidstaten tegenover het bedrijfsleven).

Samenvattend blijkt uit de raadpleging van de belanghebbenden en de evaluatie dat de middelen en het mandaat van het Enisa moeten worden aangepast, zodat het een adequate rol kan spelen bij de aanpak van huidige en toekomstige uitdagingen.

Gezien deze bevindingen wordt in het onderhavige voorstel het huidige mandaat van het Enisa herzien en wordt een hernieuwde reeks taken en functies vastgesteld, met als doel doeltreffende en efficiënte ondersteuning van de inspanningen van de lidstaten, de EU-instellingen en andere belanghebbenden met betrekking tot het waarborgen van een veilige cyberspace in de Europese Unie. Met het nieuwe, in dit voorstel opgenomen mandaat wordt

---

brengen en bijwerken van nationale beveiligingskaders alsmede als voor gebruik als referentie door beleidsmakers en professionals op het gebied van cyberbeveiliging; 4) bijstand bij bevordering van de bekendheid van de NIS-richtlijn; 5) inspanningen ter versterking van de bewustmaking inzake cyberbeveiliging door middel de maand van de cyberbeveiliging.

beoogd aan het Agentschap een sterkere en meer centrale rol toe te kennen, door onder meer de lidstaten te ondersteunen bij de uitvoering van de NIS-richtlijn, door specifieke dreigingen actiever aan te pakken (operationele capaciteit) en door een kenniscentrum te worden dat de lidstaten en de Commissie ondersteunt op het gebied van de certificering van cyberbeveiliging. Het voorstel voorziet in het volgende:

- Het Enisa zou een permanent mandaat krijgen en daardoor over een stabiele basis voor de toekomst beschikken. Het mandaat, de doelstellingen en de taken moeten net als tot dusver regelmatig worden geëvalueerd.
- In het voorgestelde mandaat wordt daarnaast verder verduidelijkt dat het ENISA het EU-agentschap voor cyberbeveiliging is en dat het dient als referentiepunt in het cyberbeveiligingsecosysteem van de UE, waarbij het nauw samenwerkt met alle andere relevante instanties binnen dat ecosysteem.
- De organisatie en het beheer van het Agentschap, die in het kader van de evaluatie een positieve beoordeling kregen, worden enigszins herzien, met name om ervoor te zorgen dat er bij de werkzaamheden van het Agentschap meer rekening wordt gehouden met de behoeften van de gemeenschap van belanghebbenden in bredere zin.
- De voorgestelde werkingssfeer van het mandaat wordt afgebakend, waarbij de gebieden worden versterkt waarop het Agentschap blijk heeft gegeven van een duidelijke meerwaarde en nieuwe gebieden worden toegevoegd waarop ondersteuning nodig is gezien de nieuwe beleidsprioriteiten en -instrumenten, met name de NIS-richtlijn, de herziening van de EU-cyberbeveiligingsstrategie, de op stapel staande blauwdruk voor de EU-cyberbeveiliging in verband met de samenwerking bij cybercrises alsmede de ICT-beveiligingscertificering:
    - **Ontwikkeling en uitvoering van EU-beleid:** Het Enisa zou worden belast proactief bij te dragen tot de ontwikkeling van beleid op het gebied van netwerk- en informatiebeveiliging alsmede tot andere beleidsinitiatieven in verschillende sectoren (bijv. energie, vervoer, financiën) waarvan cyberbeveiliging deel uitmaakt. Daartoe zou het een belangrijke adviserende rol spelen die het kan vervullen door middel van onafhankelijke adviezen en voorbereidende werkzaamheden voor de ontwikkeling en de actualisering van het beleid van beleid en wetgeving. Het Enisa zou tevens ondersteuning geven aan het beleid en de wetgeving van de EU op het gebied van elektronische communicatie en van elektronische identiteits- en vertrouwensdiensten, teneinde een hoger niveau van cyberbeveiliging te bevorderen. In de uitvoeringsfase, met name in de context van de NIS-samenwerkingsgroep, zou het Enisa de lidstaten bijstaan bij de totstandbrenging van een consistente aanpak van de uitvoering van de NIS-richtlijn over de grenzen heen en in alle sectoren, alsmede op andere relevante beleidsterreinen en in andere wetgeving. Teneinde de regelmatige evaluatie van het beleid en de wetgeving op het gebied van cyberbeveiliging te ondersteunen, zou het Enisa regelmatig verslag uitbrengen over de stand van uitvoering van het EU-wetgevingskader.
    - **Capaciteitsopbouw:** Het Enisa zou bijdragen tot de verbetering van de vermogens en expertise van de overheidsinstanties op EU- en lidstaatniveau, waaronder met betrekking tot de reactie op incidenten en het toezicht op regelgevingsmaatregelen in verband met cyberbeveiliging. Het Agentschap zou ook moeten bijdragen tot de oprichting van ISAC's (Information Sharing and Analysis Centres, centra voor informatie-uitwisseling en -analyse) in

verschillende sectoren door de verstrekking van beste praktijken en richtsnoeren betreffende beschikbare instrumenten en procedures, en door op passende wijze in te gaan op regelgevingskwesties in verband met het uitwisselen van informatie.

- **Kennis en informatie, voorlichting:** Het Enisa zou het informatiecentrum van de EU worden. Dat zou betrekking hebben op het bevorderen en uitwisselen van beste praktijken en initiatieven in de hele EU door middel van het samenbrengen van informatie over cyberbeveiliging afkomstig uit de EU- en nationale instellingen, agentschappen en organen. Verder zou het Agentschap advies, richtsnoeren en beste praktijken inzake de beveiliging van kritieke infrastructuurvoorzieningen ter beschikking stellen. Het Enisa zou bovendien na afloop van significante grensoverschrijdende cyberbeveiligingsincidenten verslagen opstellen met als doel richtsnoeren te verstrekken aan bedrijven en burgers in de hele EU. Tot dit werkgebied zou ook het regelmatig organiseren van regelmatige voorlichtingsactiviteiten in overleg met de autoriteiten van de lidstaten behoren.
- **Marktgerelateerde taken (normalisatie, certificering van cyberbeveiliging):** Het Enisa zou een aantal functies uitvoeren die specifiek zijn bedoeld voor het ondersteunen van de interne markt, en voorzien in een waarnemingspost cyberbeveiliging, door relevante trends op de cyberbeveiligingsmarkt te analyseren teneinde vraag en aanbod beter op elkaar af te stemmen, en door het ondersteunen van de ontwikkeling van EU-beleid op de gebieden ICT-normalisatie en certificering van ICT voor cyberbeveiliging. Met name ten aanzien van normalisatie, zou het de vaststelling en toepassing van normen inzake cyberbeveiliging bevorderen. Het Enisa zou ook de taken uitvoeren die zijn voorzien in het toekomstige kader voor de certificering (zie hieronder).
- **Onderzoek en innovatie:** Het Enisa zou door middel van zijn expertise een bijdrage leveren door advies te geven aan de autoriteiten op EU- en lidstaatniveau betreffende het stellen van prioriteiten voor onderzoek en ontwikkeling, onder meer in het kader van het contractuele publiek-private partnerschap voor cyberbeveiliging (cPPP). Het advies van het Enisa inzake onderzoek zou worden gebruikt voor het nieuwe Europees onderzoeks- en kenniscentrum voor cyberbeveiliging binnen het volgende meerjarig financieel kader. Het Enisa zou op verzoek van de Commissie ook worden betrokken bij de uitvoering van EU-financieringsprogramma's voor onderzoek en innovatie.
- **Operationele samenwerking en crisisbeheersing:** Dit werkgebied zou bijdragen tot de verbetering van de bestaande preventieve operationele vermogens, met name zouden de pan-Europese oefeningen inzake cyberbeveiliging (Cyber Europe) worden versterkt door deze jaarlijks uit te voeren, en tot een ondersteunende rol bij de operationele samenwerking als secretariaat van het CSIRT-netwerk (overeenkomstig de bepalingen van de NIS-richtlijn), onder meer door te waarborgen dat de IT-infrastructuur en de communicatiekanalen van het CSIRT-netwerk goed werken. In deze context zou een gestructureerde samenwerking met CERT-EU, het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) en andere relevante EU-organen vereist zijn. Bovendien zou door gestructureerde samenwerking met CERT-EU, waarbij beiden in fysieke zin dicht bij elkaar zijn gevestigd, een functie tot stand komen waarbij technische bijstand wordt geleverd in het geval

van significante incidenten en de analyse van incidenten wordt ondersteund. De lidstaten die hierom verzoeken, zouden bijstand krijgen bij het aanpakken van incidenten alsmede ondersteuning met betrekking tot de analyse van kwetsbaarheden, artefacten en incidenten ter versterking van hun eigen preventieve en responsvermogen.

- Het Enisa zou ook een rol spelen bij de **blauwdruk voor de EU-cyberbeveiliging** die als onderdeel van dit pakket wordt voorgesteld, waarbij de aanbeveling van de Commissie aan de lidstaten voor een gecoördineerde reactie op grootschalige grensoverschrijdende cyberbeveiligingsincidenten en -crises op EU-niveau wordt vastgesteld[13]. Het Enisa zou de samenwerking tussen de afzonderlijke lidstaten vergemakkelijken wat betreft de aanpak van noodmaatregelen door analyse en bundeling van nationale situatieverslagen, op basis van informatie die op vrijwillige basis door de lidstaten en andere entiteiten aan het Agentschap ter beschikking wordt gesteld.

- **Cyberbeveiligingscertificering van ICT-producten en -diensten**

Teneinde vertrouwen en beveiliging tot stand te brengen en te handhaven, moeten beveiligingskenmerken in een vroeg stadium van het technische ontwerp en de technische ontwikkeling rechtstreeks in ICT-producten en -diensten worden geïntegreerd (ingebouwde beveiliging). Bovendien moeten klanten en gebruikers in staat zijn om het niveau van zekerheid inzake de beveiliging vast te stellen van de producten en diensten die zij verwerven of aankopen.

Certificering, dat wil zeggen de formele evaluatie van producten, diensten en processen door een onafhankelijke en geaccrediteerde instantie met behulp van een gedefinieerde reeks criteria en de afgifte van een certificaat dat overeenstemming aangeeft, speelt een belangrijke rol bij het versterken van het vertrouwen in en de zekerheid van producten en diensten. Evaluaties van de beveiliging zijn weliswaar een zeer technische kwestie, maar certificering dient ertoe de kopers en gebruikers informeren en geruststellen over de beveiligingseigenschappen van de ICT-producten en -diensten die zij kopen en gebruiken.. Zoals hierboven vermeld, is dit met name van belang voor nieuwe systemen die intensief gebruik maken van digitale technologieën en die een hoog beveiligingsniveau vergen, zoals onderling communicerende en zelfrijdende auto's, elektronische gezondheidszorg en besturingssystemen voor industriële automatisatie (IACS)[14] of slimme netwerken.

Momenteel is de cyberbeveiligingscertificering van ICT-producten en -diensten in de EU tamelijk versnipperd. Er is een aantal internationale initiatieven, zoals de zogenoemde Gemeenschappelijke criteria (Common Criteria, CC) voor de evaluatie van de beveiliging van informatietechnologie (ISO 15408), een internationale norm voor de evaluatie van de beveiliging van computers. Deze norm is gebaseerd op toetsing door derde partijen en omvat

---

[13] De "blauwdruk" zal van toepassing zijn op cyberincidenten die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen of die gevolgen hebben voor twee of meer lidstaten die zo wijdverspreid zijn dat tijdige coördinatie en reactie op het politieke niveau van de Unie vereist zijn.

[14] DG JRC heeft een verslag uitgebracht waarin een voorstel wordt gedaan voor een initiële reeks gemeenschappelijke Europese eisen en brede richtsnoeren in verband met de cyberbeveiligingscertificering van IACS-componenten. Beschikbaar op: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

zeven Evaluation Assurance Levels (EAL's). De CC en de daarmee verwante gemeenschappelijke methodologie voor de evaluatie van de beveiliging informatietechnologie (CEM) vormen de technische basis voor een internationale overeenkomst, de Common Criteria Recognition Arrangement (CCRA) die waarborgt dat CC-certificaten door alle ondertekenaars van de CCRA worden erkend. In de huidige versie van de CCRA worden echter uitsluitend evaluaties tot EAL 2 wederzijds erkend. Bovendien hebben slechts 13 lidstaten de regeling ondertekend.

De certificerende instanties van twaalf lidstaten hebben een overeenkomst inzake wederzijdse erkenning gesloten betreffende in overeenstemming van de overeenkomst op basis van de gemeenschappelijke criteria afgegeven certificaten[15]. Daarnaast wordt een aantal ICT-certificeringsinitiatieven momenteel in de lidstaten toegepast of ingevoerd. Hoewel deze initiatieven belangrijk zijn, bestaat het risico dat de marktversnippering en interoperabiliteitsproblemen hierdoor toenemen. Als gevolg daarvan kan het voorkomen dat een bedrijf meerdere certificeringsprocedures moeten in verschillende lidstaten moet doorlopen indien het zijn product op meerdere markten wil aanbieden. Een voorbeeld: een fabrikant van slimme meters die zijn producten wil verkopen in drie lidstaten, bijvoorbeeld Duitsland, Frankrijk en het Verenigd Koninkrijk, moet momenteel aan drie verschillende certificeringsregelingen voldoen. Dat zijn de "Commercial Product Assurance (CPA)" in het Verenigd Koninkrijk, de "Certification de Sécurité de Premier Niveau" (CSPN) in Frankrijk, en een specifiek beschermingsprofiel op basis van de Common Criteria in Duitsland.

Deze situatie leidt tot hogere kosten en aanzienlijke administratieve lasten voor bedrijven die in verschillende lidstaten actief zijn. De kosten van certificering kunnen sterk uiteenlopen, naargelang van het betrokken product of de betrokken dienst, het beoogde EAL en/of andere factoren, maar in het algemeen worden bedrijven met aanzienlijke kosten geconfronteerd. Het certificaat van de British Standards Institution voor een "smart meter gateway" (hoogste test- en betrouwbaarheidsniveau dat niet alleen voor het product geldt maar ook voor de hele daarmee samenhangende infrastructuur) kost bijvoorbeeld meer dan 1 miljoen EUR. De kosten voor de certificering van slimme meters in het Verenigd Koninkrijk bedragen bijna 150 000 EUR. De kosten in Frankrijk zijn vergelijkbaar met die in het Verenigd Koninkrijk en bedragen 150 000 EUR of meer.

Belangrijke belanghebbenden uit de publieke en de particuliere sector hebben erkend dat bedrijven bij gebrek aan een EU-brede regeling voor cyberbeveiligingscertificering in veel gevallen in elke lidstaat moeten worden gecertificeerd, hetgeen leidt tot versnippering van de markt. Bij gebrek aan EU-wetgeving ter harmonisatie van ICT-producten en -diensten kunnen verschillen in de normen en praktijken inzake cyberbeveiligingscertificering in de lidstaten er met name toe leiden dat in de EU in de praktijk 28 verschillende beveiligingsmarkten ontstaan die elk eigen technische eisen, testmethoden en procedures inzake cyberbeveiligingscertificering hebben. Deze uiteenlopende benaderingen op nationaal niveau kunnen – indien op EU-niveau geen adequate actie wordt ondernomen – leiden tot een aanzienlijke terugval bij de totstandbrenging van de digitale eengemaakte markt en tot vertraging of belemmering van de daarmee samenhangende positieve effecten op de groei en de werkgelegenheid.

---

[15] De Groep van Hoge Ambtenaren voor de beveiliging van informatiesystemen (SOG-IS) omvat twaalf lidstaten en Noorwegen, en heeft enkele beschermingsprofielen ontwikkeld voor een beperkt aantal producten, zoals de digitale handtekening, de digitale tachograaf en chipkaarten. De deelnemers werken samen aan de coördinatie van de normalisatie van CC-beschermingsprofielen en de coördinatie van de ontwikkeling van beschermingsprofielen. De lidstaten vragen dikwijls om SOG-IS-certificering voor nationale openbare aanbestedingen.

Voortbouwend op de bovenstaande ontwikkelingen, wordt met de voorgestelde verordening een Europees kader voor cyberbeveiligingscertificering (het "**kader**") voor ICT-producten en -diensten tot stand gebracht en worden de essentiële functies en taken van het Enisa op het gebied van cyberbeveiligingscertificering gespecificeerd. Met het onderhavige voorstel wordt een algemeen kader van voorschriften vastgesteld die van toepassing zijn op Europese regelingen voor cyberbeveiligingscertificering. Het voorstel omvat geen rechtstreekse operationele certificeringsregelingen, maar het brengt een stelsel (kader) tot stand voor de vaststelling van specifieke certificeringsregelingen voor specifieke ICT-producten/-diensten (de "Europese regelingen voor cyberbeveiligingscertificering"). Europese regelingen voor cyberbeveiligingscertificering die in overeenstemming met het kader worden opgezet, zorgen ervoor dat volgens deze regelingen afgegeven certificaten in alle lidstaten geldig zijn en erkend worden en dat de huidige versnippering van de markt wordt aangepakt.

Het algemene doel van een Europese regeling voor cyberbeveiligingscertificering is bevestigen dat de overeenkomstig een dergelijke regeling gecertificeerde ICT-producten en -diensten voldoen aan gespecificeerde eisen inzake cyberbeveiliging. Daartoe behoort bijvoorbeeld het vermogen ervan om (opgeslagen, doorgegeven of anderszins bewerkte) gegevens te beschermen tegen accidentele of onbevoegde opslag, verwerking, toegang, openbaarmaking, vernietiging, accidenteel verlies of wijziging. EU-regelingen voor cyberbeveiligingscertificering zouden gebruikmaken van bestaande normen ten aanzien van de technische eisen en evaluatieprocedures waaraan de producten moeten voldoen en zouden dergelijke technische normen niet zelf ontwikkelen[16]. Een EU-brede certificering voor producten zoals chipkaarten, die momenteel worden getest aan de hand van internationale CC-normen in het kader van de multilaterale SOG-IS-regeling (hierboven reeds omschreven), zou bijvoorbeeld betekenen dat deze regeling in de hele EU geldig is.

In het voorstel wordt niet alleen een omschrijving gegeven van een specifieke reeks beveiligingsdoelstellingen waarmee bij de opzet van een specifieke Europese regeling voor cyberbeveiligingscertificering rekening moet worden gehouden, maar ook vastgesteld wat de minimale inhoud van dergelijke regelingen moet zijn. Dergelijke regelingen moeten onder meer een aantal specifieke elementen omvatten aan de hand waarvan het toepassingsgebied en het onderwerp van de cyberbeveiligingscertificering worden vastgesteld. Hiertoe behoren de identificatie van de categorieën producten en diensten die onder de regeling vallen, de gedetailleerde specificatie van de eisen inzake cyberbeveiliging (bijvoorbeeld door verwijzing naar de relevante normen of technische specificaties), de specifieke evaluatiecriteria en -methoden alsmede het zekerheidsniveau dat ermee wordt gewaarborgd (dat wil zeggen basis, substantieel of hoog).

Europese regelingen voor cyberbeveiligingscertificering zullen worden opgesteld door het Enisa, in nauwe samenwerking met de Europese Groep voor cyberbeveiligingscertificering (zie hieronder) die assistentie en deskundig advies verleent, en door middel van uitvoeringshandelingen door de Commissie worden vastgesteld. Wanneer wordt geconstateerd dat er behoefte is aan een regeling voor cyberbeveiligingscertificering, zal de Commissie het Enisa vragen een regeling op te zetten voor specifieke ICT-producten of -diensten. Het Enisa zal daarbij nauw samenwerken met de autoriteiten voor certificeringstoezicht die in de Groep zijn vertegenwoordigd. De lidstaten en de Groep kunnen de Commissie voorstellen dat zij het Enisa vraagt een bepaalde regeling op te zetten.

---

[16] In het geval van Europese normen wordt dit uitgevoerd door de Europese normalisatieorganisaties en door de Europese Commissie goedgekeurd en in het *Publicatieblad* gepubliceerd (zie Verordening nr. 1025/2012).

Certificering kan hoge kosten met zich meebrengen en daardoor tot hogere prijzen voor de klanten en consumenten leiden. De noodzaak van certificering kan ook aanzienlijk verschillen afhankelijk van de specifieke context waarin de producten en diensten worden gebruikt en van het hoge tempo waarin technologische veranderingen plaatsvinden. De toepassing van Europese regelingen voor cyberbeveiligingscertificering moet daarom vrijwillig blijven, tenzij anders is bepaald in EU-wetgeving tot vaststelling van beveiligingsvereisten van ICT-producten en -diensten.

Teneinde harmonisatie te waarborgen en versnippering te voorkomen, zullen nationale regelingen of procedures inzake cyberbeveiligingscertificering voor de ICT-producten en -diensten die onder een Europese regeling voor cyberbeveiligingscertificering vallen, niet meer van toepassing zijn met ingang van de datum die is bepaald in de uitvoeringshandeling waarbij de regeling wordt vastgesteld. Verder moeten de lidstaten geen nieuwe nationale regelingen voor cyberbeveiligingscertificering invoeren voor de ICT-producten en -diensten die onder een bestaande Europese regeling voor cyberbeveiligingscertificering vallen.

Zodra een Europese regeling voor cyberbeveiligingscertificering is vastgesteld, kunnen fabrikanten van ICT-producten of aanbieders van ICT-diensten bij een conformiteitsbeoordelingsinstantie van hun keuze een aanvraag indienen voor de certificering van hun producten of diensten. Conformiteitsbeoordelingsinstanties moeten door een accreditatie-instantie worden geaccrediteerd indien zij aan bepaalde specifieke vereisten voldoen. De accreditatie zal worden afgegeven voor een maximumperiode van vijf jaar en kan onder dezelfde voorwaarden worden verlengd, mits de conformiteitsbeoordelingsinstantie aan de vereisten voldoet. Accreditatie-instanties zullen de accreditatie van een conformiteitsbeoordelingsinstantie intrekken wanneer niet dan wel niet meer aan de voorwaarden voor de accreditatie wordt voldaan of wanneer door een conformiteitsbeoordelingsinstantie ondernomen acties indruisen tegen deze verordening.

In het voorstel is voorzien dat de taken inzake monitoring, toezicht en handhaving worden uitgevoerd door de lidstaten. De lidstaten moeten voorzien in één autoriteit voor certificeringstoezicht. Deze autoriteit zal erop toezien dat de conformiteitsbeoordelingsinstanties alsmede de door op hun grondgebied gevestigde conformiteitsbeoordelingsinstanties afgegeven certificaten in overeenstemming zijn met de vereisten van deze verordening en de desbetreffende Europese regelingen voor cyberbeveiligingscertificering. De nationale autoriteiten voor certificeringstoezicht zullen bevoegd zijn voor de behandeling van klachten van natuurlijke personen of rechtspersonen over certificaten die zijn afgegeven door op hun grondgebied gevestigde conformiteitsbeoordelingsinstanties. Zij zullen naar behoren onderzoek doen naar het onderwerp van de klacht en de klager binnen een redelijke termijn inlichten over de voortgang en het resultaat van dat onderzoek. Verder zullen zij samenwerken met andere autoriteiten voor certificeringstoezicht of andere overheidsinstanties, bijvoorbeeld door uitwisseling van informatie over mogelijke niet-naleving door ICT-producten en -diensten van de vereisten van deze verordening of van de specifieke Europese regelingen voor cyberbeveiligingscertificering.

Tot slot voorziet het voorstel in de oprichting van de Europese Groep voor cyberbeveiligingscertificering ("de Groep") die is samengesteld uit de nationale autoriteiten voor certificeringstoezicht van alle lidstaten. De voornaamste taak van de Groep is advies geven aan de Commissie over kwesties betreffende beleid inzake cyberbeveiligingscertificering en samenwerken met het Enisa in verband met de ontwikkeling van ontwerpen van Europese regelingen voor cyberbeveiligingscertificering. Het Enisa zal de Commissie bijstaan door te voorzien in het secretariaat voor de Groep en het zal zorgen voor een bijgewerkt openbaar overzicht van de overeenkomstig het Europees kader voor

cyberbeveiligingscertificering goedgekeurde regelingen. Het Enisa zal tevens overleggen met de normalisatie-organisaties om te waarborgen dat de in goedgekeurde regelingen toegepaste normen passend zijn en om gebieden vast te stellen waarvoor cyberbeveiligingsnormen nodig zijn.

Het Europees kader voor cyberbeveiligingscertificering ("het kader") zal de burgers en bedrijven meerder voordelen bieden. Meer bepaald:

- Dankzij de totstandbrenging van EU-brede regelingen voor cyberbeveiligingscertificering voor specifieke producten of diensten zullen bedrijven beschikken over een "one-stop-shop" voor cyberbeveiligingscertificering in de EU. Dergelijke bedrijven hoeven hun product slechts één maal te laten certificeren, waarbij zij een certificaat verkrijgen dat in alle lidstaten geldig is. Zij zullen niet verplicht zijn om hun producten opnieuw te laten certificeren door verschillende nationale certificeringsinstanties. Dit zal leiden tot een aanzienlijke vermindering van de kosten voor bedrijven, grensoverschrijdende activiteiten bevorderen en op lange termijn de versnippering van de interne markt voor de betrokken producten terugdringen en voorkomen.
- Het kader zorgt ervoor dat Europese regelingen voor cyberbeveiligingscertificering voorrang hebben op nationale regelingen: deze regel houdt in dat een Europese regeling voor cyberbeveiligingscertificering na vaststelling voorgaat op alle bestaande parallelle nationale regelingen voor dezelfde ICT-producten of -diensten op een gegeven zekerheidsniveau. Dit zorgt voor meer duidelijkheid doordat de verspreiding van overlappend en eventueel tegenstrijdige nationale regelingen voor cyberbeveiligingscertificering wordt tegengegaan.
- Het voorstel dient als ondersteuning van en aanvulling op de uitvoering van de NIS-richtlijn doordat de aan de richtlijn onderworpen ondernemingen de beschikking krijgen over een zeer nuttig instrument voor het aantonen van de naleving van de NIS-vereisten in de hele Unie. Door de ontwikkeling van nieuwe regelingen voor cyberbeveiligingscertificering zullen de Commissie en het Enisa in het bijzonder aandacht besteden aan de noodzaak ervoor te zorgen dat de NIS-vereisten worden geïntegreerd in de regelingen voor cyberbeveiligingscertificering.
- Het voorstel ondersteunt en vergemakkelijkt de ontwikkeling van Europees beleid inzake cyberbeveiliging door harmonisatie van de voorwaarden en materiële vereisten voor de cyberbeveiligingscertificering van ICT-producten en -diensten in de EU. Europese regelingen voor cyberbeveiligingscertificering zullen verwijzen naar gemeenschappelijke normen of criteria betreffende evaluatie- en testmethoden. Hierdoor wordt in aanzienlijke mate, zij het indirect, bijgedragen tot de toepassing van gemeenschappelijke beveiligingsoplossingen in de EU, waardoor tevens belemmeringen voor de interne markt worden weggenomen.
- Het kader is zodanig ontworpen dat de nodige flexibiliteit voor regelingen voor cyberbeveiligingscertificering is gewaarborgd. Afhankelijk van de specifieke behoeften inzake cyberbeveiliging, kan een product of dienst worden gecertificeerd voor hogere of lager beveiligingsniveaus. Bij het opzetten Europese regelingen voor cyberbeveiligingscertificering zal met deze flexibiliteit rekening worden gehouden; de regelingen zullen dan ook verschillende zekerheidsniveaus bieden (dat wil zeggen basis, substantieel of hoog), zodat deze voor verschillende doeleinden en in een verschillende context kunnen worden gebruikt.

- Alle bovengenoemde elementen zorgen ervoor dat cyberbeveiligingscertificering aantrekkelijker wordt voor ondernemingen als een doeltreffend middel om het niveau van cyberbeveiligingszekerheid van ICT-producten of -diensten aan te geven. Naarmate cyberbeveiligingscertificering goedkoper, doeltreffender en commercieel aantrekkelijker wordt, zullen ondernemingen meer worden geprikkeld om hun producten wat betreft risico's op het gebied van cyberbeveiliging te laten certificeren, waardoor wordt bijgedragen tot de verspreiding van beter cyberbeveiligingspraktijken bij het ontwerp van ICT-producten en -diensten (ingebouwde cyberbeveiliging).

- **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

In de NIS-richtlijn is bepaald dat aanbieders in voor onze economie en samenleving essentiële sectoren, zoals energie, vervoer, water, het bankwezen, financiëlemarktinfrastructuren, gezondheidszorg en digitale infrastructuur, alsmede digitaledienstverleners (dat wil zeggen zoekmachines, cloudcomputingdiensten en onlinemarktplaatsen) maatregelen moeten nemen om beveiligingsrisico's op passende wijze te beheren. De nieuwe voorschriften in dit voorstel vormen een aanvulling op en zorgen voor samenhang met de bepalingen van de NIS-richtlijn teneinde verder bij te dragen tot de cyberweerbaarheid van de EU door middel van versterkte vermogens, samenwerking, risicobeheer en cyberbewustzijn.

Daarnaast vormen de voorschriften inzake cyberbeveiligingscertificering een essentieel instrument voor ondernemingen die onder de NIS-richtlijn vallen, aangezien zij in staat zullen zijn hun ICT-producten en -diensten te laten certificeren met betrekking tot cyberbeveiligingsrisico's, op basis van regelingen voor cyberbeveiligingscertificering die in de hele EU geldig zijn en worden erkend. Tevens zullen de voorschriften een aanvulling zijn op de beveiligingsvereisten die zijn vastgesteld in de eIDAS-verordening[17] en de richtlijn inzake radioapparatuur[18].

- **Samenhang met andere beleidsterreinen van de Unie**

Verordening (EU) 2016/679 (de algemene verordening gegevensbescherming[19] omvat bepalingen betreffende het instellen van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens met als doel het aantonen van de naleving van deze verordening met betrekking tot verwerkingen door verwerkingsverantwoordelijken en verwerkers. De onderhavige verordening doet geen afbreuk aan de certificering van gegevensverwerkingen overeenkomstig de algemene verordening gegevensbescherming, ook niet als dergelijke verwerkingen zijn geïntegreerd in producten en diensten.

---

17 Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

18 Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG.

19 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

In de voorgestelde verordening is de verenigbaarheid met Verordening nr. 765/2008 inzake de eisen inzake accreditatie en markttoezicht[20] gewaarborgd doordat wordt verwezen naar de voorschriften van dat kader betreffende nationale accreditatie-instanties en conformiteitsbeoordelingsinstanties. Met betrekking tot de toezichthoudende autoriteiten, is in de voorgestelde verordening bepaald dat de lidstaten nationale autoriteiten voor certificeringstoezicht moeten aanwijzen die verantwoordelijk zijn voor het toezicht op alsmede de monitoring en de handhaving van de voorschriften. Zoals bepaald in Verordening (EG) nr. 765/2008 zullen deze organen gescheiden blijven van de conformiteitsbeoordelingsinstanties.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

- **Rechtsgrondslag**

De rechtsgrondslag voor maatregelen van de EU is artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU) dat betrekking heeft op de aanpassing van de wetgevingen van de lidstaten om doeleinden van artikel 26 VWEU te verwezenlijken, namelijk de goede werking van de interne markt.

De rechtsgrondslag betreffende de interne markt voor het oprichten van het Enisa is bevestigd door het Hof van Justitie (in zaak C-217/04 *Verenigd Koninkrijk/Europees Parlement en Raad*) en nogmaals bevestigd bij de verordening van 2013 waarin het huidige mandaat van het Agentschap is vastgesteld. Daarnaast zouden activiteiten die bijdragen tot de doelstellingen om de samenwerking en coördinatie tussen de lidstaten te versterken en om vermogens op EU-niveau toe te voegen ter aanvulling van het optreden van de lidstaten onder de categorie "operationele samenwerking" vallen. Dit komt specifiek aan bod in de NIS-richtlijn (waarvan artikel 114 VWEU de rechtsgrondslag is) als doelstelling in de context van het CSIRT-netwerk: "Het Enisa zorgt voor het secretariaat en voor een actieve ondersteuning van de samenwerking tussen de CSIRT's" (artikel 12, lid 2). Met name omvat artikel 12, lid 3, onder f), een nadere omschrijving van de identificatie van andere vormen van operationele samenwerking als taak van het CSIRT-netwerk, waaronder met betrekking tot: i) risico- en incidentcategorieën, ii) vroegtijdige waarschuwingen, iii) wederzijdse bijstand, en iv) coördinatiebeginselen en -regelingen voor gevallen waarin de lidstaten reageren op grensoverschrijdende risico's en -incidenten.

- De huidige versnippering van de certificeringsregelingen voor ICT-producten en -diensten vloeit mede voort uit het gebrek aan een gemeenschappelijk wettelijk bindend en doeltreffend kader dat van toepassing is op de lidstaten. Dit belemmert de totstandkoming van een interne markt voor ICT-producten en -diensten alsmede de concurrentiekracht van de Europese industrie in deze sector. Het onderhavige voorstel streeft ernaar de bestaande versnippering en de daarmee samenhangende obstakels voor de interne markt aan te pakken door te voorzien in een gemeenschappelijk kader voor de totstandbrenging van regelingen voor cyberbeveiligingscertificering die in de hele EU geldig zijn.

[20] Verordening (EG) nr. 765/2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93.

Subsidiariteit (bij niet-exclusieve bevoegdheid)

Het subsidiariteitsbeginsel vereist dat de noodzaak en de toegevoegde waarde van de EU-maatregelen worden beoordeeld. De naleving van het subsidiariteitsbeginsel op dit gebied kwam al aan bod bij de vaststelling van de huidige Enisa-verordening[21].

Cyberbeveiliging is een kwestie van gemeenschappelijk belang van de Unie. De onderlinge afhankelijkheid van netwerk- en informatiesystemen is van dien aard dat afzonderlijke actoren (publiek en privaat, met inbegrip van burgers) zeer vaak niet in staat zijn geïsoleerd in te gaan op de dreigingen van cyberincidenten of de risico's en mogelijke gevolgen daarvan te beheersen. Enerzijds zorgt de onderlinge afhankelijkheid van de lidstaten, waaronder met betrekking tot de exploitatie van kritieke infrastructuurvoorzieningen (energie, vervoer, water, om er maar een paar te noemen) ervoor dat overheidsinterventie op Europees niveau niet alleen nuttig, maar ook noodzakelijk is. Anderzijds kan het optreden van de EU een positief "spillover"-effect uitgaan door het uitwisselen van goede praktijken in alle lidstaten, hetgeen verbeterde cyberbeveiliging van de Unie tot gevolg kan hebben.

Samenvattend kan in de huidige context en met het oog op toekomstscenario's worden gesteld dat voor het **versterken van de gezamenlijke cyberweerbaarheid** van de Unie **afzonderlijke acties door de EU-lidstaten en een versnipperde aanpak van de cyberbeveiliging** niet afdoende zullen zijn.

Maatregelen van de EU worden tevens noodzakelijk geacht om de versnippering van de huidige regelingen voor cyberbeveiligingscertificering aan te pakken. Dergelijke maatregelen zouden fabrikanten in staat stellen om volledig te profiteren van de interne markt, waarbij aanzienlijk kan worden bespaard op de test- en herontwerpkosten. Hoewel dankzij de overeenkomst inzake wederzijdse erkenning van de Groep van Hoge Ambtenaren voor de beveiliging van informatiesystemen (SOG-IS) bijvoorbeeld belangrijke resultaten in dit verband zijn geboekt, zorgen de aanzienlijke beperkingen van de overeenkomst ervoor dat deze minder geschikt is om te voorzien in duurzame langetermijnoplossingen met het oog op het verwezenlijk van het volledige potentieel van de interne markt.

De toegevoegde waarde van actie op EU-niveau, met name ter versterking van de samenwerking tussen de lidstaten, maar ook tussen de netwerk- en informatiebeveiligingsgemeenschappen, is erkend in de conclusies van de Raad van 2016[22] en blijkt duidelijk uit de evaluatie van het Enisa.

- **Evenredigheid**

De voorgestelde maatregelen gaan niet verder dan strikt noodzakelijk is om de beoogde beleidsdoelstellingen te verwezenlijken. Evenmin vormt de werkingssfeer van het optreden van de EU een belemmering voor enige verdere nationale acties op het gebied van nationale beveiligingskwesties. Maatregelen door de EU zijn derhalve gerechtvaardigd om redenen van subsidiariteit en evenredigheid.

---

21 Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad van 21 mei 2013 inzake het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en tot intrekking van Verordening (EG) nr. 460/2004.

22 Conclusies van de Raad over het versterken van het Europese cyberbeveiligingssysteem en het bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche - 15 november 2016.

- **Keuze van het instrument**

Bij het onderhavige voorstel wordt Verordening (EU) nr. 526/2013 herzien, waarin het huidige mandaat en de huidige taken van het Enisa zijn vastgesteld. Gezien de belangrijke rol die het Enisa speelt bij het opzetten en beheren van een EU-kader voor cyberbeveiligingscertificering, vindt de vaststelling van het nieuwe mandaat van het Enisa en van het genoemde kader het beste plaats door middel van één rechtsinstrument, namelijk een verordening.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

Evaluatie van bestaande wetgeving en controle van de resultaatgerichtheid ervan

Overeenkomstige de evaluatie-routekaart[23] heeft de Commissie een beoordeling gemaakt van de **relevantie, de impact, de doeltreffendheid, de efficiëntie, de samenhang en de toegevoegde waarde** van het Agentschap wat betreft de prestaties, de governance, de interne organisatiestructuur en de werkmethoden in de periode 2013-2016. De voornaamste bevindingen kunnen als volgt worden samengevat (meer informatie is beschikbaar in het desbetreffende werkdocument van de diensten van de Commissie dat de effectbeoordeling begeleidt).

- **Relevantie:** Binnen een context van technologische ontwikkelingen en veranderende dreigingen, rekening houdend met de significante behoefte aan versterkte cyberbeveiliging in de EU, zijn de doelstellingen van het Enisa relevant gebleken. De lidstaten en EU-organen vertrouwen op de aanzienlijke expertise die het Enisa heeft op het gebied van cyberbeveiliging. De capaciteit in de lidstaten moet worden opgebouwd, zodat dreigingen beter worden ingeschat en er adequaat op wordt gereageerd, en de belanghebbenden moeten over de grenzen van thematische gebieden en instellingen heen samenwerken. Cyberbeveiliging blijft een essentiële politieke prioriteit van de EU en van het Enisa wordt verwacht dat het hierop ingaat; de opzet van het Enisa als EU-agentschap met een tijdelijk mandaat zorgt er echter voor dat: i) langetermijnplanning en duurzame ondersteuning van de lidstaten en EU-instellingen niet mogelijk zijn; ii) er een juridisch vacuüm kan ontstaan, aangezien de bepalingen van de NIS-richtlijn waarbij de taken van het Enisa zijn vastgesteld, van permanente aard zijn[24]; iii) er geen samenhang is met een visie waarin het Enisa wordt gekoppeld aan een versterkt EU-cyberbeveiligingsecosysteem.
- **Doeltreffendheid**: Algemeen gezien, heeft het Enisa zijn doelstellingen verwezenlijkt en zijn taken uitgevoerd. Het heeft bijdragen tot versterkte netwerk- en informatiebeveiliging in Europa door middel van zij voornaamste activiteiten (capaciteitsopbouw, het verstrekken van expertise, gemeenschapsopbouw en ondersteuning ten behoeve van beleid). Op elk van deze gebieden zijn echter verbeteringen mogelijk. In de evaluatie wordt geconcludeerd dat het Enisa op doeltreffende wijze sterke en betrouwbare betrekkingen met een aantal belanghebbenden tot stand heeft gebracht, met name met de lidstaten en de CSIRT-gemeenschap. Acties op het gebied van capaciteitsopbouw werden als doeltreffend aangemerkt, met name met betrekking tot lidstaten die over minder middelen

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

[24] Zie de artikelen 7, 9, 11, 12 en 19 van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn).

beschikken. Het stimuleren van brede samenwerking wordt beschouwd als een van de hoogtepunten: een groot aantal belanghebbenden was het erover eens dat het Enisa een positieve rol speelt bij het samenbrengen van mensen. Het Enisa had echter moeite zijn stempel te drukken op het uitgestrekte gebied van de netwerk- en informatiebeveiliging. Dit was mede te wijten aan het feit dat het in verhouding tot het zeer ruime mandaat slechts over redelijk beperkte personele en financiële middelen beschikte. Uit de evaluatie is ook gebleken dat het Enisa de doelstelling van het verstrekken van expertise slechts gedeeltelijk heeft verwezenlijkt vanwege problemen bij de aanwerving van deskundigen (zie ook hieronder in het gedeelte over efficiëntie).

- **Efficiëntie**: Hoewel het Agentschap over een budget beschikt dat tot de laagste behoort vergeleken met andere EU-agentschappen, is het erin geslaagd bij te dragen tot de beoogde doelstellingen door algeheel efficiënt gebruik van de beschikbare middelen. Uit de evaluatie is gebleken dat de processen over het algemeen efficiënt waren en dat de duidelijke afbakening van de verantwoordelijkheden binnen de organisatie heeft geleid tot degelijke uitvoering van de werkzaamheden. Een van de belangrijkste uitdagingen waarmee het Enisa wordt geconfronteerd, is de moeite die wordt ondervonden bij het aanwerven en vasthouden van hooggekwalificeerde deskundigen. Uit de bevindingen blijkt dat dit te wijten is aan een combinatie van factoren, waaronder de in de overheidssector algemeen voorkomende moeilijkheden wat betreft het concurreren met de particuliere sector bij het inhuren van uiterst gespecialiseerde deskundigen, het soort arbeidsovereenkomst (tijdelijk) dat het Agentschap in de meeste gevallen kon aanbieden en het de enigszins lage mate van aantrekkelijkheid van de locatie waar het Enisa is gevestigd, bijvoorbeeld in verband met problemen die echtgenoten ondervinden bij het vinden van werk. De twee locaties, in Athene en Heraklion, vereisten extra inspanningen wat betreft de coördinatie en zorgden voor extra kosten; doordat de kernactiviteiten in 2013 naar Athene zijn verplaatst, werd de operationele efficiëntie van het Agentschap verbeterd.
- **Samenhang**: In het algemeen was de samenhang van de activiteiten van het Enisa met de beleidsmaatregelen en activiteiten van de betrokken belanghebbenden op nationaal en EU-niveau, maar er is behoefte aan een meer gecoördineerde aanpak van cyberbeveiliging op EU-niveau. Het potentieel wat betreft de samenwerking tussen het Enisa en andere EU-organen is niet volledig benut. Door de ontwikkeling van het juridische en beleidskader van de EU is de samenhang van het mandaat momenteel afgenomen.
- **Toegevoegde waarde voor de EU**: De toegevoegde waarde van het Enisa is voornamelijk dat het de samenwerking kan bevorderen, met name tussen de lidstaten, maar ook met verwante netwerk- en informatiebeveiligingsgemeenschappen. Op EU-niveau is er geen andere actor die de samenwerking van een dergelijke variatie aan belanghebbenden op het gebied van netwerk- en informatiebeveiliging ondersteunt. De toegevoegde waarde die het Agentschap biedt, varieerde naargelang van de uiteenlopende behoeften van de betrokken belanghebbenden (bijv. grote ten opzichte van kleine lidstaten, lidstaten ten opzichte van het bedrijfsleven) en van het feit dat het Agentschap op basis van het werkprogramma prioriteit aan bepaalde activiteiten moest geven. Uit de evaluatie is gebleken dat een eventuele stopzetting van het Enisa een gemiste kans voor alle lidstaten zou zijn. Het zou dan niet mogelijk zijn dezelfde mate van gemeenschapsopbouw en samenwerking tussen alle lidstaten op het gebied van cyberbeveiliging te waarborgen. Zonder een meer gecentraliseerd EU-

agentschap, zou er meer versnippering plaatsvinden en zou de lacunes die het Enisa achterlaat, worden gevuld door middel van bilaterale of regionale samenwerking.

Specifiek rekening houdend met betrekking tot de vroegere prestaties en de toekomst van het Enisa, komen uit de raadpleging van 2017 de volgens belangrijkste tendensen naar voren[25]:

- De algehele prestaties van het Enisa tijdens de periode 2013-2016 werden door de meerderheid van de respondenten (74 %) positief beoordeeld. De meerderheid van de respondenten was bovendien van mening dat het Enisa zijn verschillende doelstellingen bereikt (ten minste 63 % voor elk van de doelstellingen). De diensten en producten van Enisa worden regelmatig (maandelijks of vaker) gebruikt door bijna de helft van de respondenten (46 %); daarbij worden deze op prijs gesteld omdat ze afkomstig zijn van een instantie op EU-niveau (83 %) en vanwege de kwaliteit (62 %).
- De respondenten wezen op een aantal lacunes en uitdagingen met betrekking tot de toekomst van de cyberbeveiliging in de EU, waarbij de volgende vijf bovenaan de lijst van 16 stonden: samenwerking tussen de lidstaten, capaciteit om grootschalige cyberaanvallen te voorkomen, op te sporen en op te lossen, samenwerking tussen de lidstaten wat betreft kwesties op het gebied van cyberbeveiliging, samenwerking en uitwisseling van informatie tussen de verschillende belanghebbenden, waaronder publiek-private samenwerking en de bescherming van kritieke infrastructuur tegen cyberaanvallen.
- Een grote meerderheid (88 %) van de respondenten was van mening dat de huidige, op EU-niveau beschikbare instrumenten en mechanismen onvoldoende of slechts gedeeltelijk adequaat zijn voor de aanpak de bovengenoemde punten. Een grote meerderheid van de respondenten (98 %) gaf aan dat een EU-orgaan in deze behoeften zou moeten voorzoen, waarbij 99 % van mening was dat het Enisa daarvoor de juiste organisatie is.

Raadpleging van belanghebbenden

- De Commissie heeft van 12 april tot 5 juli 2016 een openbare raadpleging betreffende de herziening van het Enisa georganiseerd en daarop 421 antwoorden ontvangen[26]. Daaruit blijkt dat 67,5 % van de respondenten vond dat het Enisa een rol kan spelen bij de vaststelling van een geharmoniseerd kader voor de beveiligingscertificering van IT-producten en -diensten.

---

25 90 belanghebbenden uit 19 lidstaten hebben op de raadpleging gereageerd (88 reacties en twee standpuntnota's), waarvan nationale autoriteiten uit 15 lidstaten, waaronder Frankrijk, Italië, Ierland en Griekenland, en acht overkoepelende organisaties die een significant aantal Europese organisaties vertegenwoordigen, bijvoorbeeld de Federatie van banken in de Europese Unie, Digital Europe (dat de sector digitale technologie in Europa vertegenwoordigt), en de European Telecommunications Network Operators' Association (ETNO). De openbare raadpleging betreffende het Enisa werd aangevuld door verschillende andere bronnen, waaronder i) diepgaande gesprekken met ongeveer 50 belangrijke spelers die tot de cyberbeveiligingsgemeenschap behoren, ii) een onderzoek betreffende het CSIRT-netwerk en iii) een onderzoek betreffende de raad van bestuur, het dagelijks bestuur en de permanent groep van belanghebbenden van het Enisa.

26 162 bijdragen van burgers, 33 van het maatschappelijk middenveld en consumentenorganisaties; 186 uit het bedrijfsleven en 40 van overheden, waaronder de bevoegde autoriteiten die de e-privacyrichtlijn handhaven.

Uit de resultaten van de raadpleging van 2016 over het cyberbeveiliging-cPPP[27] betreffende certificering bleek dat:

- 50,4 % (dat wil zeggen 121 van de 240) respondenten wist niet of nationale certificeringsregelingen in alle EU-lidstaten wederzijds worden erkend. 25.8 % (62 van de 240) gaf '"nee" als antwoord en 23,8 % (57 van de 240) "ja".
- 37,9 % van de respondenten (91 van de 240) was van mening dat de bestaande certificeringsregelingen niet tegemoetkomen aan de behoeften van het bedrijfsleven in Europa. 17,5 % (42 van de 240) van de respondenten – voornamelijk op de Europese markt actieve multinationals – was echter van mening dat wel in die behoeften wordt voorzien.
- 49,6 % (119 van de 240) respondenten gaf aan dat het niet eenvoudig is om de gelijkwaardigheid van normen, certificeringsregelingen en labels aan te tonen. 37,9 % (91 van de 240) gaf '"weet ik niet" als antwoord en slechts 12,5 % (30 van de 240) "ja".

Bijeenbrengen en gebruik van expertise

De Commissie heeft gebruikgemaakt van het volgende advies van externe deskundigen:

- studie over de evaluatie van het Enisa (Ramboll/Carsa 2017; SMART nr. 2016/0077);
- studie over de beveiligingscertificering en -labelling van ICT – verzamelen van bewijsmateriaal en effectbeoordeling (PriceWaterhouseCoopers 2017; SMART nr. 2016/0029).

Effectbeoordeling

- In het effectbeoordelingsverslag inzake dit initiatief is geconstateerd dat de volgende hoofdproblemen moeten worden aangepakt:
- versnippering van het beleid en de aanpak betreffende cyberbeveiliging in de lidstaten;
- versnippering van de middelen en benaderingen betreffende cyberbeveiliging binnen de EU-instellingen, -agentschappen en -organen; en
- onvoldoende bewustzijn en informatievoorziening voor burgers en bedrijven, gekoppeld met de toename van verschillende nationale en sectorale certificeringsregelingen.

In het verslag worden de volgende opties met betrekking tot het mandaat van het Enisa beoordeeld:

- handhaving van de huidige toestand, dus een verlening van het mandaat dat nog steeds tijdelijk blijft (basisoptie);
- verstrijken van het huidige mandaat van het Enisa zonder dat het wordt verlengd, en dientengevolge stopzetting van het Enisa (geen interventie);

[27] 240 belanghebbenden uit nationale overheden, grote ondernemingen, het mkb, micro-ondernemingen en onderzoeksinstellingen reageerden op het gedeelte over certificering.

- een "hervormd Enisa"; en
- een EU-cyberbeveiligingsagentschap met volledige operationele vermogens.

In het verslag worden de volgende opties met betrekking tot cyberbeveiligingscertificering beoordeeld:

- geen interventie (basisoptie);
- niet-wetgevende maatregelen ("soft law");
- een EU-wetgevingshandeling om een verplicht stelsel voor alle lidstaten tot stand te brengen op basis van het SOG-IS-stelsel; en
- een algemeen EU-kader voor ICT-cyberbeveiligingscertificering.

Op basis van de analyse is de conclusie getrokken dat een "hervormd Enisa" in combinatie met een algemeen EU-kader voor ICT-cyberbeveiligingscertificering de voorkeursoptie is.

De voorkeursoptie wordt beschouwd als meest doeltreffende manier met het oog op het bereiken van de vastgestelde doelstellingen van het versterken van de vermogens inzake cyberbeveiliging, paraatheid, samenwerking, bewustzijn, transparantie en het vermijden van marktversnippering. Deze optie heeft tevens de voorkeur wat betreft de samenhang met de beleidsprioriteiten van de EU-strategie inzake cyberbeveiliging en aanverwant beleid (bijv. de NIS-richtlijn), en de strategie voor de digitale eengemaakte markt. Bovendien is uit de raadpleging gebleken dat de meerderheid van de belanghebbenden achter de voorkeursoptie staat. Daarnaast is uit de in het kader van de effectbeoordeling uitgevoerde analyse gebleken dat door middel van de voorkeursoptie de doelstellingen kunnen worden bereikt met een redelijk gebruik van middelen.

De Raad voor regelgevingstoetsing van de Commissie heeft op 24 juli aanvankelijk een negatief advies uitgebracht, waarna een nieuwe versie werd ingediend waarover op 25 augustus 2017 een positief advies werd uitgebracht. De gewijzigde effectbeoordeling bevatte aanvullende ondersteunend bewijsmateriaal, de definitieve conclusies van de evaluatie van het Enisa en aanvullende uitleg over de beleidsopties en de impact daarvan. In bijlage 1 bij het definitieve effectbeoordelingsverslag wordt samengevat op welke manier rekening is gehouden met de opmerkingen van de Raad in het tweede advies. In het bijzonder is het verslag zodanig bijgewerkt dat gedetailleerder wordt ingegaan op de context van de EU-cyberbeveiliging, met inbegrip van de maatregelen die zijn opgenomen in de gezamenlijk mededeling "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU", (JOIN(2017) 450) en die van bijzonder belang zijn voor het Enisa, de blauwdruk voor de EU-cyberbeveiliging en het Europees onderzoeks- en kenniscentrum voor cyberbeveiliging, waaraan het Agentschap zijn adviezen over de EU-onderzoeksbehoeften zou koppelen.

In het verslag wordt uiteengezet hoe de hervorming van het Agentschap, met inbegrip van de nieuwe taken, de betere arbeidsvoorwaarden en de structurele samenwerking met EU-organen die op het gebied actief zijn, zijn aantrekkelijkheid als werkgever zou verbeteren en ertoe zou bijdragen de problemen bij de aanwerving van deskundigen aan te pakken. Verder bevat bijlage 6 bij het verslag een herziene raming van de kosten voor de beleidsopties voor het Enisa. Met betrekking tot het onderwerp certificering is het verslag herzien teneinde meer gedetailleerde uitleg, waaronder een grafische presentatie, te geven voor de voorkeursoptie, en ramingen te verstrekken van de kosten die de lidstaten en de Commissie moeten maken in verband met het nieuwe certificeringskader. De motivering van de keuze voor het Enisa als belangrijke actor in het kader is nadere verklaard op basis van zijn expertise op het gebied en het feit dat het het enige agentschap voor cyberbeveiliging op EU-niveau is. Tot slot zijn de

gedeelten over certificering herzien teneinde verduidelijking te bieden over aspecten in verband met het verschil met het huidige SOG-IS-stelsel en over de voordelen van de verschillende beleidsopties, en uiteen te zetten dat het type ICT-producten en -diensten dat onder een Europese certificeringsregeling valt, in de goedgekeurde regeling zelf zal worden bepaald.

Resultaatgerichtheid en vereenvoudiging

Niet van toepassing.

Gevolgen voor de grondrechten

Voor cyberbeveiliging is een essentiële rol weggelegd bij de bescherming van de persoonlijke levenssfeer en de persoonsgegevens voor personen in overeenstemming met de artikelen 7 en 8 van het Handvest van de grondrechten van de EU. In het geval van cyberincidenten lopen de persoonlijke levenssfeer en de bescherming van persoonsgegevens duidelijk gevaar. Cyberbeveiliging is derhalve een noodzakelijke voorwaarde voor eerbiediging van de persoonlijke levenssfeer en de vertrouwelijkheid van onze persoonsgegevens. Daarmee rekening houdend streeft het voorstel ernaar de cyberbeveiliging in Europa te versterken; het voorziet daartoe in een belangrijke aanvulling op de bestaande wetgeving ter bescherming van het grondrecht op bescherming van de persoonlijke levenssfeer en van persoonsgegevens. Cyberbeveiliging is ook van essentieel belang voor de bescherming van de vertrouwelijkheid van onze elektronische communicatie en dus voor de uitoefening van de vrijheid van meningsuiting en van informatie alsmede van andere daarmee samenhangende rechten, zoals de vrijheid van gedachte, geweten en godsdienst.

4. GEVOLGEN VOOR DE BEGROTING

Zie financieel memorandum.

5. OVERIGE ELEMENTEN

- **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

De Commissie zal toezicht houden op de toepassing van deze verordening en brengt om de vijf jaar verslag over haar evaluatie uit bij het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité. Deze verslagen zijn openbaar en geven nadere toelichting over de daadwerkelijke toepassing en handhaving van deze verordening.

- **Artikelsgewijze toelichting**

Titel I van de verordening omvat de volgende algemene bepalingen: het onderwerp (artikel 1), de definities (artikel 2), met inbegrip van verwijzingen naar de desbetreffende definities in andere EU-instrumenten, zoals Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS-richtlijn), Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 en Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad betreffende Europese normalisatie.

Titel II van de verordening bevat de belangrijkste bepalingen in verband met Enisa, het EU-cyberbeveiligingsagentschap.

Hoofdstuk I van deze titel omvat een omschrijving van het mandaat (artikel 3), de doelstellingen (artikel 4) en de taken van het Agentschap (artikelen 5 tot en met 11).

In hoofdstuk II wordt de organisatie van het Enisa omschreven; het omvat verder belangrijke bepalingen inzake de structuur ervan (artikel 12). Verder komen in dit hoofdstuk de samenstelling, de voorschriften voor stemming en de functies van de raad van bestuur (afdeling 1, artikelen 13 tot en met 17), het dagelijks bestuur (afdeling 2, artikel 18) en de uitvoerend directeur (afdeling 3, artikel 19) aan bod. Daarnaast bevat het hoofdstuk bepalingen inzake de samenstelling en de rol van de permanente groep van belanghebbenden (afdeling 4, artikel 20). Tot slot omvat afdeling 5 van dit hoofdstuk een nauwkeurige omschrijving van de operationele regels voor het Agentschap, onder meer wat betreft de programmering van de activiteiten, belangenconflicten, transparantie, vertrouwelijkheid en de toegang tot documenten (artikelen 21 tot en met 25).

Hoofdstuk III heeft betrekking op de vaststelling en structuur van het budget van het Agentschap (artikelen 26 en 27) en op de voorschriften voor de uitvoering ervan (artikelen 28 en 29). Het bevat verder bepalingen ter vergemakkelijking van de bestrijding van fraude, corruptie en andere onwettige activiteiten (artikel 30).

Hoofdstuk IV heeft betrekking op het personeel van het Agentschap. Het bevat algemene bepalingen inzake het statuut, de regeling voor andere personeelsleden en de regels inzake voorrechten en immuniteiten (artikelen 31 en 32). Verder bevat het een nauwkeurige omschrijving van de regels inzake de aanwerving en aanstelling van de uitvoerend directeur van het Agentschap (artikel 33). Tevens bevat het de bepalingen inzake het gebruikmaken van gedetacheerde nationale deskundigen of ander personeel dat niet in dienst is van het Agentschap (artikel 34).

Tot slot bevat hoofdstuk V de algemene bepalingen betreffende het Agentschap. In het hoofdstuk wordt de juridische status omschreven (artikel 35). Verder omvat het bepalingen inzake aansprakelijkheid, taalregelingen, de bescherming van persoonsgegevens (artikelen 36 tot en met 38) alsmede beveiligingsvoorschriften ter bescherming van gerubriceerde informatie en gevoelige niet-gerubriceerde informatie (artikel 40). Het bevat een omschrijving van de regels voor de samenwerking van het Agentschap met derde landen en internationale organisaties (artikel 39). Tot slot bevat het bepalingen inzake het hoofdkwartier van het Agentschap en de voorwaarden voor de bedrijfsuitoefening alsmede inzake administratieve controle door de Ombudsman (artikelen 41 en 42).

In titel III van de verordening wordt het Europees kader voor cyberbeveiligingscertificering (het "**kader**") voor ICT-producten en -diensten als *lex generalis* vastgesteld (artikel 1). In deze titel wordt het algemene doel van Europese regelingen voor cyberbeveiligingscertificering vastgesteld, dat wil zeggen waarborgen dat ICT-producten en -diensten voldoen aan gespecificeerde cyberbeveiligingseisen wat betreft hun capaciteit om op een bepaald zekerheidsniveau weerstand te bieden tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, doorgegeven of verwerkte gegevens of de daarmee samenhangende functies of van diensten in gevaar brengen (artikel 43). Daarnaast komen de beveiligingsdoelstellingen aan bod die met de Europese regelingen voor cyberbeveiligingscertificering worden nagestreefd (artikel 45), waaronder de capaciteit om gegevens te beschermen tegen accidentele of onrechtmatige toegang of openbaarmaking, vernietiging of wijziging, alsmede de inhoud (dat wil zeggen de elementen) van Europese regelingen voor cyberbeveiligingscertificering, zoals een gedetailleerde specificatie van het toepassingsgebied, de beveiligingsdoelstellingen, de evaluatiecriteria enz. (artikel 47).

In titel III worden verder de voornaamste juridische effecten van Europese regelingen voor cyberbeveiligingscertificering vastgesteld, namelijk i) de verplichting om de regeling op nationaal niveau toe te passen en de vrijwillige aard van certificering, ii) het effect dat nationale regelingen niet meer gelden als er Europese regelingen voor cyberbeveiligingscertificering op dezelfde producten of diensten van toepassing zijn (artikelen 48 en 49).

Verder omvat deze titel de procedure voor de vaststelling van Europese regelingen voor cyberbeveiligingscertificering en worden de respectievelijke rollen van de Commissie, het Enisa en de Europese Groep voor cyberbeveiligingscertificering ("de Groep") vastgesteld (artikel 44). Tot slot omvat deze titel de bepalingen inzake conformiteitsbeoordelingsinstanties, met inbegrip van de desbetreffende vereisten, bevoegdheden en taken, alsmede inzake nationale autoriteiten voor certificeringstoezicht en sancties.

Tevens wordt in deze titel de Groep vastgesteld als essentieel orgaan dat is samengesteld uit vertegenwoordigers van de nationale autoriteiten voor certificeringstoezicht en dat als voornaamste functie samen met het Enisa werkt aan de voorbereiding van Europese regelingen voor cyberbeveiligingscertificering alsmede het adviseren van de Commissie wat betreft algemene of specifieke kwesties in verband met het beleid inzake cyberbeveiligingscertificering.

Titel IV van de verordening bevat de slotbepalingen over de uitoefening van de bevoegdheidsdelegatie, evaluatievereisten, intrekking en opvolging alsmede de inwerkingtreding.

2017/0225 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[28],

Gezien het advies van het Comité van de Regio's[29],

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Netwerk- en informatiesystemen alsmede telecommunicatienetwerken en -diensten spelen een cruciale rol in de maatschappij en zijn de ruggengraat van de economische groei geworden. Informatie- en communicatietechnologie vormt de basis van de complexe systemen die maatschappelijke activiteiten ondersteunen en onze economieën draaiende houden in essentiële sectoren zoals gezondheid, energie, financiën en vervoer, en met name de werking van de interne markt ondersteunen.

(2) Burgers, ondernemingen en regeringen in de hele Unie maken alom gebruik van netwerk- en informatiesystemen. Digitalisering en connectiviteit zijn cruciale kenmerken van steeds meer producten en diensten, en door de opkomst van het internet der dingen zullen naar verwachting de volgende tien jaar in de hele EU miljoenen, zo niet miljarden verbonden digitale toestellen worden gebruikt. Er worden weliswaar steeds meer toestellen met het internet verbonden, maar bij het ontwerp wordt onvoldoende rekening gehouden met de beveiliging en de weerbaarheid, waardoor de cyberbeveiliging te wensen overlaat. Het beperkte gebruik van certificering leidt er in deze context toe dat gebruikers binnen organisaties en afzonderlijke gebruikers te weinig informatie hebben over de cyberbeveiligingskenmerken van ICT-producten en -diensten, hetgeen schadelijk is voor het vertrouwen in digitale oplossingen.

(3) De toenemende digitalisering en connectiviteit leiden tot grotere risico's op het gebied van cyberbeveiliging, waardoor de maatschappij in het algemeen kwetsbaarder wordt

[28] PB C , blz. .
[29] PB C , blz. .

voor cyberdreigingen en waardoor individuen, waaronder kwetsbare personen zoals kinderen, met steeds ernstigere gevaren worden geconfronteerd. Om dit risico voor de samenleving te beperken, moeten alle noodzakelijke maatregelen worden genomen om de cyberbeveiliging in de EU te versterken en netwerk- en informatiesystemen, telecommunicatienetwerken, digitale producten, diensten en toestellen die worden gebruikt door burgers, overheden en bedrijven – van het mkb tot exploitanten van kritieke infrastructuurvoorzieningen – beter te beschermen tegen cyberdreigingen.

(4) Cyberaanvallen komen steeds vaker voor, en een verbonden economie en samenleving die kwetsbaarder is voor cyberdreigingen en -aanvallen moet beter worden beschermd. Hoewel cyberaanvallen vaak grensoverschrijdend zijn, nemen cyberbeveiligingsautoriteiten en wetshandhavingsinstanties vaak op nationaal niveau beleidsmaatregelen. Grootschalige cyberincidenten kunnen de voorziening van essentiële diensten in de hele EU verstoren. Dit vereist doeltreffende respons en crisisbeheer op EU-niveau, gebaseerd op specifiek beleid en bredere instrumenten voor Europese solidariteit en wederzijdse bijstand. Bovendien is een regelmatige beoordeling van de staat van de cyberbeveiliging en -weerbaarheid in de Unie, op basis van betrouwbare EU-gegevens, alsmede een systematische prognose van toekomstige ontwikkelingen, uitdagingen en dreigingen, zowel op EU- als op mondiaal niveau, belangrijk voor beleidmakers, het bedrijfsleven en de gebruikers.

(5) Gezien de toegenomen uitdagingen waarmee de Unie op het vlak van cyberbeveiliging wordt geconfronteerd, moet een uitvoerige reeks maatregelen worden genomen die voortbouwen op eerdere EU-maatregelen en die bijdragen tot doelstellingen die elkaar wederzijds versterken. Zo moeten de vermogens en paraatheid van de lidstaten en het bedrijfsleven worden versterkt en moet de samenwerking en coördinatie tussen de lidstaten en de EU-instellingen, -agentschappen en -organen worden verbeterd. Aangezien cyberdreigingen zich niet door grenzen laten tegenhouden, moeten er een versterking komen van de vermogens op EU-niveau die een aanvulling kunnen vormen op maatregelen van de lidstaten, met name in het geval van grootschalige grensoverschrijdende cyberincidenten en -crises. Er moeten meer inspanningen worden geleverd om de burgers en ondernemingen bewuster te maken van cyberbeveiligingskwesties. Tevens moet het vertrouwen in de digitale eengemaakte markt verder worden versterkt door transparante informatie te verstrekken over het beveiligingsniveau van ICT-producten en -diensten. Dit kan mede mogelijk worden gemaakt door middel van EU-brede certificering met gemeenschappelijke cyberbeveiligingsvereisten en evaluatiecriteria, ongeacht de nationale markten en sectoren.

(6) In 2004 hebben het Europees Parlement en de Raad Verordening (EG) nr. 460/2004[30] tot oprichting van Enisa vastgesteld teneinde bij te dragen tot een hoog niveau van netwerk- en informatiebeveiliging in de Unie en tot de ontwikkeling van een cultuur van netwerk- en informatiebeveiliging ten bate van de burgers, consumenten, ondernemingen en overheidsadministraties. In 2008 hebben het Europees Parlement en de Raad Verordening (EG) nr. 1007/2008[31] vastgesteld, waarbij het mandaat van het

[30] Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging (PB L 77 van 13.3.2004, blz. 1).

[31] Verordening (EG) nr. 1007/2008 van het Europees Parlement en de Raad van 24 september 2008 tot wijziging van Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor

Agentschap werd verlengd tot maart 2012. Bij Verordening (EG) nr. 580/2011[32] werd het mandaat van het Agentschap tot 13 september 2013 verlengd. In 2013 hebben het Europees Parlement en de Raad met betrekking tot het Enisa Verordening (EU) nr. 526/2013[33] vastgesteld, waarbij Verordening (EG) nr. 460/2004 werd ingetrokken en het mandaat van het Agentschap tot juni 2020 werd verlengd

(7) De EU heeft reeds belangrijke maatregelen genomen om voor cyberbeveiliging te zorgen en om het vertrouwen in digitale technologieën te vergroten. In 2013 werd de EU-strategie inzake cyberbeveiliging goedgekeurd als leidraad voor de beleidsreactie van de Unie op cyberdreigingen en risico's voor de cyberbeveiliging. Om ervoor te zorgen dat de Europeanen online beter worden beschermd, heeft de Unie in 2016 de eerste wetgevingshandeling op het gebied van cyberbeveiliging vastgesteld, Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (de "NIS-richtlijn"). Bij de NIS-richtlijn werden eisen vastgesteld betreffende nationale vermogens inzake cyberbeveiliging, werden de eerste mechanismen opgezet om de strategische en operationele samenwerking tussen de lidstaten te versterken, en werden verplichtingen ingevoerd met betrekking tot beveiligingsmaatregelen en melding van incidenten in alle sectoren die van vitaal belang zijn voor de economie en de samenleving, zoals energie, vervoer, water, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, digitale infrastructuur en belangrijke digitaledienstverleners (zoekmachines, cloudcomputingdiensten en onlinemarktplaatsen). Aan het Enisa werd een cruciale rol toegewezen in het ondersteunen van de implementatie van deze richtlijn. Daarnaast is de doeltreffende bestrijding van cybercriminaliteit een belangrijke prioriteit in de Europese Veiligheidsagenda, hetgeen bijdraagt tot de algemene doelstelling om een hoog cyberbeveiligingsniveau tot stand te brengen.

(8) Erkend wordt dat de algehele beleidscontext aanzienlijk veranderd is sinds de EU-strategie inzake cyberbeveiliging in 2013 werd vastgesteld en het mandaat van het Agentschap de laatste keer werd herzien, onder meer doordat de omstandigheden wereldwijd minder zeker en minder veilig zijn geworden. In deze context en binnen het kader van het nieuwe EU-beleid inzake cyberbeveiliging moet het mandaat van het Enisa worden herzien teneinde de rol van het Enisa in het veranderde cyberbeveiligingsecosysteem te bepalen en te waarborgen dat het op doeltreffende wijze bijdraagt tot de respons van de Unie op uitdagingen op het gebied van cyberbeveiliging die voortvloeien uit de radicaal gewijzigde cyberdreiging, waarvoor, zoals is gebleken uit de evaluatie van het Agentschap, het huidige mandaat niet toereikend is.

(9) Het bij deze verordening vastgestelde Agentschap moet het Enisa, zoals opgericht bij Verordening (EG) nr. 526/2013, opvolgen. Het Agentschap moet de taken uitvoeren die er bij deze verordening en bij de wetgevingshandelingen van de Unie op het gebied van cyberbeveiliging aan worden toegewezen, onder meer door expertise en advies te

---

netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap (PB L 293 van 31.10.2008, blz. 1).

[32] Verordening (EU) nr. 580/2011 van het Europees Parlement en de Raad van 8 juni 2011 tot wijziging van Verordening (EG) nr. 460/2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, ten aanzien van de looptijd van het Agentschap (PB L 165 van 24.6.2011, blz. 3).

[33] Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad van 21 mei 2013 inzake het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en tot intrekking van Verordening (EG) nr. 460/2004 (OJ L 165 van 18.6.2013, blz. 41).

verstrekken en te fungeren als informatie- en kenniscentrum van de EU. Het Agentschap moet de uitwisseling van beste praktijken tussen de lidstaten en particuliere belanghebbenden bevorderen, advies verstrekken over beleidsmaatregelen aan de Europese Commissie en de lidstaten, fungeren als referentiepunt voor sectorale beleidsinitiatieven van de EU inzake cyberbeveiligingskwesties, en de operationele samenwerking tussen de lidstaten onderling en tussen de lidstaten en de EU-instellingen, -agentschappen en -organen bevorderen.

(10) Binnen het kader van Besluit 2004/97/EG, Euratom, vastgesteld tijdens de Europese Raad van 13 december 2003, hebben de vertegenwoordigers van de lidstaten besloten dat het Enisa zou worden gevestigd in een door de Griekse regering aan te wijzen stad in Griekenland. De lidstaat van vestiging moet zorgen voor zo gunstig mogelijke voorwaarden voor de vlotte en doeltreffende werking van het Agentschap. Met het oog op de goede en doeltreffende uitvoering van zijn taken, het aanwerven en behouden van zijn personeel en efficiëntere netwerkactiviteiten is het noodzakelijk dat het Agentschap op een passende locatie wordt gehuisvest, waar onder meer goede vervoersverbindingen en passende faciliteiten voorhanden zijn voor echtgenoten en kinderen die meereizen met de leden van het personeel van het Agentschap. De noodzakelijke bepalingen moeten worden vastgelegd in een overeenkomst tussen het Agentschap en de lidstaat van vestiging, die wordt gesloten nadat de raad van bestuur van het Agentschap daarmee heeft ingestemd.

(11) Gezien de toenemende uitdagingen op het gebied van cyberbeveiliging waarmee de Unie wordt geconfronteerd, moeten de financiële en personele middelen die aan het Agentschap worden toegewezen, worden uitgebreid om recht te doen aan zijn versterkte rol en taken en zijn kritieke positie bij de verdediging van het Europese digitale ecosysteem.

(12) Het Agentschap moet een hoog expertiseniveau ontwikkelen en handhaven, als referentiepunt fungeren en vertrouwen in de eengemaakte markt scheppen door zijn onafhankelijkheid, de kwaliteit van zijn advies en informatie, de transparantie van zijn procedures en werkmethoden, en de toewijding bij de uitvoering van zijn taken. Het Agentschap moet proactief bijdragen tot nationale en EU-inspanningen en daarbij zijn taken uitvoeren in nauwe samenwerking met de instellingen, organen, instanties en agentschappen van de Unie en de lidstaten. Bovendien moet het Agentschap voortbouwen op de input van en de samenwerking met de privésector en andere relevante belanghebbenden. In een reeks taken moet worden vastgesteld hoe het Agentschap zijn doelstellingen moet verwezenlijken en toch flexibel kan functioneren.

(13) Het Agentschap moet de Commissie bijstaan met advies, standpunten en analyses over alle Unie-aangelegenheden in verband met de ontwikkeling van beleid en wetgeving en in verband met actualiseringen en herzieningen op het gebied van cyberbeveiliging, met inbegrip van de bescherming van kritieke infrastructuur en cyberweerbaarheid. Het Agentschap moet fungeren als referentiepunt voor advies en expertise ten behoeve van sectorspecifieke beleids- en wetgevingsinitiatieven van de EU in verband met cyberbeveiliging.

(14) De onderliggende taak van het Agentschap bestaat uit het bevorderen van de consistente uitvoering van het desbetreffende juridische kader, en met name de doeltreffende uitvoering van de NIS-richtlijn die van essentieel belang is om de cyberweerbaarheid te versterken. Gezien het snel veranderende cyberdreigingslandschap is het duidelijk dat de lidstaten moeten worden ondersteund

met een meer alomvattende, beleidsoverschrijdende aanpak voor de opbouw van de cyberweerbaarheid.

(15) Het Agentschap moet de lidstaten en de instellingen, organen, instanties en agentschappen van de Unie helpen bij hun inspanningen om vermogens en paraatheid te ontwikkelen en te vergroten om problemen en incidenten op het gebied van cyberbeveiliging en in verband met de beveiliging van netwerk- en informatiesystemen te voorkomen, op te sporen en aan te pakken. Het Agentschap moet met name steun verlenen bij de ontwikkeling en versterking van de nationale CSIRT's om ervoor te zorgen dat deze in de Unie een hoog gemeenschappelijk maturiteitsniveau bereiken. Het Agentschap moet ook helpen bij het ontwikkelen en bijwerken van strategieën van de EU en de lidstaten voor de beveiliging van netwerk- en informatiesystemen, en met name voor cyberbeveiliging, alsmede de verspreiding ervan bevorderen en de voortgang van de uitvoering ervan volgen. Het Agentschap moet overheidsinstanties ook opleidingen en opleidingsmateriaal aanbieden en waar passend voorzien in opleidingen voor de opleiders teneinde de lidstaten te helpen bij de ontwikkeling van hun eigen opleidingscapaciteit.

(16) Het Agentschap moet de op grond van de NIS-richtlijn opgerichte samenwerkingsgroep helpen bij de uitvoering van zijn taken, in het bijzonder door expertise en advies te verstrekken en de uitwisseling van goede praktijken te bevorderen, met name wat betreft de identificatie van aanbieders van essentiële diensten door de lidstaten, onder meer met betrekking tot grensoverschrijdende afhankelijkheid, inzake risico's en incidenten.

(17) Met het oog op de bevordering van de samenwerking tussen de overheidssector en de particuliere sector enerzijds, en binnen de particuliere sector anderzijds, in het bijzonder wat betreft de ondersteuning van kritieke infrastructuurvoorzieningen, moet het Agentschap de oprichting van sectorale centra voor informatie-uitwisseling en -analyse (ISAC's) stimuleren door beste praktijken en richtsnoeren over beschikbare instrumenten en procedures te verstrekken, en door richtsnoeren te verstrekken over de manier waarop problemen op regelgevingsgebied in verband met informatie-uitwisseling kunnen worden opgelost.

(18) Het Agentschap moet nationale verslagen van de CSIRT's en CERT-EU verzamelen en analyseren, alsmede gemeenschappelijke regels, een taalregeling en terminologie voor de uitwisseling van informatie vaststellen. Het Agentschap moet verder zorgen voor betrokkenheid van de particuliere sector, binnen het kader van de NIS-richtlijn dat met de oprichting van het CSIRT-netwerk de basis heeft gelegd voor de vrijwillige uitwisseling van technische informatie op operationeel niveau.

(19) Het Agentschap moet bijdragen tot een reactie op EU-niveau in het geval van grootschalige grensoverschrijdende cyberbeveiligingsincidenten en -crises. Tot deze functie behoort het vergaren van relevante informatie en het optreden als bemiddelaar tussen het CSIRT-netwerk enerzijds en de technische gemeenschap en de beleidsmakers die belast zijn met crisisbeheer anderzijds. Daarnaast kan het Agentschap vanuit technisch oogpunt ondersteuning bieden bij de aanpak van incidenten door de relevante technische uitwisseling van oplossingen tussen de lidstaten te faciliteren en input te leveren voor publieke communicatie. Het Agentschap moet het desbetreffende proces ondersteunen door de modaliteiten van een dergelijke samenwerking in het kader van jaarlijkse cyberbeveiligingsoefeningen te testen.

(20) Bij de uitvoering van zijn operationele taken moet het Agentschap gebruikmaken van de expertise waarover CERT-EU beschikt door middel van gestructureerde samenwerking die in fysieke zin dicht bij elkaar plaatsvindt. Door deze gestructureerde samenwerking worden de nodige synergie-effecten en de opbouw van de expertise van het Enisa bevorderd. Wanneer passend moeten specifieke regelingen tussen de twee organisaties worden vastgesteld teneinde de praktische uitvoering van een dergelijke samenwerking te bepalen.

(21) Overeenkomstig zijn operationele taken moet het Agentschap in staat zijn ondersteuning te bieden aan de lidstaten, bijvoorbeeld door advies of technische bijstand te verstrekken, of door de analyse van dreigingen en incidenten te verzorgen. In de aanbeveling van de Commissie voor een gecoördineerde respons op grootschalige grensoverschrijdende cyberincidenten en -crises wordt aanbevolen dat de lidstaten te goeder trouw samenwerken en zowel onderling als met het Enisa onverwijld informatie uitwisselen betreffende grootschalige cyberincidenten en -crises. Dergelijke informatie moet het Enisa verder helpen bij de uitoefening van zijn operationele taken.

(22) In het kader van de regelmatige samenwerking op technisch niveau ter ondersteuning van het situatiebewustzijn van de Unie, moet het Agentschap regelmatig het technisch situatieverslag inzake EU-cyberbeveiliging over incidenten en bedreigingen opstellen, op basis van publiek beschikbare informatie en eigen analyses en verslagen die het ontvangt van de CSIRT's van de lidstaten (op vrijwillige basis) of de bij de NIS-richtlijn opgerichte centrale contactpunten, het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol en CERT-EU, en, voor zover passend, het EU-centrum voor inlichtingen (INTCEN) van de Europese Dienst voor extern optreden (EDEO). Dit verslag moet ter beschikking worden gesteld van de relevante instanties van de Raad, de Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid, en het CSIRT-netwerk.

(23) Technisch ex-postonderzoek van incidenten met een aanzienlijke impact in meer dan een lidstaat dat wordt ondersteund of uitgevoerd door het Agentschap op verzoek van of met toestemming van de betrokken lidstaten, dient te zijn gericht op de preventie van toekomstige incidenten en te worden verricht zonder afbreuk te doen aan gerechtelijke of administratieve procedures ter vaststelling van schuld of aansprakelijkheid.

(24) De betrokken lidstaten moeten het Agentschap ten behoeve van het onderzoek de nodige informatie verstrekken en de nodige bijstand verlenen, zonder afbreuk te doen aan artikel 346 van het Verdrag betreffende de werking van de Europese Unie en onverminderd andere redenen van overheidsbeleid.

(25) De lidstaten kunnen de bij het incident betrokken ondernemingen verzoeken medewerking te verlenen door het Agentschap de nodige informatie en bijstand te geven, zonder afbreuk te doen aan hun recht om commercieel gevoelige informatie te beschermen.

(26) Om de uitdagingen op het gebied van cyberbeveiliging beter te begrijpen en de lidstaten en de EU-instellingen strategisch langetermijnadvies te verstrekken, moet het Agentschap bestaande en opkomende risico's analyseren. Daartoe moet het Agentschap, in samenwerking met de lidstaten en, wanneer passend, met bureaus voor de statistiek en anderen, relevante informatie verzamelen, opkomende technologieën analyseren en themaspecifieke beoordelingen verstrekken over de verwachte maatschappelijke, juridische, economische en regelgevende gevolgen van

technologische innovaties op het vlak van netwerk- en informatiebeveiliging, en met name op het vlak van cyberbeveiliging. Ook moet het Agentschap de lidstaten en de EU-instellingen, -agentschappen en –organen door middel van dreigings- en incidentanalyse ondersteunen bij het constateren van nieuwe trends en het voorkomen van problemen in verband met cyberbeveiliging.

(27) Om de weerbaarheid van de Unie te versterken, moet het Agentschap in staat zijn topprestaties te leveren op het gebied van de beveiliging van internetinfrastructuur kritieke infrastructuurvoorzieningen door het verstrekken van advies, richtsnoeren en beste praktijken. Met het oog op het waarborgen van gemakkelijkere toegang tot beter gestructureerde informatie over cyberbeveiligingsrisico's en potentiële oplossingen, moet het Agentschap zorgen voor de ontwikkeling en instandhouding van het "informatiecentrum" van de Unie, een centraal portaal dat het publiek voorziet van informatie over cyberbeveiliging, afkomstig van de instellingen, agentschappen en organen van de EU en de lidstaten.

(28) Het Agentschap moet bijdragen tot de bewustmaking van het publiek omtrent de risico's die samenhangen met cyberbeveiliging, en richtsnoeren verstrekken inzake goede praktijken voor afzonderlijke gebruikers, gericht op burgers en organisaties. Verder moet het Agentschap bijdragen tot de bevordering van beste praktijken en oplossingen op het niveau van individuen en organisaties door publiekelijk beschikbare informatie over significante incidenten te verzamelen en te analyseren, en door verslagen op te stellen met het oog op het verstrekken van richtsnoeren aan bedrijven en burgers, waarbij het algemene niveau van paraatheid en weerbaarheid wordt verhoogd. Het Agentschap moet daarnaast regelmatig, in samenwerking met de lidstaten en de EU-instellingen, -organen, -instanties en -agentschappen, aan de eindgebruikers gerichte voorlichtingscampagnes opzetten om een veiliger individueel online-gedrag te promoten, het publiek bewuster te maken van potentiële gevaren in de cyberruimte, waaronder cybermisdaden zoals phishing-aanvallen, botnets, financiële en bankfraude, en ook door fundamenteel authentificatie- en gegevensbeschermingsadvies te verlenen. Het Agentschap moet een centrale rol spelen bij de snellere voorlichting van de eindgebruikers over de beveiliging van toestellen.

(29) Om bedrijven die actief zijn in de cyberbeveiligingssector en de gebruikers van cyberbeveiligingsoplossingen te ondersteunen, moet het Agentschap een "waarnemingspost" opzetten en onderhouden door regelmatig analyses uit te voeren en voorlichting te geven over de voornaamste tendensen op de markt voor cyberbeveiliging, zowel aan de vraag- als aan de aanbodzijde.

(30) Om te waarborgen dat het Agentschap zijn doelstellingen volledig verwezenlijkt, moet het overleggen met de relevante instellingen, agentschappen en organen, met inbegrip van CERT-EU, het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol, het Europees Defensieagentschap (EDA), het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen (eu-LISA), het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA) en alle andere EU-agentschapen die bij cyberbeveiliging zijn betrokken. Het moet overleggen met de autoriteiten die belast zijn met gegevensbescherming teneinde kennis en beste praktijken uit te wisselen en advies te geven over cyberbeveiligingsaspecten die een effect kunnen hebben op hun werkzaamheden. De vertegenwoordigers van de wetshandhavings- en gegevensbeschermingsautoriteiten van de lidstaten en de Unie moeten recht hebben op vertegenwoordiging in de permanente groep van belanghebbenden van het Agentschap. Wanneer het Agentschap contact opneemt met wethandhavingsinstanties betreffende netwerk- en

informatiebeveiligingsaspecten die van invloed kunnen zijn op hun werkzaamheden, moet het Agentschap de bestaande informatiekanalen en gevestigde netwerken respecteren.

(31) Het Agentschap, dat als lid tevens het secretariaat van het CSIRT-netwerk verzorgt, moet de CSIRT's van de lidstaten en CERT-EU ondersteunen wat betreft de operationele samenwerking in verband met alle relevant taken van het CSIRT-netwerk, zoals vastgesteld in de NIS-richtlijn. In het geval van incidenten, aanvallen of storingen in netwerken of infrastructuurvoorzieningen die door de CSIRT's worden beheerd of beveiligd en waarbij ten minste twee CERT's betrokken zijn of kunnen zijn, moet het Agentschap bovendien de samenwerking bevorderen tussen de betrokken CSIRT's, daarbij terdege rekening houdend met de standaardwerkwijzen van het CSIRT-netwerk.

(32) Om de paraatheid van de Unie betreffende de reactie op cyberbeveiligingsincidenten te verhogen, moet het Agentschap jaarlijks cyberbeveiligingsoefeningen op EU-niveau organiseren, en de lidstaten alsmede EU-instellingen,- agentschappen en -organen op hun verzoek ondersteunen bij het organiseren van oefeningen.

(33) Verder moet het Agentschap expertise op het gebied van cyberbeveiligingscertificering ontwikkelen en in stand houden met het oog op de ondersteuning van het EU-beleid op dit gebied. Het Agentschap moet het gebruik van cyberbeveiligingscertificering binnen de Unie bevorderen, onder meer door bij te dragen aan de totstandbrenging en instandhouding van een kader voor cyberbeveiligingscertificering op EU-niveau, om de transparantie van de cyberbeveiligingszekerheid van ICT-producten en –diensten, en daarmee het vertrouwen in de digitale interne markt, te versterken.

(34) Efficiënte beleidsmaatregelen inzake cyberbeveiliging moeten zijn gebaseerd op goed ontwikkelde methoden voor risicoanalyse, zowel in de overheidssector als in de particuliere sector. Methoden voor risicoanalyse worden op verschillende niveaus ingezet zonder dat er een gemeenschappelijke praktijk bestaat over de manier waarop deze efficiënt kunnen worden toegepast. Door beste praktijken voor risicoanalyse en voor interoperabele oplossingen voor risicobeheersing binnen overheids- en particuliere organisaties te promoten en te ontwikkelen, zal het cyberbeveiligingsniveau in de Unie worden verbeterd. Daartoe moet het Agentschap de samenwerking tussen belanghebbenden op het niveau van de Unie bevorderen door hen te ondersteunen in hun inspanningen om Europese en internationale normen vast te stellen en te gebruiken met betrekking tot risicobeheer en meetbare beveiliging van elektronische producten, systemen, netwerken en diensten die, samen met software, de netwerk- en informatiesystemen vormen.

(35) Het Agentschap moet de lidstaten en dienstverleners stimuleren hun algemene veiligheidsnormen op te voeren, zodat alle internetgebruikers de nodige stappen kunnen ondernemen om voor hun eigen cyberbeveiliging te zorgen. Wanneer producten en diensten niet aan cyberbeveiligingsnormen voldoen, moeten dienstverleners en fabrikanten van producten deze intrekken of recyclen. In samenwerking met de bevoegde autoriteiten kan het Enisa informatie verspreiden over het cyberbeveiligingsniveau van de producten en diensten die op de interne markt worden aangeboden, en kan het aanbieders en fabrikanten waarschuwen en hen verplichten de beveiliging, waaronder de cyberbeveiliging, van hun producten en diensten te verbeteren.

(36) Het Agentschap moet ten volle rekening houden met de lopende activiteiten op het gebied van onderzoek, ontwikkeling en technologiebeoordeling, en in het bijzonder met de activiteiten van de verschillende onderzoeksinitiatieven van de Unie om de instellingen, organen en instanties van de Unie en in voorkomend geval de lidstaten op hun verzoek te adviseren over onderzoeksbehoeften op het gebied van netwerk- en informatiebeveiliging, en met name cyberbeveiliging.

(37) Problemen inzake cyberbeveiliging zijn wereldwijde problemen. Er is dan ook behoefte aan nauwere internationale samenwerking om de beveiligingsnormen, met inbegrip van de omschrijving van gemeenschappelijke gedragsnormen, en de informatie-uitwisseling te verbeteren om snellere internationale samenwerking bij – en een gemeenschappelijke wereldwijde aanpak van – problemen op het gebied van netwerk- en informatiebeveiliging te stimuleren. Daartoe moet het Agentschap een verregaandere betrokkenheid van de Unie en samenwerking met derde landen en internationale organisaties ondersteunen door, voor zover van toepassing, de desbetreffende instellingen, organen en instellingen van de Unie van de noodzakelijke expertise en analyses te voorzien.

(38) Het Agentschap moet kunnen reageren op ad-hocverzoeken om advies en bijstand van de lidstaten en de EU-instellingen, -agentschappen en -organen in overeenstemming met de doelstellingen van het Agentschap.

(39) Het is noodzakelijk met betrekking tot het bestuur van het Agentschap bepaalde beginselen toe te passen om te voldoen aan de gezamenlijke verklaring en gemeenschappelijke aanpak die in juli 2012 door de interinstitutionele werkgroep voor gedecentraliseerde EU-agentschappen zijn overeengekomen en die tot doel hebben de activiteiten van de agentschappen te stroomlijnen en hun prestaties te verbeteren. De gezamenlijke verklaring en gemeenschappelijke aanpak moeten ook naar behoren tot uiting komen in de werkprogramma's, de beoordelingen en de verslaglegging en de administratieve werkwijzen van het Agentschap.

(40) De raad van bestuur, die is samengesteld uit vertegenwoordigers van de lidstaten en van de Commissie, moet de algemene richting van de werkzaamheden van het Agentschap vaststellen en garanderen dat het Agentschap zijn taken overeenkomstig deze verordening uitvoert. De raad van bestuur dient de noodzakelijke bevoegdheden toegewezen te krijgen voor de vaststelling van de begroting, de controle op de uitvoering ervan, de vaststelling van passende financiële regels, de opstelling van transparante werkprocedures voor besluitvorming door het Agentschap, de goedkeuring van het enig programmeringsdocument van het Agentschap, de vaststelling van zijn eigen reglement van orde, de benoeming van de uitvoerend directeur en de besluitvorming over de verlenging van de ambtstermijn van de uitvoerend directeur en de beëindiging ervan.

(41) Omwille van de goede en doeltreffende werking van het Agentschap moeten de Commissie en de lidstaten erop toezien dat personen die worden benoemd tot de raad van bestuur over passende professionele deskundigheid en ervaring op functionele gebieden beschikken. De Commissie en de lidstaten dienen zich tevens in te spannen om het verloop onder hun respectievelijke vertegenwoordigers in de raad van bestuur te beperken om continuïteit in haar werk zeker te stellen.

(42) Voor een goede werking van het Agentschap is het noodzakelijk dat de uitvoerend directeur wordt benoemd op grond van zowel verdiensten en aantoonbare administratieve en bestuurskundige vaardigheden, als van bekwaamheid en ervaring die relevant is voor cyberbeveiliging. Daarnaast dient hij zijn taken op volledig

onafhankelijke wijze uit te voeren. De uitvoerend directeur moet een voorstel voor het werkprogramma van het Agentschap voorbereiden, na overleg met de Commissie, en alle nodige stappen ondernemen om de goede uitvoering van het werkprogramma van het Agentschap te garanderen. Hij moet een jaarverslag opstellen, dat moet worden voorgelegd aan de raad van bestuur, een ontwerpverklaring van de geraamde inkomsten en uitgaven van het Agentschap opstellen en de begroting ten uitvoer leggen. De uitvoerend directeur moet over de mogelijkheid beschikken om ad-hocwerkgroepen op te richten voor specifieke kwesties, met name van wetenschappelijke, technische, juridische of sociaaleconomische aard. De uitvoerend directeur moet erop toezien dat de leden van de ad-hocwerkgroepen overeenkomstig de hoogste normen inzake deskundigheid worden geselecteerd, ermee rekening houdende dat, afhankelijk van de specifieke kwestie, een passend evenwicht moet worden bereikt tussen de overheidsinstanties van de lidstaten, de instellingen van de Unie, de private sector, inclusief het bedrijfsleven, de gebruikers en universitaire deskundigen op het gebied van netwerk- en informatiebeveiliging.

(43) Het dagelijks bestuur moet bijdragen tot de doeltreffende werking van de raad van bestuur. In het kader van de voorbereidende werkzaamheden met betrekking tot besluiten van de raad van bestuur, moet het dagelijks bestuur relevante informatie nauwkeurig onderzoeken, de beschikbare opties onderzoeken alsmede advies en oplossingen bieden ter voorbereiding voor relevante besluiten van de raad van bestuur.

(44) Het Agentschap moet beschikken over een permanente groep van belanghebbenden als adviserend orgaan teneinde regelmatig overleg met de private sector, consumentenorganisaties en andere relevante belanghebbenden te waarborgen. De op voorstel van de uitvoerend directeur door de raad van bestuur opgerichte permanente groep van belanghebbenden moet zich richten op voor de belanghebbenden relevante kwesties en deze onder de aandacht van het Agentschap brengen. De samenstelling van de permanente groep van belanghebbenden, de aan deze groep toegewezen taken en het feit dat de groep moet worden geraadpleegd met betrekking tot het ontwerp van het werkprogramma, moeten waarborgen dat de belanghebbenden voldoende worden vertegenwoordigd in de werkzaamheden van het Agentschap.

(45) Het Agentschap moet beschikken over regels ter voorkoming en beheersing van belangenconflicten. Het Agentschap moet verder de relevante bepalingen van de Unie inzake publieke toegang tot documenten toepassen, zoals uiteengezet in Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad[34]. Persoonsgegevens moeten worden verwerkt overeenkomstig Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens[35]. Het Agentschap dient in het bijzonder de bepalingen na te leven die van toepassing zijn op de EU-instellingen alsmede de nationale wetgeving inzake de behandeling van informatie, in het bijzonder gevoelige niet-gerubriceerde informatie en gerubriceerde EU-informatie.

---

[34] Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (PB L 145 van 31.5.2001, blz. 43).

[35] PB L 8 van 12.1.2001, blz. 1.

(46) Om de volledige autonomie en onafhankelijkheid van het Agentschap te waarborgen en het in staat te stellen bijkomende en nieuwe taken te verrichten, waaronder onvoorziene noodmaatregelen, dient aan het Agentschap een toereikende eigen begroting te worden toegekend die hoofdzakelijk wordt gefinancierd uit een bijdrage van de Unie en bijdragen van derde landen die deelnemen aan de werkzaamheden van het Agentschap. Het merendeel van het personeel van het Agentschap moet rechtstreeks ingezet worden voor de operationele tenuitvoerlegging van het mandaat van het Agentschap. De lidstaat van vestiging of om het even welke andere lidstaat mag een vrijwillige bijdrage leveren aan de inkomsten van het Agentschap. De EU-begrotingsprocedure blijft van toepassing op eventuele subsidies die ten laste van de algemene begroting van de Unie komen. Bovendien controleert de Rekenkamer de rekeningen van het Agentschap teneinde transparantie en verantwoording zeker te stellen.

(47) Een conformiteitsbeoordeling is het proces waarin wordt aangetoond of voldaan is aan de vastgestelde eisen voor een product, proces, dienst, systeem, persoon of instantie. Voor de toepassing van deze verordening moet certificering worden beschouwd als een soort conformiteitsbeoordeling met betrekking tot de cyberbeveiligingskenmerken van een product, proces, dienst, systeem of een combinatie daarvan ("ICT-producten en -diensten") door een onafhankelijke derde partij die niet de fabrikant van het product of de dienstverlener is. Door middel van certificering kan niet per definitie worden gewaarborgd dat gecertificeerde ICT-producten en -diensten cyberbeveiligd zijn. Certificering is veeleer een procedure en een technische methode om officieel te bevestigen dat ICT-producten en -diensten zijn getest en dat deze voldoen aan bepaalde eisen op het gebied van cyberbeveiliging die elders zijn vastgesteld, bijvoorbeeld in technische normen.

(48) Cyberbeveiligingscertificering is belangrijk om het vertrouwen in en de beveiliging van ICT-producten en -diensten te verhogen. De digitale eengemaakte markt, en met name de data-economie en het internet der dingen, kan enkel gedijen als het grote publiek er vertrouwen in heeft dat dergelijke producten en diensten een bepaald niveau van zekerheid inzake cyberbeveiliging bieden. Verbonden en zelfsturende auto's, elektronische medische toestellen, besturingssystemen voor industriële automatisatie of slimme netten zijn slechts enkele voorbeelden van sectoren waarin certificering reeds op grote schaal wordt gebruikt of naar verwachting in de toekomst zal worden gebruikt. De sector waarop de NIS-richtlijn van toepassing is, zijn tevens de sectoren waarin cyberbeveiligingscertificering van cruciaal belang is.

(49) In de mededeling "Versterken van het Europese cyberbeveiligingssysteem en bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche" van 2016 heeft de Commissie gesteld dat er behoefte is aan hoogwaardige, betaalbare en interoperabele producten en oplossingen op het gebied van cyberbeveiliging. De levering van ICT-producten en -diensten binnen de eengemaakte markt blijft in geografisch opzicht zeer versnipperd, omdat de cyberbeveiligingsbranche in Europa zich grotendeels op basis van de vraag van nationale overheden heeft ontwikkeld. Daarnaast zijn het ontbreken van interoperabele oplossingen (technische normen), praktijken en EU-wijde certificeringsmechanismen lacunes waarmee de eengemaakte markt voor cyberbeveiliging kampt. Enerzijds maakt dit het voor Europese ondernemingen moeilijk om op nationaal, Europees en mondiaal niveau te concurreren. Anderzijds hebben burgers en bedrijven hierdoor slechts toegang tot een beperkte keuze aan levensvatbare en bruikbare cyberbeveiligingstechnologieën. Verder heeft de Commissie in de tussentijdse evaluatie van de uitvoering van de

strategie voor de digitale eengemaakte markt gewezen op de noodzaak van veilige verbonden producten en systemen en aangegeven dat door het opzetten van een Europees ICT-beveiligingskader met regels voor het organiseren van ICT-beveiligingscertificering in de Unie zowel het vertrouwen in het internet in stand kan worden gehouden als de huidige versnippering van de markt voor cyberbeveiliging kan worden aangepakt.

(50) Momenteel wordt de cyberbeveiligingscertificering van ICT-producten en -diensten slechts in beperkte mate gebruikt. Indien deze certificering bestaat, is dat meestal op het niveau van de lidstaten of in het kader van regelingen die op initiatief van het bedrijfsleven zijn opgezet. In deze context wordt een certificaat dat is afgegeven door een nationale cyberbeveiligingsautoriteit in principe niet erkend door andere lidstaten. Bijgevolg moeten bedrijven hun producten en diensten wellicht laten certificeren in de verschillende lidstaten waarin zij actief zijn, bijvoorbeeld met het oog op deelname aan nationale aanbestedingsprocedures. Er worden weliswaar nieuwe regelingen opgezet, maar er schijnt geen samenhangende en alomvattende benadering te zijn met betrekking tot horizontale kwesties inzake cyberbeveiliging, bijvoorbeeld op het gebied van het internet der dingen. Bestaande regelingen omvatten aanzienlijke tekortkomingen en verschillen wat betreft de producten waarop ze van toepassing zijn, de zekerheidsniveaus, de materiële criteria en de daadwerkelijke benutting.

(51) In het verleden zijn enige inspanningen gedaan om te komen tot wederzijdse erkenning van certificaten in Europa. Deze zijn echter slechts gedeeltelijk geslaagd. Het voornaamste voorbeeld daarvan is de overeenkomst inzake wederzijdse erkenning van de Groep van Hoge Ambtenaren voor de beveiliging van informatiesystemen (SOG-IS). Dit is weliswaar het belangrijkste model voor samenwerking en wederzijdse erkenning op het gebied van beveiligingscertificering, maar de overeenkomst inzake wederzijdse erkenning van SOG-IS heeft een aantal ernstige tekortkomingen in verband met de hoge kosten en de beperkte werkingssfeer. Tot dusver zijn er slechts enkele beschermingsprofielen voor digitale producten ontwikkeld, zoals de digitale handtekening, de digitale tachograaf en chipkaarten. Van groter belang is echter dat SOG-IS slechts een deel van de EU-lidstaten omvat. De doeltreffendheid van de overeenkomst inzake wederzijdse erkenning van SOG-IS is daardoor vanuit het oogpunt van de interne markt slechts beperkt.

(52) Gezien het bovenstaande is het noodzakelijk om een Europees kader voor cyberbeveiliging op te zetten waarin de voornaamste horizontale vereisten voor te ontwikkelen Europese regelingen voor cyberbeveiligingscertificering worden vastgesteld, en dat het mogelijk maakt dat certificaten voor ICT-producten en -diensten in alle lidstaten worden erkend en gebruikt. Het Europees kader moet een tweeledig doel hebben: enerzijds moet het bijdragen aan een groter vertrouwen in ICT-producten en -diensten die door middel van dergelijke regelingen zijn gecertificeerd, anderzijds moet het voorkomen dat er meerdere tegenstrijdige of elkaar overlappende nationale cyberbeveiligingscertificeringen bestaan, en zodoende zorgen voor lagere kosten voor ondernemingen die actief zijn op de digitale interne markt. De regelingen moeten niet-discriminerend zijn en zijn gebaseerd op internationale en/of EU-normen, tenzij dergelijke normen met het oog op het verwezenlijken van de desbetreffende legitieme EU-doelstellingen niet doeltreffend of niet passend zijn.

(53) De Commissie dient de bevoegdheid te krijgen om Europese regelingen voor cyberbeveiligingscertificering met betrekking tot bepaalde groepen van ICT-producten en –diensten vast te stellen. De uitvoering van en het toezicht op deze regelingen moeten worden verricht door de nationale autoriteiten voor certificeringstoezicht en de

in het kader van deze regelingen afgegeven certificaten moeten in de hele Unie geldig zijn en worden erkend. Certificeringsregelingen die door de branche of andere particuliere organisaties worden geïmplementeerd, moeten buiten het toepassingsgebied van de verordening vallen. De organisaties die dergelijke regelingen implementeren, kunnen de Commissie echter voorstellen deze in overweging te nemen als basis voor de verbetering ervan in de vorm van een Europese regeling.

(54) De bepalingen van deze verordening moeten EU-wetgeving waarbij specifieke regels voor de certificering van ICT-producten en -diensten zijn vastgesteld, onverlet laten. Met name omvat de algemene verordening gegevensbescherming bepalingen betreffende het instellen van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens met als doel het aantonen van de naleving van die verordening met betrekking tot verwerkingen door verwerkingsverantwoordelijken en verwerkers. Met behulp van dergelijke certificeringsmechanismen en gegevensbeschermingszegels en -merktekens kunnen betrokkenen beoordelen wat het beschermingsniveau van relevante producten en diensten is. De onderhavige verordening doet geen afbreuk aan de certificering van gegevensverwerkingen overeenkomstig de algemene verordening gegevensbescherming, ook niet als dergelijke verwerkingen zijn geïntegreerd in producten en diensten.

(55) Europese regelingen voor cyberbeveiligingscertificering moeten tot doel hebben te waarborgen dat ICT-producten en -diensten die door middel van een dergelijke regeling zijn gecertificeerd, aan gespecificeerde vereisten voldoen. Dergelijke vereisten hebben betrekking op het vermogen om op een bepaald zekerheidsniveau weerstand te bieden aan acties die erop zijn gericht de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of verzonden gegevens en de daaraan gerelateerde diensten die via deze producten, processen, diensten en systemen worden aangeboden of toegankelijk zijn, in gevaar te brengen. Het is niet mogelijk om in deze verordening de vereisten inzake cyberbeveiliging voor alle ICT-producten en -diensten in detail op te nemen. ICT-producten en -diensten en de daarmee verband houdende behoeften inzake cyberbeveiliging zijn zodanig uiteenlopend dat het zeer moeilijk is te voorzien in algemene, in alle gevallen geldende cyberbeveiligingsvoorschriften. Met het oog op certificering is daarom een breed en algemeen begrip van cyberbeveiliging noodzakelijk, aangevuld met een reeks specifieke doelstellingen inzake cyberbeveiliging waarmee rekening moet worden gehouden bij het opzetten van Europese regelingen voor cyberbeveiligingscertificering. De manier waarop deze doelstellingen zullen worden verwezenlijkt in specifieke ICT-producten en -diensten moet vervolgens nauwkeuring worden gespecificeerd op het niveau van de afzonderlijke, door de Commissie vastgestelde certificeringsregeling, bijvoorbeeld door middel van verwijzing naar normen of technische specificaties.

(56) De Commissie moet de bevoegdheid krijgen om het Enisa te vragen potentiële regelingen voor specifieke ICT-producten of -diensten voor te bereiden. De Commissie moet de bevoegdheid krijgen om vervolgens, op basis van de door het Enisa voorgestelde potentiële regeling, de Europese regeling voor cyberbeveiligingscertificering door middel van uitvoeringshandelingen vast te stellen. Rekening houdend met het algemene doel en de beveiligingsdoelstellingen die in deze verordening zijn opgenomen, moet in door de Commissie vastgestelde Europese regelingen voor cyberbeveiligingscertificering een minimale reeks elementen worden gespecificeerd die betrekking hebben op het onderwerp, het toepassingsgebied en de werking van de afzonderlijke regeling. Daartoe moeten onder meer het

toepassingsgebied en het onderwerp van de cyberbeveiligingscertificering behoren, met inbegrip van de betrokken categorieën ICT-producten en -diensten, de gedetailleerde specificatie van de eisen inzake cyberbeveiliging, bijvoorbeeld onder verwijzing naar de relevante normen of technische specificaties, de specifieke evaluatiecriteria en -methoden alsmede het beoogde zekerheidsniveau (dat wil zeggen basis, substantieel en/of hoog).

(57) De toepassing van Europese regelingen voor cyberbeveiligingscertificering moet vrijwillig blijven, tenzij anders is bepaald in EU-wetgeving of nationale wetgeving. Om de doelstellingen van deze verordening te verwezenlijken en de versnippering van de interne markt te vermijden, moeten nationale regelingen of procedures voor cyberbeveiligingscertificering voor de ICT-producten en -diensten die onder een Europese regeling voor cyberbeveiligingscertificering vallen, geen effect meer hebben vanaf de door de Commissie bij de uitvoeringshandeling vastgestelde datum. Bovendien moeten de lidstaten geen nieuwe nationale regelingen voor cyberbeveiligingscertificering invoeren die voorzien in cyberbeveiliging voor ICT-producten en -diensten die reeds onder een bestaande Europese regeling voor cyberbeveiligingscertificering vallen.

(58) Zodra een Europese regeling voor cyberbeveiligingscertificering is vastgesteld, moeten fabrikanten van ICT-producten of aanbieders van ICT-diensten bij een conformiteitsbeoordelingsinstantie van hun keuze een aanvraag indienen voor de certificering van hun producten of diensten. Conformiteitsbeoordelingsinstanties moeten door een accreditatie-instantie worden geaccrediteerd indien zij aan bepaalde, in deze verordening vastgestelde specifieke vereisten voldoen. De accreditatie moet worden afgegeven voor een maximumperiode van vijf jaar en kan onder dezelfde voorwaarden worden verlengd, mits de conformiteitsbeoordelingsinstantie aan de vereisten voldoet. Accreditatie-instanties moeten de accreditatie van een conformiteitsbeoordelingsinstantie intrekken wanneer niet of niet meer aan de voorwaarden voor de accreditatie wordt voldaan of wanneer door een conformiteitsbeoordelingsinstantie ondernomen acties indruisen tegen deze verordening.

(59) Alle lidstaten moeten worden verplicht om één autoriteit voor cyberbeveiligingscertificeringstoezicht aan te wijzen die erop toeziet dat de conformiteitsbeoordelingsinstanties en de door op hun grondgebied gevestigde conformiteitsbeoordelingsinstanties afgegeven certificaten voldoen aan de vereisten van deze verordening en de desbetreffende regelingen voor cyberbeveiligingscertificering. De nationale autoriteiten voor certificeringstoezicht moeten klachten van natuurlijke of rechtspersonen behandelen over certificaten die zijn afgegeven door op hun grondgebied gevestigde conformiteitsbeoordelingsinstanties, de inhoud van de klacht onderzoeken in de mate waarin dat gepast is, en de klager binnen een redelijke termijn in kennis stellen van de vooruitgang en het resultaat van het onderzoek. Verder moeten zij samenwerken met andere nationale autoriteiten voor certificeringstoezicht of andere overheidsinstanties, onder meer door uitwisseling van informatie over mogelijke niet-naleving door ICT-producten en -diensten van de vereisten van deze verordening of van specifieke regelingen voor cyberbeveiliging.

(60) Om de consistente toepassing van het Europees kader voor cyberbeveiligingscertificering te waarborgen moet een Europese Groep voor cyberbeveiligingscertificering ("de Groep") worden opgericht die is samengesteld uit de nationale autoriteiten voor certificeringstoezicht. De voornaamste taken van de

Groep moeten zijn: de Commissie adviseren en bijstaan bij haar werkzaamheden ter waarborging van een samenhangende uitvoering en toepassing van het Europees kader voor cyberbeveiligingscertificering, het Agentschap bijstaan en er nauw mee samenwerken bij de voorbereiding van potentiële regelingen voor cyberbeveiligingscertificering, aanbevelen dat de Commissie het Agentschap verzoekt om een potentiële Europese regeling voor cyberbeveiligingscertificering voor te bereiden, en aan de Commissie gerichte adviezen uitbrengen met betrekking tot het onderhoud en de herziening van bestaande Europese regelingen voor cyberbeveiligingscertificering.

(61) Om toekomstige EU-regelingen voor cyberbeveiliging onder de aandacht te brengen en de acceptatie ervan te bevorderen, kan de Europese Commissie algemene of sectorspecifieke richtsnoeren inzake cyberbeveiliging uitbrengen, bijv. betreffende goede praktijken op het gebied van cyberbeveiliging of verantwoordelijk cyberbeveiligingsgedrag, waarbij wordt gewezen op het gunstige effect van het gebruik van gecertificeerde ICT-producten en -diensten.

(62) Tot de steun die het Agentschap aan cyberbeveiligingscertificering verleent, moet ook overleg met het Beveiligingscomité van de Raad en het desbetreffende nationale orgaan behoren, wat betreft de cryptografische goedkeuring van in gerubriceerde netwerken te gebruiken producten.

(63) Om de criteria voor de accreditatie van conformiteitsbeoordelingsinstanties verder te specificeren, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 van het Verdrag betreffende de werking van de Europese Unie handelingen vast te stellen. Bij haar voorbereidende werkzaamheden moet de Commissie passend overleg plegen, onder meer op het niveau van de deskundigen. Dergelijke raadplegingen moeten worden uitgevoerd overeenkomstig de beginselen van het Interinstitutioneel Akkoord over beter wetgeven van 13 april 2016. Om met name te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen, moeten het Europees Parlement en de Raad alle documenten op hetzelfde moment ontvangen als de deskundigen van de lidstaten, en moeten hun deskundigen systematisch toegang hebben tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van gedelegeerde handelingen.

(64) Om te zorgen voor uniforme voorwaarden voor de tenuitvoerlegging van deze verordening dienen aan de Commissie uitvoeringsbevoegdheden te worden verleend waar dit in deze verordening is voorzien. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011.

(65) De onderzoeksprocedure moet worden toegepast voor de vaststelling van uitvoeringshandelingen inzake Europese regelingen voor cyberbeveiligingscertificering voor ICT-producten en -diensten, inzake modaliteiten betreffende door het Agentschap uit te voeren onderzoeken, alsmede voor de omstandigheden, formaten en procedures voor kennisgeving betreffende geaccrediteerde conformiteitsbeoordelingsinstanties door de nationale autoriteiten voor certificeringstoezicht aan de Commissie.

(66) Het optreden van het Agentschap moet aan een onafhankelijke evaluatie worden onderworpen. Deze evaluatie moet betrekking hebben op de verwezenlijking van de doelstellingen van het Agentschap, zijn werkmethoden en de relevantie van zijn taken. Bij de evaluatie moeten tevens de impact, de doeltreffendheid en de efficiëntie van het Europees kader voor cyberbeveiligingscertificering worden beoordeeld.

(67) Verordening (EU) nr. 526/2013 moet worden ingetrokken.

(68) Aangezien de doelstellingen van deze verordening niet voldoende door de lidstaten kunnen worden verwezenlijkt en beter op het niveau van de Unie kunnen worden gerealiseerd, kan de Unie maatregelen nemen overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat de verordening niet verder dan nodig is om dit doel te verwezenlijken,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

TITEL I
ALGEMENE BEPALINGEN

Artikel 1
Onderwerp en toepassingsgebied

Om de goede werking van de interne markt te waarborgen en tegelijkertijd te streven naar een hoog niveau van cyberbeveiliging, cyberweerbaarheid en vertrouwen binnen de Unie, wordt met deze verordening het volgende vastgesteld:

(a) de doelstellingen, taken en organisatorische aspecten van het Enisa, het "agentschap van de Europese Unie voor cyberbeveiliging", hierna "het Agentschap" genoemd; en

(b) een kader voor de vaststelling van Europese regelingen voor cyberbeveiligingscertificering met als doel het waarborgen van een toereikend cyberbeveiligingsniveau van ICT-producten en -diensten in de Unie. Dit kader is van toepassing onverminderd specifieke bepalingen inzake vrijwillige of verplichte certificering in andere handelingen van de Unie.

Artikel 2
Definities

Voor de toepassing van deze verordening wordt verstaan onder:

(1) "cyberbeveiliging": alle activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers daarvan en betrokken personen te beschermen tegen cyberdreigingen;

(2) "netwerk- en informatiesysteem": een systeem in de zin van artikel 4, punt 1), van Richtlijn (EU) 2016/1148;

(3) "nationale strategie voor de beveiliging van netwerk- en informatiesystemen": een kader in de zin van artikel 4, punt 3), van Richtlijn (EU) 2016/1148;

(4) "aanbieder van essentiële diensten": een publieke of private entiteit als bedoeld in artikel 4, punt 4), van Richtlijn (EU) 2016/1148;

(5) "digitaledienstverlener": elke rechtspersoon die een digitale dienst aanbiedt als bedoeld in artikel 4, punt 6), van Richtlijn (EU) 2016/1148;

(6) "incident": elke gebeurtenis als bedoeld in artikel 4, punt 7), van Richtlijn (EU) 2016/1148;

(7) "incidentenbehandeling": elke procedure als bedoeld in artikel 4, punt 8), van Richtlijn (EU) 2016/1148;

(8) "cyberdreiging": elke potentiële omstandigheid of gebeurtenis die schadelijk kan zijn voor netwerk- en informatiesystemen, de gebruikers daarvan en betrokken personen;

(9) "Europese regeling voor cyberbeveiligingscertificering": de uitvoerige reeks voorschriften, technische vereisten, normen en procedures die op EU-niveau zijn gedefinieerd en die van toepassing zijn op de certificering van producten en diensten op het gebied van informatie- en communicatietechnologie (ICT) die onder het toepassingsgebied van die specifieke regeling vallen;

(10) "Europees cyberbeveiligingscertificaat": een door een conformiteitsbeoordelingsinstantie afgegeven document dat bevestigt dat een bepaald ICT-product of een bepaalde ICT-dienst voldoet aan de specifieke, in een Europese regeling voor cyberbeveiligingscertificering vastgestelde vereisten;

(11) "ICT-product en -dienst": elk element of elke groep elementen van netwerk- en informatiesystemen;

(12) "accreditatie": accreditatie als bedoeld in artikel 2, punt 10, van Verordening (EG) nr. 765/2008;

(13) "nationale accreditatie-instantie": een nationale accreditatie-instantie als bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 765/2008;

(14) "conformiteitsbeoordeling": conformiteitsbeoordeling als bedoeld in artikel 2, punt 12, van Verordening (EG) nr. 765/2008;

(15) "conformiteitsbeoordelingsinstantie": een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;

(16) "norm": een norm als bedoeld in artikel 2, punt 1), van Verordening (EU) nr. 1025/2012.

TITEL II
Enisa – het "agentschap van de Europese Unie voor cyberbeveiliging"

HOOFDSTUK I
MANDAAT, DOELSTELLINGEN EN TAKEN

Artikel 3
Mandaat

1. Het Agentschap verricht de bij deze verordening aan hem toegewezen taken met als doel bij te dragen tot een hoog niveau van cyberbeveiliging binnen de Unie.
2. Het Agentschap verricht taken die hem worden toegedeeld bij EU-handelingen tot vaststelling van maatregelen voor de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die betrekking hebben op cyberbeveiliging.
3. De doelstellingen en taken van het Agentschap laten de bevoegdheden van de lidstaten betreffende cyberbeveiliging en in ieder geval de activiteiten op het gebied van openbare beveiliging, defensie, staatsveiligheid en activiteiten van de staat op het gebied van het strafrecht, onverlet.

Artikel 4
Doelstellingen

1. Het Agentschap is een expertisecentrum voor cyberbeveiliging door zijn onafhankelijkheid, de wetenschappelijke en technische kwaliteit van zijn advies en bijstand, de informatie die het verstrekt, de transparantie van zijn werkwijzen en -methoden, en de toewijding bij de uitvoering van zijn taken.
2. Het Agentschap verleent bijstand aan de EU-instellingen, -agentschappen en -organen alsmede aan de lidstaten bij de ontwikkeling en uitvoering van beleid inzake cyberbeveiliging.
3. Het Agentschap ondersteunt de capaciteitsopbouw en de paraatheid in de hele Unie door bijstand te verlenen aan de Unie, de lidstaten alsmede publieke en private belanghebbenden teneinde de bescherming van hun netwerk- en informatiesystemen te verbeteren, bij te dragen tot de ontwikkeling van vaardigheden en kennis op het gebied van cyberbeveiliging, en cyberweerbaarheid te kweken.
4. Het Agentschap bevordert de samenwerking en coördinatie op EU-niveau tussen de lidstaten, de EU-instellingen, -agentschappen en -organen, en relevante belanghebbenden, met inbegrip van de particuliere sector, betreffende kwesties op het gebied van cyberbeveiliging.
5. Het Agentschap zorgt ervoor dat de vermogens inzake cyberbeveiliging op EU-niveau worden versterkt als aanvulling op maatregelen van de lidstaten om cyberdreigingen te voorkomen en erop te reageren, met name in het geval van grensoverschrijdende incidenten.

6. Het Agentschap bevordert het gebruik van certificering, onder meer door bij te dragen aan de totstandbrenging en instandhouding van een kader voor cyberbeveiligingscertificering op EU-niveau overeenkomstig titel III van deze verordening, zodat de transparantie van de cyberbeveiligingszekerheid van ICT-producten en -diensten en daarmee het vertrouwen in de digitale interne markt worden versterkt.

7. Het Agentschap draagt ertoe bij dat burgers en bedrijven zich in grote mate bewust worden van kwesties op het gebied van cyberbeveiliging.

Artikel 5

Taken in verband met de ontwikkeling en uitvoering van EU-beleid en -wetgeving

Het Agentschap draagt bij tot de ontwikkeling en uitvoering van EU-beleid en -wetgeving door:

1. bijstand te verlenen en raad te geven, met name door het verstrekken van onafhankelijke adviezen en het verrichten van voorbereidende werkzaamheden, bij de ontwikkeling en herziening van EU-beleid en -wetgeving op het gebied van cyberbeveiliging en van sectorspecifieke beleids- en wetgevingsinitiatieven die verband houden met cyberbeveiliging;

2. de lidstaten bij te staan bij de consistente uitvoering van het EU-beleid en de EU-wetgeving inzake cyberbeveiliging, met name in verband met Richtlijn (EU) 2016/1148, onder meer door middel van adviezen, richtsnoeren, raadgeving en beste praktijken op gebieden als risicobeheer, melding van incidenten en uitwisseling van informatie, alsmede door bevordering van de uitwisseling van beste praktijken tussen op dat gebied bevoegde autoriteiten;

3. bij te dragen tot de werkzaamheden van de samenwerkingsgroep overeenkomstig artikel 11 van Richtlijn (EU) 2016/1148, door expertise en bijstand te verstrekken;

4. ondersteuning te bieden bij:

   (1) de ontwikkeling en uitvoering van EU-beleid op het gebied van elektronische identiteits- en vertrouwensdiensten, in het bijzonder door advies en technische richtsnoeren te verstrekken en de uitwisseling van beste praktijken tussen de bevoegde autoriteiten te bevorderen;

   (2) de bevordering van een verhoogd beveiligingsniveau van elektronische communicatie, onder meer door expertise en advies te verstrekken en de uitwisseling van beste praktijken tussen de bevoegde autoriteiten te bevorderen;

5. ondersteuning te bieden bij de regelmatige toetsing van EU-beleidsactiviteiten door jaarlijks verslag uit te brengen over de stand van uitvoering van het respectieve wettelijke kader voor:

   (a) de meldingen van incidenten die door de centrale contactpuntenvan iedere lidstaat worden ingediend bij de samenwerkingsgroep overeenkomstig artikel 10, lid 3, van Richtlijn (EU) 2016/1148;

   (b) de meldingen van inbreuken op beveiliging en integriteitsverlies die zijn ontvangen van verleners van vertrouwensdiensten, door de toezichthoudende

organen aan het Agentschap verstrekt overeenkomstig artikel 19, lid 3, van Verordening (EU) nr. 910/2014;

(c) de meldingen van inbreuken op beveiliging door ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten aanbieden, door de bevoegde autoriteiten aan het Agentschap verstrekt overeenkomstig artikel 40 van [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie].

Artikel 6

Taken in verband met capaciteitsopbouw

1. Het Agentschap verstrekt bijstand aan:

(a) de lidstaten bij hun inspanningen ter verbetering van de preventie, opsporing en analyse van problemen en incidenten betreffende cyberbeveiliging, alsmede het vermogen hierop te reageren, door hen te voorzien van de noodzakelijke kennis en expertise;

(b) de EU-instellingen, -organen, -instanties en -agentschappen bij hun inspanningen ter verbetering van de preventie, opsporing en analyse van problemen en incidenten betreffende cyberbeveiliging, alsmede het vermogen hierop te reageren, door middel van passende ondersteuning voor het CERT voor de EU-instellingen, -agentschappen en -organen (CERT-EU);

(c) de lidstaten, op hun verzoek, bij de ontwikkeling van nationale Computer Security Incident Response Teams (CSIRT's) overeenkomstig artikel 9, lid 5, van Richtlijn (EU) 2016/1148;

(d) de lidstaten, op hun verzoek, bij de ontwikkeling van nationale strategieën voor de beveiliging van netwerk- en informatiesystemen overeenkomstig artikel 7, lid 2, van Richtlijn (EU) 2016/1148; het Agentschap bevordert ook de verspreiding van die strategieën en volgt de voortgang van de uitvoering ervan in de hele Unie teneinde beste praktijken te bevorderen;

(e) de EU-instellingen bij de ontwikkeling en evaluatie van EU-strategieën inzake cyberbeveiliging, door de verspreiding van deze strategieën te bevorderen en de voortgang van de uitvoering ervan te volgen;

(f) de nationale CSIRT's en EU-CSIRT's bij het verhogen van het niveau van hun vermogens, onder meer door de dialoog en de informatie-uitwisseling te bevorderen, met als doel ervoor te zorgen dat iedere CSIRT, rekening houdend met de stand van de techniek, over een gemeenschappelijke set minimumvermogens beschikt en in overeenstemming met de beste praktijken te werk gaat;

(g) de lidstaten door jaarlijks grootschalige oefeningen op het gebied van cyberbeveiliging op EU-niveau te organiseren overeenkomstig artikel 7, lid 6, en door beleidsaanbevelingen te verstrekken op basis van de evaluatie van de oefeningen en de daaruit getrokken lessen;

(h) betrokken overheidsinstanties door opleidingen op het gebied van cyberbeveiliging aan te bieden, in voorkomend geval in samenwerking met belanghebbenden;

(i) de samenwerkingsgroep door beste praktijken uit te wisselen, met name voor de identificatie van aanbieders van essentiële diensten, onder meer wat betreft

grensoverschrijdende afhankelijkheid inzake risico's en -incidenten, overeenkomstig artikel 11, lid 3, onder l), van Richtlijn (EU) 2016/1148.

2. Het Agentschap vergemakkelijkt de oprichting van sectorale centra voor informatie-uitwisseling en -analyse (ISAC's) en zorgt voor permanente steun aan deze centra, met name in de in bijlage II bij Richtlijn (EU) 2016/1148 genoemde sectoren, door beste praktijken en richtsnoeren te verstrekken over beschikbare instrumenten en procedures, en over de manier waarop regelgevingsvraagstukken in verband met informatie-uitwisseling kunnen worden opgelost.

Artikel 7

Taken in verband met de operationele samenwerking op EU-niveau

1. Het Agentschap ondersteunt de operationele samenwerking tussen de bevoegde overheidsinstanties en tussen de belanghebbenden.

2. Het Agentschap werkt op operationeel niveau samen en brengt synergie-effecten tot stand met de EU-instellingen, -organen, -instanties en -agentschappen, met inbegrip van CERT-EU, de diensten die zich bezighouden met cybercriminaliteit, en de toezichthoudende autoriteiten die zich bezighouden met de bescherming van de persoonlijke levenssfeer en persoonsgegevens, met als doel gemeenschappelijke zorgpunten aan te pakken, onder meer door:

   (a) het uitwisselen van kennis en beste praktijken;

   (b) het verstrekken van advies en richtsnoeren over relevante kwesties in verband met cyberbeveiliging;

   (c) het vaststellen, na raadpleging van de Commissie, van praktische regelingen voor de uitvoering van specifieke taken.

3. Het Agentschap verzorgt het secretariaat van het CSIRT-netwerk overeenkomstig artikel 12, lid 2, van Richtlijn (EU) 2016/1148 en bevordert op actieve wijze de uitwisseling van informatie en de samenwerking tussen zijn leden.

4. Het Agentschap draagt bij aan de operationele samenwerking binnen het CSIRT-netwerk en ondersteunt de lidstaten door:

   (a) advies te verstrekken over de wijze waarop zij hun preventie-, opsporings- en responsvermogens ten aanzien van incidenten kunnen versterken;

   (b) op hun verzoek technische bijstand te verlenen in het geval van incidenten met aanzienlijke of substantiële gevolgen;

   (c) kwetsbaarheden, artefacten en incidenten te analyseren.

Bij de uitvoering van deze taken werken het Agentschap en CERT-EU op gestructureerde wijze samen om te kunnen profiteren van synergieën, met name met betrekking tot operationele aspecten.

5. Op verzoek van twee of meer betrokken lidstaten, en met als enig doel advies te verstrekken voor de preventie van toekomstige incidenten, ondersteunt of verricht het Agentschap een technisch ex-postonderzoek naar aanleiding van door de betrokken ondernemingen gemaakte meldingen van incidenten met aanzienlijke of substantiële gevolgen overeenkomstig Richtlijn (EU) 2016/1148. Het Agentschap verricht een dergelijk onderzoek ook op naar behoren gemotiveerd verzoek van de Commissie, in

overeenstemming met de betrokken lidstaten, indien dergelijke incidenten gevolgen hebben voor meer dan twee lidstaten.

Over de reikwijdte van het onderzoek en de bij het verrichten van een dergelijk onderzoek te volgen procedure wordt overeenstemming bereikt tuyssen de betrokken lidstaten en het Agentschap, onverminderd enig lopend strafrechtelijk onderzoek met betrekking tot hetzelfde incident. Het onderzoek wordt afgesloten met een technisch eindverslag dat door het Agentschap wordt opgesteld, met name op basis van informatie en opmerkingen die door de betrokken lidstaten en onderneming(en) zijn verstrekt en met de betrokken lidstaten zijn overeengekomen. Een samenvatting van het verslag, gericht op de aanbevelingen voor de preventie van toekomstige incidenten, wordt aan het CSIRT-netwerk ter beschikking gesteld.

6. Het Agentschap organiseert jaarlijkse cyberbeveiligingsoefeningen op EU-niveau en ondersteunt de EU-instellingen,- agentschappen en -organen op hun verzoek bij het organiseren van oefeningen. De jaarlijkse oefeningen op EU-niveau omvatten technische, operationele en strategische elementen en dragen bij tot de voorbereiding van de gezamenlijke reactie op EU-niveau op grootschalige grensoverschrijdende cyberbeveiligingsincidenten. Het Agentschap draagt in voorkomend geval ook bij tot sectorale cyberbeveiligingsoefeningen, en helpt deze te organiseren, samen met de betrokken ISAC's, en staat toe dat de ISAC's ook deelnemen aan cyberbeveiligingsoefeningen op EU-niveau.

7. Het Agentschap stelt regelmatig een technisch situatieverslag inzake de EU-cyberbeveiliging op met betrekking tot incidenten en dreigingen, waarbij het gebruikmaakt van publiek beschikbare informatie, eigen analyses en verslagen die ter beschikking worden gesteld door onder meer de CSIRT's van de lidstaten (op vrijwillige basis), de bij de NIS-richtlijn opgerichte centrale contactpunten (overeenkomstig artikel 14, lid 5, van de NIS-richtlijn), het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol en CERT-EU.

8. Het Agentschap draagt bij tot de ontwikkeling van een gezamenlijke respons, op het niveau van de Unie en van de lidstaten, op grootschalige grensoverschrijdende incidenten of crises in verband met cyberbeveiliging, met name door:

   (a) verslagen van nationale bronnen te bundelen om tot de totstandbrenging van een gemeenschappelijk situatiebewustzijn bij te dragen;

   (b) te zorgen voor een efficiënte informatiestroom en voor escalatiemechanismes tussen het CSIRT-netwerk en de technische en politieke besluitvormers op EU-niveau;

   (c) de technische afhandeling van een incident of crisis te ondersteunen, onder meer door de uitwisseling van technische oplossingen tussen de lidstaten te bevorderen;

   (d) de publieke communicatie in verband met het incident of de crisis te ondersteunen;

   (e) de samenwerkingsplannen wat betreft de reactie op dergelijke incidenten of crises te toetsen.

Artikel 8

Taken in verband met de markt, cyberbeveiligingscertificering en normalisatie

Het Agentschap:

(a) ondersteunt en bevordert de ontwikkeling en uitvoering van het EU-beleid inzake cyberbeveiligingscertificering van ICT-producten en -diensten, zoals vastgesteld in titel III van deze verordening, door:

(1) potentiële Europese regelingen voor cyberbeveiligingscertificering voor ICT-producten en -diensten overeenkomstig artikel 44 van deze verordening voor te bereiden;

(2) de Commissie bijstand te verlenen bij het verzorgen van het secretariaat voor de Europese Groep voor cyberbeveiligingscertificering overeenkomstig artikel 53 van deze verordening;

(3) richtsnoeren op te stellen en te publiceren en goede praktijken te ontwikkelen in verband met de cyberbeveiligingsvereisten van ICT-producten en -diensten, in samenwerking met de nationale autoriteiten voor certificeringstoezicht en de branche;

(b) bevordert de vaststelling en toepassing van Europese en internationale normen inzake risicobeheersing en inzake de beveiliging van ICT-producten en -diensten, en stelt in samenwerking met de lidstaten advies en richtsnoeren op met betrekking tot de technische gebieden die verband houden met de beveiligingseisen voor aanbieders van essentiële diensten en digitaledienstverleners, en met betrekking tot reeds bestaande normen, met inbegrip van nationale normen van de lidstaten, overeenkomstig artikel 19, lid 2, van Richtlijn (EU) 2016/1148;

(c) analyseert regelmatig de voornaamste tendensen op de markt voor cyberbeveiliging, zowel aan de vraag- als aan de aanbodzijde, en verspreidt deze analyses, teneinde de markt voor cyberbeveiliging in de Unie te stimuleren.

Artikel 9

Taken in verband met kennis, informatie en bewustmaking

Het Agentschap:

(a) verricht analyses van opkomende technologieën en verstrekt themaspecifieke beoordelingen betreffende de verwachte maatschappelijke, juridische, economische en regelgevende gevolgen van technologische innovaties voor cyberbeveiliging;

(b) verricht strategische langetermijnanalyses van cyberbeveiligingsdreigingen en -incidenten teneinde nieuwe trends te constateren en problemen in verband met cyberbeveiliging te voorkomen;

(c) verstrekt, in samenwerking met deskundigen van autoriteiten van de lidstaten , advies, richtsnoeren en beste praktijken voor de beveiliging van netwerk- en informatiesystemen, met name voor de beveiliging van internetinfrastructuur en de infrastructuurvoorzieningen die de in bijlage II bij Richtlijnen (EU) 2016/1148 genoemde sectoren ondersteunen;

(d) bundelt en organiseert door middel van een hiervoor bestemd portaal door de EU-instellingen, -agentschappen en -organen verstrekt informatie over cyberbeveiliging, en maakt deze openbaar;

(e) draagt bij tot de bewustmaking van het publiek omtrent risico's inzake cyberbeveiliging en verstrekt richtsnoeren inzake goede praktijken voor afzonderlijke gebruikers, gericht op burgers en organisaties;

(f) verzamelt en analyseert publiekelijk beschikbare informatie over significante incidenten, en stelt verslagen op met het oog op het verstrekken van richtsnoeren aan bedrijven en burgers in de hele Unie;

(g) organiseert, in samenwerking met de lidstaten en de EU-instellingen, -organen, -instanties en agentschappen, regelmatig publieke voorlichtingscampagnes teneinde de cyberbeveiliging en de zichtbaarheid ervan in de Unie te versterken.

Artikel 10

Taken in verband met onderzoek en innovatie

In verband met onderzoek en innovatie voert het Agentschap de volgende taken uit:

(a) advies verlenen aan de Unie en de lidstaten over onderzoeksbehoeften en prioriteiten op het gebied van cyberbeveiliging om doelmatig te kunnen reageren op bestaande en opkomende risico's en dreigingen, onder meer met betrekking tot nieuwe en opkomende informatie- en communicatietechnologieën, en om risicopreventietechnologieën doelmatig te kunnen gebruiken;

(b) deelnemen, wanneer de Commissie de desbetreffende bevoegdheden aan het Agentschap heeft gedelegeerd, aan de uitvoeringsfase van financieringsprogramma's voor onderzoek en innovatie, of als begunstigde.

Artikel 11

Taken in verband met internationale samenwerking

Het Agentschap draagt bij tot de inspanningen van de Unie om samen te werken met derde landen en internationale organisaties teneinde de internationale samenwerking op het gebied van cyberbeveiliging te bevorderen, door:

(a) betrokken te zijn, waar toepasselijk, als waarnemer bij en medeorganisator van internationale oefeningen, en de resultaten van dergelijke oefeningen te analyseren alsmede verslag daarover uit te brengen aan de raad van bestuur;

(b) op verzoek van de Commissie de uitwisseling van beste praktijken tussen de desbetreffende internationale organisaties te bevorderen;

(c) de Commissie, op verzoek, van expertise te voorzien.

HOOFDSTUK II
ORGANISATIE VAN HET AGENTSCHAP

Artikel 12
Structuur

De administratieve en beheersstructuur van het Agentschap is samengesteld uit:

(a) een raad van bestuur, die de in artikel 14 vastgestelde taken uitvoert;

(b) een dagelijks bestuur, dat de in artikel 18 vastgestelde taken uitvoert;

(c) een uitvoerend directeur, die de in artikel 19 genoemde verantwoordelijkheden draagt; en

(d) een permanente groep van belanghebbenden, die de in artikel 20 vastgestelde taken uitvoert.

AFDELING 1
RAAD VAN BESTUUR

Artikel 13
Samenstelling van de raad van bestuur

1. De raad van bestuur bestaat uit één vertegenwoordiger per lidstaat en twee door de Commissie benoemde vertegenwoordigers. Alle vertegenwoordigers hebben stemrecht.

2. Elk lid van de raad van bestuur heeft een plaatsvervanger om het lid te vertegenwoordigen in geval van afwezigheid.

3. De leden van de raad van bestuur en hun plaatsvervangers worden benoemd op grond van hun kennis op het gebied van cyberbeveiliging, met inachtneming van hun relevante bestuurlijke, administratieve en budgettaire vaardigheden. De Commissie en de lidstaten spannen zich ter wille van de continuïteit van het werk van de raad van bestuur in om het verloop onder hun vertegenwoordigers in de raad van bestuur te beperken. De Commissie en de lidstaten streven naar een evenwichtige deelname van mannen en vrouwen in de raad van bestuur.

4. De ambtstermijn van de leden van de raad van bestuur en hun plaatsvervangers bedraagt vier jaar. Die termijn kan worden verlengd.

Artikel 14
Functies van de raad van bestuur

1. De raad van bestuur:

   (a) bepaalt de algemene opzet van de werkzaamheden van het Agentschap en ziet erop toe dat de werkzaamheden van het Agentschap in overeenstemming zijn met de in deze verordening vastgestelde regels en beginselen. Ook zorgt de raad van bestuur voor samenhang tussen de werkzaamheden van het Agentschap en de activiteiten op het niveau van de lidstaten en de Unie;

(b) stelt het in artikel 21 bedoelde ontwerp van het enig programmeringsdocument van het Agentschap vast, voordat het bij de Commissie ter advies wordt ingediend;

(c) stelt, rekening houdend met het advies van de Commissie, het enig programmeringsdocument van het Agentschap vast met een tweederdemeerderheid van zijn leden en in overeenstemming met artikel 17;

(d) stelt met een tweederdemeerderheid van zijn leden de jaarbegroting van het Agentschap vast en oefent andere functies uit met betrekking tot de begroting van het Agentschap overeenkomstig hoofdstuk III;

(e) beoordeelt het geconsolideerde jaarverslag over de activiteiten van het Agentschap en keurt het goed, en doet het verslag en zijn beoordeling daarvan uiterlijk op 1 juli van het volgende jaar toekomen aan het Europees Parlement, de Raad, de Commissie en de Rekenkamer. Het jaarverslag bevat de rekeningen en beschrijft hoe het Agentschap zijn prestatie-indicatoren heeft nageleefd. Dit jaarverslag wordt openbaar gemaakt;

(f) stelt overeenkomstig artikel 29 de financiële regels vast die van toepassing zijn op het Agentschap;

(g) stelt een fraudebestrijdingsstrategie vast die in verhouding staat tot de frauderisico's, rekening houdend met een kosten-batenanalyse van de uit te voeren maatregelen;

(h) stelt regels vast voor de preventie en beheersing van belangenconflicten met betrekking tot zijn leden;

(i) zorgt voor adequate follow-up van de bevindingen en aanbevelingen die voortkomen uit onderzoeken van het Europees Bureau voor fraudebestrijding (OLAF) en de diverse interne of externe auditverslagen en evaluaties;

(j) stelt zijn reglement van orde vast;

(k) oefent, overeenkomstig lid 2, ten aanzien van het personeel van het Agentschap de bevoegdheden uit die het Statuut van de ambtenaren van de Europese Unie toekent aan het tot aanstelling bevoegde gezag en die de regeling welke van toepassing is op de andere personeelsleden van de Unie toekent aan het tot het sluiten van contracten bevoegde gezag (hierna "de bevoegdheden van het tot aanstelling bevoegde gezag" genoemd);

(l) stelt overeenkomstig de procedure van artikel 110 van het Statuut voorschriften op voor de toepassing van het Statuut en van de Regeling die van toepassing is op de andere personeelsleden;

(m) benoemt de uitvoerend directeur en, indien relevant, verlengt zijn ambtstermijn of ontheft hem uit zijn functie overeenkomstig artikel 33 van deze verordening;

(n) benoemt een rekenplichtige, die de rekenplichtige van de Commissie kan zijn en die volledig onafhankelijk is bij de uitvoering van zijn taken;

(o) neemt alle beslissingen in verband met het opzetten van de interne structuren van het Agentschap en, waar nodig, de wijziging ervan, rekening houdend met de activiteitenbehoeften van het Agentschap en met het oog op een gezond begrotingsbeheer;

(p) geeft machtiging tot het sluiten van werkafspraken overeenkomstig de artikelen 7 en 39.

2. De raad van bestuur neemt overeenkomstig artikel 110 van het Statuut een beslissing die is gebaseerd op artikel 2, lid 1, van het Statuut en artikel 6 van de Regeling die van toepassing is op de andere personeelsleden, waarin hij de nodige bevoegdheden van het tot aanstelling bevoegde gezag delegeert aan de uitvoerend directeur en de voorwaarden vastlegt voor de opschorting van deze gedelegeerde bevoegdheden. De uitvoerend directeur kan deze bevoegdheden op zijn beurt delegeren.

3. Wanneer uitzonderlijke omstandigheden dat vereisen, kan de raad van bestuur door middel van een besluit de delegatie van de bevoegdheden van het tot aanstelling bevoegde gezag aan de uitvoerend directeur en de bevoegdheden die deze laatste op zijn beurt heeft gedelegeerd, tijdelijk opschorten en deze bevoegdheden zelf uitoefenen of delegeren aan een van zijn leden of aan een ander personeelslid dan de uitvoerend directeur.

Artikel 15
Voorzitter van de raad van bestuur

De raad van bestuur kiest met een tweederdemeerderheid van zijn leden uit zijn midden een voorzitter en een vicevoorzitter voor een periode van vier jaar, die éénmaal kan worden verlengd. Indien tijdens hun ambtstermijn hun lidmaatschap van de raad van bestuur echter eindigt, loopt hun ambtstermijn op dezelfde datum als die van deze eindiging automatisch af. De vicevoorzitter vervangt ambtshalve de voorzitter wanneer deze is verhinderd zijn taken te verrichten.

Artikel 16
Vergaderingen van de raad van bestuur

1. De raad van bestuur wordt door de voorzitter in vergadering bijeengeroepen.

2. De raad van bestuur houdt ten minste twee gewone vergaderingen per jaar. Op verzoek van de voorzitter, van de Commissie of van ten minste een derde van zijn leden belegt de raad van bestuur ook buitengewone vergaderingen.

3. De uitvoerend directeur neemt zonder stemrecht deel aan de vergaderingen van de raad van bestuur.

4. Op uitnodiging van de voorzitter kunnen leden van de permanente groep van belanghebbenden zonder stemrecht deelnemen aan de vergaderingen van de raad van bestuur.

5. De leden van de raad van bestuur en hun plaatsvervangers kunnen zich overeenkomstig de bepalingen van het reglement van orde tijdens de vergaderingen laten bijstaan door adviseurs of deskundigen.

6. Het Agentschap vervult de secretariaatstaken voor de raad van bestuur.

Artikel 17

Stemprocedure in de raad van bestuur

1. De raad van bestuur neemt besluiten met meerderheid van de leden.
2. Voor de vaststelling van het enig programmeringsdocument en de jaarlijkse begroting alsmede voor de benoeming, de verlenging van de ambtstermijn of de ambtsontheffing van de uitvoerend directeur, is een tweederdemeerderheid van alle leden van de raad van bestuur vereist.
3. Elk lid heeft één stem. Bij afwezigheid van een lid is zijn plaatsvervanger gerechtigd diens stemrecht uit te oefenen.
4. De voorzitter neemt aan de stemming deel.
5. De uitvoerend directeur neemt niet aan de stemming deel.
6. In het reglement van orde van de raad van bestuur wordt de stemprocedure nader uitgewerkt, met name betreffende de gevallen waarin een lid mag handelen namens een ander lid.

AFDELING 2
DAGELIJKS BESTUUR

Artikel 18

Dagelijks bestuur

1. De raad van bestuur wordt bijgestaan door een dagelijks bestuur.
2. Het dagelijks bestuur:
   (a) stelt de besluiten op die ter goedkeuring aan de raad van bestuur worden voorgelegd;
   (b) zorgt samen met de raad van bestuur voor adequate follow-up van de bevindingen en aanbevelingen die voortkomen uit onderzoeken van OLAF en de diverse interne of externe auditverslagen en evaluaties;
   (c) assisteert en adviseert, onverminderd de in artikel 19 genoemde verantwoordelijkheden van de uitvoerend directeur, de uitvoerend directeur bij de uitvoering van de besluiten van de raad van bestuur aangaande administratieve en budgettaire aangelegenheden;
3. Het dagelijks bestuur bestaat uit vijf uit de raad van bestuur benoemde leden, onder wie de voorzitter van de raad van bestuur, die ook het dagelijks bestuur kan voorzitten, en een van de vertegenwoordigers van de Commissie. De uitvoerend directeur neemt deel aan de vergaderingen van het dagelijks bestuur, maar heeft geen stemrecht.
4. De ambtstermijn van de leden van het dagelijks bestuur bedraagt vier jaar. Die termijn kan worden verlengd.
5. Het dagelijks bestuur vergadert ten minste eens in de drie maanden. De voorzitter van het dagelijks bestuur belegt aanvullende vergaderingen op verzoek van de leden ervan.
6. De raad van bestuur stelt het reglement van orde van het dagelijks bestuur vast.

7. Indien nodig wegens hoogdringendheid kan het dagelijks bestuur namens de raad van bestuur bepaalde voorlopige besluiten nemen, met name op het gebied van administratief beheer, met inbegrip van de opschorting van de delegatie van de bevoegdheden van het tot aanstelling bevoegde gezag en begrotingskwesties.

AFDELING 3
UITVOEREND DIRECTEUR

Artikel 19
Verantwoordelijkheden van de uitvoerend directeur

1. Het Agentschap wordt geleid door de uitvoerend directeur, die onafhankelijk is in de uitvoering van zijn taken. De uitvoerend directeur legt verantwoording af aan de raad van bestuur.

2. De uitvoerend directeur brengt desgevraagd verslag uit aan het Europees Parlement over de uitvoering van zijn taken. De Raad kan de uitvoerend directeur verzoeken verslag uit te brengen over de uitvoering van zijn taken.

3. De uitvoerend directeur is verantwoordelijk voor:

   (a) het dagelijks leiden van het Agentschap;

   (b) het uitvoeren van de besluiten van de raad van bestuur;

   (c) het opstellen van het enig programmeringsdocument en het indienen ervan bij de raad van bestuur voordat het bij de Commissie wordt ingediend;

   (d) het uitvoeren van het enig programmeringsdocument en het uitbrengen van verslag erover aan de raad van bestuur;

   (e) het voorbereiden van het geconsolideerde jaarverslag over de activiteiten van het Agentschap en het ter beoordeling en goedkeuring ervan indienen bij de raad van bestuur;

   (f) het opstellen van een actieplan voor de follow-up van de conclusies van de beoordelingen achteraf, en het elke twee jaar uitbrengen van verslag aan de Commissie over de geboekte vooruitgang;

   (g) het opstellen van een actieplan voor de follow-up van de conclusies van interne of externe auditverslagen, alsook van onderzoeken van het Europees Bureau voor fraudebestrijding (OLAF), en verslag uitbrengen over de geboekte vooruitgang, twee maal per jaar aan de Commissie en op regelmatige tijdstippen aan de raad van bestuur;

   (h) het opstellen van een ontwerp van financiële regeling die van toepassing is op het Agentschap;

   (i) het opstellen van de ontwerpraming van ontvangsten en uitgaven van het Agentschap en het uitvoeren van de begroting van het Agentschap;

   (j) het beschermen van de financiële belangen van de Unie door maatregelen ter voorkoming van fraude, corruptie en andere onwettige activiteiten toe te passen, controles te verrichten en,

wanneer er onregelmatigheden worden ontdekt, ten onrechte betaalde bedragen terug te vorderen en desgevallend effectieve, evenredige en afschrikkende administratieve en geldelijke sancties op te leggen;

(k) het opstellen van een fraudebestrijdingsstrategie voor het Agentschap en het ter goedkeuring ervan voorleggen aan de raad van bestuur;

(l) het leggen en onderhouden van contacten met het bedrijfsleven en consumentenorganisaties om een regelmatige dialoog met de belanghebbenden te waarborgen;

(m) andere taken waarmee de uitvoerend directeur krachtens deze verordening is belast.

4. Indien dit noodzakelijk is, binnen het mandaat van het Agentschap valt en in overeenstemming is met de doelstellingen en taken van het Agentschap, kan de uitvoerend directeur ad-hocwerkgroepen oprichten, samengesteld uit deskundigen, onder meer van de bevoegde autoriteiten van de lidstaten. De raad van bestuur wordt daarvan van tevoren in kennis gesteld. De procedures betreffende met name de samenstelling van de werkgroepen, de benoeming van de deskundigen van de werkgroepen door de uitvoerend directeur en de werkwijze van de werkgroepen worden in het huishoudelijk reglement van het Agentschap vastgesteld.

5. De uitvoerend directeur beslist of het voor de efficiënte en doeltreffende uitvoering van de taken van het Agentschap noodzakelijk is personeelsleden in een of meer lidstaten onder te brengen. Voordat de uitvoerend directeur besluit een lokaal kantoor op te richten, verkrijgt hij daarvoor voorafgaande toestemming van de Commissie, de raad van bestuur en de betrokken lidstaat of lidstaten. In het besluit wordt het toepassingsgebied van de in dat lokale kantoor te verrichten activiteiten omschreven, op zodanige wijze dat onnodige kosten en verdubbeling van administratieve functies van het Agentschap worden vermeden. Wanneer passend of vereist, wordt een overeenkomst met de betrokken lidstaat of lidstaten gesloten.

AFDELING 4
PERMANENTE GROEP VAN BELANGHEBBENDEN

Artikel 20
Permanente groep van belanghebbenden

1. De raad van bestuur richt, op voorstel van de uitvoerend directeur, een permanente groep van belanghebbenden op, samengesteld uit erkende deskundigen die de relevante belanghebbenden vertegenwoordigen, zoals de ICT-industrie, aanbieders van openbare elektronische communicatienetwerken of -diensten, consumentenorganisaties, universitaire deskundigen op het gebied van cyberbeveiliging en vertegenwoordigers van krachtens [richtlijn tot vaststelling van het Europees wetboek voor elektronische communicatie] aangemelde bevoegde autoriteiten, alsook autoriteiten op het gebied van rechtshandhaving en toezichthoudende autoriteiten op het gebied van gegevensbescherming.

2. Procedures voor de permanente groep van belanghebbenden, met name betreffende het aantal, de samenstelling en de benoeming van zijn leden door de raad van

bestuur, het voorstel van de uitvoerend directeur en de werking van de groep, worden in het huishoudelijk reglement van het Agentschap vastgesteld en gepubliceerd.

3. De permanente groep van belanghebbenden wordt voorgezeten door de uitvoerend directeur of door een andere persoon die door de uitvoerend directeur per geval wordt benoemd.

4. De ambtstermijn van de leden van de permanente groep van belanghebbenden bedraagt tweeënhalf jaar. Leden van de raad van bestuur kunnen geen lid zijn van de permanente groep van belanghebbenden. Deskundigen van de Commissie en van de lidstaten mogen de vergaderingen van de permanente groep van belanghebbenden bijwonen en aan de werkzaamheden ervan deelnemen. Vertegenwoordigers van andere door de uitvoerend directeur relevant geachte organen, die geen lid zijn van de permanente groep van belanghebbenden, mogen worden uitgenodigd op de vergaderingen van de permanente groep van belanghebbenden en deelnemen aan de werkzaamheden ervan.

5. De permanente groep van belanghebbenden adviseert het Agentschap met betrekking tot de uitvoering van zijn activiteiten. De permanente groep van belanghebbenden adviseert met name de uitvoerend directeur met betrekking tot de opstelling van een voorstel voor het werkprogramma van het Agentschap en met betrekking tot de communicatie met de relevante belanghebbenden over alle met het werkprogramma verband houdende kwesties.

AFDELING 5
WERKING

Artikel 21
Enig programmeringsdocument

1. Het Agentschap voert zijn werkzaamheden uit overeenkomstig een enig programmeringsdocument, bestaande uit een meerjarige en jaarlijkse programmering, dat alle geplande activiteiten van het Agentschap bevat.

2. Elk jaar stelt de uitvoerend directeur overeenkomstig artikel 32 van Gedelegeerde Verordening (EU) nr. 1271/2013 van de Commissie[36] een ontwerp van het enig programmeringsdocument op dat de meerjarige en jaarlijkse programmering met de bijbehorende planning van personele en financiële middelen bevat, rekening houdend met de richtsnoeren van de Commissie.

3. De raad van bestuur stelt elk jaar uiterlijk op 30 november het in lid 1 bedoelde enig programmeringsdocument vast en stuurt het uiterlijk op 31 januari van het jaar daarna toe aan het Europees Parlement, de Raad en de Commissie; dit gebeurt ook met alle daarna bijgewerkte versies van dat document.

---

36 Gedelegeerde Verordening (EU) nr. 1271/2013 van de Commissie van 30 september 2013 houdende de financiële kaderregeling van de organen, bedoeld in artikel 208 van Verordening (EU, Euratom) nr. 966/2012 van het Europees Parlement en de Raad (PB L 328 van 7.12.2013, blz. 42).

4. Het enig programmeringsdocument wordt definitief na de definitieve vaststelling van de algemene begroting van de Unie en wordt, indien nodig, dienovereenkomstig aangepast.

5. Het jaarlijkse werkprogramma bevat gedetailleerde doelstellingen en de beoogde resultaten, met inbegrip van prestatie-indicatoren. Het bevat voorts een beschrijving van de te financieren acties en een indicatie van de financiële en personele middelen die aan iedere actie worden toegewezen overeenkomstig de beginselen betreffende activiteitsgestuurde begroting en beheer. Het jaarlijkse werkprogramma is consistent met het in lid 7 bedoelde meerjarige werkprogramma. Het vermeldt duidelijk de taken die zijn toegevoegd, gewijzigd of geschrapt ten opzichte van het vorige begrotingsjaar.

6. De raad van bestuur past het vastgestelde jaarlijkse werkprogramma aan wanneer een nieuwe taak aan het Agentschap wordt toegewezen. Iedere wezenlijke wijziging van het jaarlijkse werkprogramma wordt vastgesteld door middel van dezelfde procedure als die welke voor het oorspronkelijke jaarlijkse werkprogramma geldt. De raad van bestuur kan aan de uitvoerend directeur de bevoegdheid delegeren om niet-wezenlijke wijzigingen door te voeren in het jaarlijkse werkprogramma.

7. Het meerjarige werkprogramma omvat een beschrijving van de algemene strategische programmering, met inbegrip van de doelstellingen, beoogde resultaten en prestatie-indicatoren. Het behelst ook de programmering van de middelen, met inbegrip van de meerjarige begroting en de personele middelen.

8. Deze programmering van de middelen wordt jaarlijks bijgewerkt. De strategische programmering wordt in voorkomend geval geactualiseerd, met name indien zulks nodig is om rekening te houden met de resultaten van de in artikel 56 bedoelde evaluatie.

Artikel 22
Belangenverklaring

1. De leden van de raad van bestuur, de uitvoerend directeur en de door de lidstaten op tijdelijke basis gedetacheerde ambtenaren leggen elk een verklaring over hun verplichtingen en een verklaring over hun belangen af waaruit blijkt dat zij wel of geen directe of indirecte belangen hebben die als nadelig voor hun onafhankelijkheid kunnen worden beschouwd. De verklaringen zijn accuraat en volledig, en worden jaarlijks schriftelijk afgelegd en telkens wanneer dat nodig is geactualiseerd.

2. De leden van de raad van bestuur, de uitvoerend directeur en de externe deskundigen die deelnemen aan ad-hocwerkgroepen leggen elk uiterlijk aan het begin van elke vergadering een nauwkeurige en volledige verklaring af over belangen die met betrekking tot de agendapunten als nadelig voor hun onafhankelijkheid zouden kunnen worden beschouwd, en nemen niet deel aan de bespreking van en de stemming over die punten.

3. Het Agentschap legt in zijn huishoudelijk reglement de praktische regelingen voor de toepassing van de in de leden 1 en 2 bedoelde bepalingen inzake belangenverklaring vast.

Artikel 23

Transparantie

1. Het Agentschap voert zijn activiteiten uit met een hoog niveau van transparantie en overeenkomstig artikel 25.

2. Het Agentschap ziet erop toe dat geïnteresseerden en alle belanghebbenden van passende, objectieve, betrouwbare en gemakkelijk toegankelijke informatie worden voorzien, in het bijzonder met betrekking tot de resultaten van zijn werkzaamheden. Tevens maakt het de overeenkomstig artikel 22 afgelegde belangenverklaringen openbaar.

3. De raad van bestuur kan op voorstel van de uitvoerend directeur belanghebbenden toestemming geven om de uitvoering van sommige activiteiten van het Agentschap als waarnemer bij te wonen.

4. Het Agentschap legt in zijn huishoudelijk reglement de praktische regelingen voor de toepassing van de in de leden 1 en 2 bedoelde transparantiebepalingen vast.

Artikel 24

Vertrouwelijkheid

1. Onverminderd artikel 25 onthult het Agentschap aan derden geen verwerkte of ontvangen informatie waarvoor een met redenen omkleed verzoek om gehele of gedeeltelijke vertrouwelijke behandeling is ingediend.

2. De leden van de raad van bestuur, de uitvoerend directeur, de leden van de permanente groep van belanghebbenden, de externe deskundigen die deelnemen aan ad-hocwerkgroepen en de personeelsleden van het Agentschap, met inbegrip van de door de lidstaten tijdelijk gedetacheerde ambtenaren, leven na het beëindigen van hun functie de geheimhoudingsplicht uit hoofde van artikel 339 van het Verdrag betreffende de werking van de Europese Unie (VWEU) na.

3. Het Agentschap legt in zijn huishoudelijk reglement de praktische regelingen voor de toepassing van de in de leden 1 en 2 bedoelde vertrouwelijkheidsregels vast.

4. Indien dat voor de verrichting van de taken van het Agentschap noodzakelijk is, besluit de raad van bestuur het Agentschap toestemming te geven om gerubriceerde informatie te verwerken. In dat geval stelt de raad van bestuur, in overleg met de diensten van de Commissie, een huishoudelijk reglement vast waarbij de veiligheidsbeginselen van Besluit (EU, Euratom) 2015/443[37] en Besluit (EU, Euratom) 2015/444[38] worden toegepast. Dit reglement omvat onder meer bepalingen betreffende de uitwisseling, de verwerking en de opslag van gerubriceerde gegevens.

---

37 Besluit (EU, Euratom) 2015/443 van de Commissie van 13 maart 2015 betreffende veiligheid binnen de Commissie (PB L 72 van 17.3.2015, blz. 41).

38 Besluit (EU, Euratom) 2015/444 van de Commissie van 13 maart 2015 betreffende de veiligheidsvoorschriften voor de bescherming van gerubriceerde EU-informatie (PB L 72 van 17.3.2015, blz. 53).

Artikel 25

Toegang tot documenten

1. Op documenten die in het bezit zijn van het Agentschap is Verordening (EG) nr. 1049/2001 van toepassing.

2. De raad van bestuur stelt binnen zes maanden na de oprichting van het Agentschap regelingen voor de uitvoering van Verordening (EG) nr. 1049/2001 vast.

3. Tegen besluiten van het Agentschap uit hoofde van artikel 8 van Verordening (EG) nr. 1049/2001 kan een klacht bij de ombudsman worden ingediend uit hoofde van artikel 228 VWEU of een beroep bij het Hof van Justitie van de Europese Unie worden ingesteld uit hoofde van artikel 263 VWEU.

HOOFDSTUK III
OPSTELLING EN STRUCTUUR VAN DE BEGROTING

Artikel 26

Opstelling van de begroting

1. De uitvoerend directeur stelt jaarlijks een ontwerpraming op van de ontvangsten en uitgaven van het Agentschap voor het volgende begrotingsjaar en zendt die, tezamen met een ontwerpoverzicht van de personeelsformatie, aan de raad van bestuur. De ontvangsten en uitgaven moeten in evenwicht zijn.

2. De raad van bestuur stelt jaarlijks de raming van de ontvangsten en uitgaven van het Agentschap voor het volgende begrotingsjaar vast op basis van de in lid 1 bedoelde opgestelde ontwerpraming van de ontvangsten en uitgaven.

3. Uiterlijk op 31 januari van elk jaar stuurt de raad van bestuur de in artikel 2 bedoelde raming, die deel uitmaakt van het ontwerp van het enig programmeringsdocument, naar de Commissie en de derde landen waarmee de Unie overeenkomstig artikel 39 een overeenkomst heeft gesloten.

4. Op basis van deze raming voert de Commissie in het ontwerp van algemene begroting van de Europese Unie, dat zij overeenkomstig de artikelen 313 en 314 VWEU bij het Europees Parlement en de Raad indient, de ramingen op die zij nodig acht voor het overzicht van de personeelsformatie en voor de bijdrage ten laste van de algemene begroting.

5. Het Europees Parlement en de Raad keuren de kredieten voor de bijdrage aan het Agentschap goed.

6. Het Europees Parlement en de Raad stellen de personeelsformatie van het Agentschap vast.

7. De raad van bestuur stelt, samen met het enig programmeringsdocument, de begroting van het Agentschap vast. De begroting wordt definitief na de definitieve vaststelling van de algemene begroting van de Unie. Voor zover van toepassing past de raad van bestuur de begroting en het enig programmeringsdocument van het Agentschap aan in overeenstemming met de algemene begroting van de Unie.

Artikel 27

Structuur van de begroting

1. Onverminderd andere middelen zijn de ontvangsten van het Agentschap samengesteld uit:

   (a) een bijdrage uit de begroting van de Unie;

   (b) bestemmingsontvangsten voor de financiering van specifieke uitgaven in overeenstemming met de in artikel 29 bedoelde financiële regeling;

   (c) financiering van de Unie in de vorm van delegatieovereenkomsten of ad-hocsubsidies in overeenstemming met de in artikel 29 bedoelde financiële regeling en met de bepalingen van de relevante instrumenten die het beleid van de Unie ondersteunen;

   (d) bijdragen van derde landen die aan de werkzaamheden van het Agentschap deelnemen op grond van artikel 39;

   (e) eventuele vrijwillige bijdragen in geld of in natura van de lidstaten; Lidstaten die vrijwillig bijdragen, kunnen geen aanspraak maken op specifieke rechten of diensten op grond daarvan.

2. De uitgaven van het Agentschap hebben betrekking op het personeel, administratieve en technische ondersteuning, infrastructuur, werkingskosten en uitgaven die voortvloeien uit contracten met derden.

Artikel 28

Uitvoering van de begroting

1. De uitvoerend directeur is verantwoordelijk voor de uitvoering van de begroting van het Agentschap.

2. De interne controleur van de Commissie heeft ten aanzien van het Agentschap dezelfde bevoegdheden als ten aanzien van de diensten van de Commissie.

3. Uiterlijk op 1 maart van het jaar dat volgt op elk begrotingsjaar (1 maart van jaar N + 1) dient de rekenplichtige van het Agentschap de voorlopige rekeningen in bij de rekenplichtige van de Commissie en bij de Rekenkamer.

4. Na ontvangst van de opmerkingen van de Rekenkamer over de voorlopige rekeningen van het Agentschap maakt de rekenplichtige van het Agentschap onder eigen verantwoordelijkheid de definitieve rekeningen van het Agentschap op.

5. De uitvoerend directeur dient de definitieve rekeningen voor advies in bij de raad van bestuur.

6. Uiterlijk op 31 maart van het jaar N + 1 zendt de uitvoerend directeur het verslag over het budgettair en financieel beheer toe aan het Europees Parlement, de Raad, de Commissie en de Rekenkamer.

7. Uiterlijk op 1 juli van jaar N + 1 zendt de rekenplichtige de definitieve rekeningen en het advies van de raad van bestuur toe aan het Europees Parlement, de Raad, de rekenplichtige van de Commissie en de Rekenkamer.

8. Tegelijkertijd met de toezending van de definitieve rekeningen zendt de rekenplichtige aan de Rekenkamer een begeleidende brief betreffende die definitieve rekeningen toe, alsmede een kopie daarvan aan de rekenplichtige van de Commissie.

9. De uitvoerend directeur publiceert de definitieve rekeningen uiterlijk op 15 november van het volgende jaar.

10. De uitvoerend directeur stuurt uiterlijk op 30 september van jaar N + 1 aan de Rekenkamer een antwoord op diens opmerkingen, alsmede een kopie daarvan aan de raad van bestuur en de Commissie.

11. De uitvoerend directeur verstrekt het Europees Parlement op verzoek, overeenkomstig het bepaalde in artikel 165, lid 3, van het Financieel Reglement, alle inlichtingen die nodig zijn voor het goede verloop van de kwijtingsprocedure voor het betrokken begrotingsjaar.

12. Het Europees Parlement verleent op aanbeveling van de Raad vóór 15 mei van jaar N + 2 aan de uitvoerend directeur kwijting inzake de uitvoering van de begroting van het jaar N.

Artikel 29
Financiële regeling

De financiële regeling die van toepassing is op het Agentschap wordt vastgesteld door de raad van bestuur, na raadpleging van de Commissie. Deze regeling wijkt niet af van Gedelegeerde Verordening (EU) nr. 1271/2013 tenzij dit in verband met de werking van het Agentschap specifiek vereist is en de Commissie vooraf toestemming heeft verleend.

Artikel 30
Fraudebestrijding

1. Om de bestrijding van fraude, corruptie en andere illegale handelingen als bedoeld in Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad[39] te bevorderen, treedt het Agentschap binnen zes maanden na de datum waarop het operationeel is geworden toe tot het Interinstitutioneel Akkoord van 25 mei 1999 betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF) en stelt het de geschikte, voor alle werknemers van het Agentschap geldende bepalingen vast volgens het model van de bijlage bij dat akkoord.

2. De Rekenkamer is bevoegd om bij alle begunstigden van subsidies, contractanten en subcontractanten die van het Agentschap middelen van de Unie hebben ontvangen, controles op stukken of controles ter plaatse te verrichten.

3. OLAF kan overeenkomstig de bepalingen en procedures van Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad en Verordening (Euratom, EG) nr. 2185/96 van de Raad[40] van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Unie tegen fraudes en andere onregelmatigheden controles en verificaties ter plaatse verrichten om vast te stellen

[39] Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 11 september 2013 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) en tot intrekking van Verordening (EG) nr. 1073/1999 van het Europees Parlement en de Raad en Verordening (Euratom) nr. 1074/1999 van de Raad (PB L 248 van 18.9.2013, blz. 1).

[40] Verordening (Euratom, EG) nr. 2185/96 van de Raad van 11 november 1996 betreffende de controles en verificaties ter plaatse die door de Commissie worden uitgevoerd ter bescherming van de financiële belangen van de Europese Gemeenschappen tegen fraudes en andere onregelmatigheden (PB L 292 van 15.11.1996, blz. 2).

of er in verband met een door het Agentschap gefinancierde subsidie of overeenkomst sprake is van fraude, corruptie of andere illegale handelingen waardoor de financiële belangen van de Unie worden geschaad.

4. Onverminderd de leden 1, 2 en 3 bevatten samenwerkingsovereenkomsten met derde landen en internationale organisaties, contracten, subsidieovereenkomsten en subsidiebesluiten van het Agentschap bepalingen die de Rekenkamer en OLAF uitdrukkelijk de bevoegdheid verlenen dergelijke audits en onderzoeken binnen hun respectieve bevoegdheden te verrichten.

HOOFDSTUK IV
PERSONEEL VAN HET AGENTSCHAP

Artikel 31
Algemene bepalingen

Het Statuut en de Regeling die van toepassing is op de andere personeelsleden, alsook de voorschriften die onderling overeengekomen zijn tussen de instellingen van de Unie om daaraan uitvoering te geven, zijn van toepassing op het personeel van het Agentschap.

Artikel 32
Voorrechten en immuniteiten

Protocol nr. 7 betreffende de voorrechten en immuniteiten van de Europese Unie dat is gehecht aan het Verdrag betreffende de Europese Unie en het VWEU, is van toepassing op het Agentschap en op het personeel ervan.

Artikel 33
Uitvoerend directeur

1. De uitvoerend directeur wordt in dienst genomen als een tijdelijke functionaris van het Agentschap overeenkomstig artikel 2, onder a), van de Regeling die van toepassing is op de andere personeelsleden.

2. De uitvoerend directeur wordt benoemd door de raad van bestuur, uit een kandidatenlijst die door de Commissie wordt opgesteld na een open en transparante selectieprocedure.

3. Voor de sluiting van het contract met de uitvoerend directeur wordt het Agentschap vertegenwoordigd door de voorzitter van de raad van bestuur.

4. Vóór de benoeming wordt de door de raad van bestuur gekozen kandidaat uitgenodigd een verklaring voor de betreffende commissie van het Europees Parlement af te leggen en vragen van leden te beantwoorden.

5. De ambtstermijn van de uitvoerend directeur is vijf jaar. Aan het eind van deze termijn voert de Commissie een beoordeling uit waarin rekening wordt gehouden met de evaluatie van de prestaties van de uitvoerend directeur en de toekomstige taken en uitdagingen van het Agentschap.

6. De raad van bestuur neemt met een tweederdemeerderheid van zijn stemgerechtigde leden besluiten over de benoeming van de uitvoerend directeur, de verlenging van diens ambtstermijn en de ontheffing van de uitvoerend directeur uit zijn functie.

7. Op voorstel van de Commissie, waarin rekening wordt gehouden met de beoordeling als bedoeld in lid 5, kan de raad van bestuur de ambtstermijn van de uitvoerend bestuurder eenmaal verlengen met ten hoogste vijf jaar.

8. De raad van bestuur stelt het Europees Parlement in kennis van zijn voornemen om de ambtstermijn van de directeur te verlengen. Binnen drie maanden voorafgaand aan een dergelijke verlenging legt de uitvoerend directeur, indien daartoe uitgenodigd, een verklaring af voor de betreffende commissie van het Europees Parlement en beantwoordt vragen van leden.

9. Een uitvoerend directeur wiens ambtstermijn is verlengd, mag niet deelnemen aan een andere selectieprocedure voor dezelfde betrekking.

10. De uitvoerend directeur kan uitsluitend uit zijn functie worden ontheven bij besluit van de raad van bestuur op voorstel van de Commissie.

Artikel 34
Gedetacheerde nationale deskundigen en ander personeel

1. Het Agentschap kan gebruikmaken van gedetacheerde nationale deskundigen of ander personeel dat niet in dienst is van het Agentschap. Het Statuut van de ambtenaren van de Europese Unie en de Regeling die van toepassing is op de andere personeelsleden, zijn niet van toepassing op dit personeel.

2. De raad van bestuur stelt een besluit vast houdende voorschriften inzake de detachering van nationale deskundigen bij het Agentschap.

HOOFDSTUK V
ALGEMENE BEPALINGEN

Artikel 35
Juridische status van het Agentschap

1. Het Agentschap is een orgaan van de Unie en heeft rechtspersoonlijkheid.

2. In elke lidstaat heeft het de ruimste handelingsbevoegdheid die door de nationale wetgeving aan rechtspersonen wordt toegekend. Het Agentschap kan in het bijzonder roerende en onroerende zaken verkrijgen of vervreemden en kan in rechte optreden, of beide.

3. Het Agentschap wordt vertegenwoordigd door zijn uitvoerend directeur.

Artikel 36
Aansprakelijkheid van het Agentschap

1. De contractuele aansprakelijkheid van het Agentschap valt onder het recht dat van toepassing is op de desbetreffende overeenkomst.

2. Het Hof van Justitie van de Europese Unie is bevoegd uitspraak te doen krachtens een arbitrageclausule in een door het Agentschap gesloten overeenkomst.

3. In geval van niet-contractuele aansprakelijkheid vergoedt het Agentschap, overeenkomstig de algemene beginselen die de wetgevingen van de lidstaten gemeen

hebben, alle schade die door het Agentschap zelf of zijn personeelsleden in de uitoefening van hun functie is veroorzaakt.

4. Het Hof van Justitie van de Europese Unie is bevoegd voor geschillen over de vergoeding van dergelijke schade.

5. De persoonlijke aansprakelijkheid van de personeelsleden van het Agentschap ten aanzien van het Agentschap is geregeld bij de desbetreffende bepalingen die van toepassing zijn op het personeel van het Agentschap.

Artikel 37

Talenregeling

1. Verordening nr. 1 van de Raad is van toepassing op het Agentschap[41].De lidstaten en de overige door de lidstaten aangewezen instanties kunnen hun verzoeken aan het Agentschap richten en daarop een antwoord verlangen in de officiële taal van de instellingen van de Unie van hun keuze.

2. De voor het functioneren van het agentschap vereiste vertaaldiensten worden geleverd door het Vertaalbureau voor de organen van de Europese Unie.

Artikel 38

Bescherming van persoonsgegevens

1. Op de verwerking van persoonsgegevens door het Agentschap is Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad[42] van toepassing.

2. De raad van bestuur stelt uitvoeringsvoorschriften als bedoeld in artikel 24, lid 8, van Verordening (EG) nr. 45/2001 vast. De raad van bestuur kan aanvullende maatregelen vaststellen met het oog op de toepassing van Verordening (EG) nr. 45/2001 door het Agentschap.

Artikel 39

Samenwerking met derde landen en internationale organisaties

1. Voor zover noodzakelijk voor de verwezenlijking van de doelstellingen van deze verordening, kan het Agentschap samenwerken met de bevoegde autoriteiten van derde landen en/of met internationale organisaties. Daartoe kan het Agentschap, onder voorbehoud van voorafgaande goedkeuring door de Commissie, werkregelingen treffen met de autoriteiten van derde landen en met internationale organisaties. Deze regelingen scheppen geen wettelijke verplichtingen voor de Unie en haar lidstaten.

2. Het Agentschap staat open voor deelname van derde landen die met de Unie overeenkomsten in die zin hebben gesloten. Krachtens de desbetreffende bepalingen van deze overeenkomsten worden regelingen uitgewerkt voor met name de aard, de omvang en de werkwijze van de deelname van elk van die landen aan de

---

41 Verordening nr. 1 tot regeling van het taalgebruik in de Europese Gemeenschap voor Atoomenergie (PB 17 van 6.10.1958, blz. 401).

42 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (PB L 8 van 12.1.2001, blz. 1).

werkzaamheden van het Agentschap, met inbegrip van bepalingen betreffende de deelname aan initiatieven van het Agentschap enbetreffende financiële en personele bijdragen. Wat personeelszaken betreft, voldoen deze regelingen in elk geval aan het Statuut.

3. De raad van bestuur stelt een strategie op voor de betrekkingen met derde landen en internationale organisaties wat betreft aangelegenheden waarvoor het Agentschap bevoegd is. De Commissie waarborgt dat het Agentschap binnen zijn mandaat en het bestaande institutionele kader handelt door een passende werkovereenkomst met de uitvoerend directeur van het Agentschap te sluiten.

Artikel 40

Beveiligingsvoorschriften ter bescherming van gerubriceerde gegevens en gevoelige niet-gerubriceerde gegevens

Het Agentschap stelt in overleg met de Commissie zijn beveiligingsvoorschriften vast en past daarbij de beginselen inzake beveiliging toe die zijn opgenomen in de beveiligingsvoorschriften van de Commissie voor de bescherming van gerubriceerde EU-informatie (EUCI) en gevoelige niet-gerubriceerde informatie, als vermeld in Besluit (EU, Euratom) 2015/443 en Besluit (EU, Euratom) 2015/444 van de Commissie. Dit geldt onder meer voor de bepalingen voor de uitwisseling, verwerking en opslag van dergelijke gegevens.

Artikel 41

Vestigingsovereenkomst en voorwaarden voor de werking

1. De noodzakelijke bepalingen betreffende de accommodatie die het Agentschap in de gastlidstaat moet worden geboden en de door deze lidstaat ter beschikking te stellen faciliteiten, alsook de specifieke voorschriften die in de gastlidstaat gelden voor de uitvoerend directeur, de leden van de raad van bestuur, de personeelsleden van het Agentschap en hun gezinsleden, worden vastgesteld in een vestigingsovereenkomst tussen het Agentschap en de lidstaat waar de locatie van de vestiging zich bevindt, die wordt gesloten nadat de raad van bestuur daarmee heeft ingestemd en niet later dan [twee jaar na de inwerkingtreding van de onderhavige verordening].

2. De lidstaat van vestiging van het Agentschap verschaft zo goed mogelijke voorwaarden om een goede werking van het Agentschap te waarborgen, met inbegrip van de bereikbaarheid van de locatie, de aanwezigheid van passende onderwijsvoorzieningen voor de kinderen van personeelsleden en passende arbeidsmogelijkheden, sociale zekerheid en medische zorg voor kinderen en echtgenoten van personeelsleden.

Artikel 42

Administratieve controle

De Ombudsman ziet toe op de activiteiten van het Agentschap in overeenstemming met artikel 228 VWEU.

TITEL III
KADER VOOR CYBERBEVEILIGINGSCERTIFICERING

Artikel 43

Europese regelingen voor cyberbeveiligingscertificering

Een Europese regeling voor cyberbeveiliging bevestigt dat de ICT-producten en -diensten die overeenkomstig een dergelijke regeling zijn gecertificeerd, voldoen aan specifieke vereisten met betrekking tot hun vermogen om met een gegeven zekerheidsniveau weerstand te bieden aan acties die erop zijn gericht de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens en de functies of diensten die via deze producten, processen, diensten en systemen worden aangeboden of toegankelijk zijn, in gevaar te brengen.

Artikel 44

Voorbereiding en vaststelling van een Europese regeling voor cyberbeveiligingscertificering

1. Naar aanleiding van een verzoek van de Commissie bereidt het Enisa een potentiële Europese regeling voor cyberbeveiligingscertificering voor die voldoet aan de vereisten van de artikelen 45, 46 en 47 van deze verordening. De lidstaten of de bij artikel 53 ingestelde Europese Groep voor cyberbeveiligingscertificering ("de Groep") kunnen de Commissie voorstellen een potentiële regeling voor cyberbeveiligingscertificering voor te bereiden.
2. Bij de voorbereiding van potentiële regelingen als bedoeld in lid 1 van dit artikel, raadpleegt het Enisa alle betrokken partijen en werkt het nauw samen met de Groep. De Groep staat het Enisa bij met assistentie en deskundige raad die nodig zijn voor de voorbereiding van de potentiële regeling, onder meer door indien nodig adviezen te verstrekken.
3. Het Enisa dient de potentiële Europese regeling voor cyberbeveiligingscertificering, opgesteld in overeenstemming met lid 2 van dit artikel, in bij de Commissie.
4. Op basis van de door het Enisa voorgestelde potentiële regeling kan de Commissie uitvoeringshandelingen vaststellen overeenkomstig artikel 55, lid 1, om te voorzien in Europese regelingen voor cyberbeveiligingscertificering van ICT-producten en -diensten die voldoen aan de vereisten van de artikelen 45, 46 en 47 van deze verordening.
5. Het Enisa beheert een specifieke website met informatie en publiciteit over Europese regelingen voor cyberbeveiligingscertificering.

Artikel 45

Beveiligingsdoelstellingen van Europese regelingen voor cyberbeveiligingscertificering

Bij de opzet van een Europese regeling voor cyberbeveiligingscertificering wordt, in voorkomend geval, rekening gehouden met de volgende doelstellingen:

(a) opgeslagen, doorgegeven of anderszins bewerkte gegevens beschermen tegen accidentele of onbevoegde opslag, verwerking, toegang of openbaarmaking;

(b) opgeslagen, doorgegeven of anderszins bewerkte gegevens beschermen tegen accidentele of onbevoegde vernietiging, accidenteel verlies of wijziging;

(c) ervoor zorgen dat bevoegde personen, programma's of machines uitsluitend toegang hebben tot gegevens, diensten of functies waarvoor hun recht van toegang geldt;

(d) registreren welke gegevens, functies of diensten op welk tijdstip en door wie zijn meegedeeld;

(e) ervoor zorgen dat kan worden nagegaan wie op welk tijdstip toegang heeft gehad of gebruik heeft gemaakt van welke gegevens, diensten of functies;

(f) de beschikbaarheid van en toegang tot gegevens, diensten en functies tijdig herstellen in het geval van een fysiek of technisch incident;

(g) ervoor zorgen dat ICT-producten en -diensten worden geleverd met geüpdatete software die geen bekende kwetsbaarheden bevat en met mechanismen voor veilige software-updates.

Artikel 46

Zekerheidsniveaus van Europese regelingen voor cyberbeveiligingscertificering

1. Voor ICT-producten en -diensten die op grond van een Europese regeling voor cyberbeveiligingscertificering zijn gecertificeerd, kunnen in die regeling een of meer van de volgende zekerheidsniveaus worden gespecificeerd: basis, substantieel en/of hoog.

2. De zekerheidsniveaus basis, substantieel en hoog voldoen respectievelijk aan de volgende criteria:

(a) het zekerheidsniveau "basis" betreft een in het kader van een Europese regeling voor cyberbeveiligingscertificering uitgegeven certificaat dat een beperkte mate van vertrouwen in de opgegeven of beweerde cyberbeveiligingskwaliteiten van een ICT-product of -dienst biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van cyberincidenten te verkleinen;

(b) het zekerheidsniveau "substantieel" betreft een in het kader van een Europese regeling voor cyberbeveiligingscertificering uitgegeven certificaat dat een substantiële mate van vertrouwen in de opgegeven of beweerde cyberbeveiligingskwaliteiten van een ICT-product of -dienst biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van cyberincidenten substantieel te verkleinen;

(c) het zekerheidsniveau "hoog" betreft een in het kader van een Europese regeling voor cyberbeveiligingscertificering uitgegeven certificaat dat een hogere mate van vertrouwen in de opgegeven of beweerde cyberbeveiligingskwaliteiten van een ICT-product of -dienst biedt dan certificaten met zekerheidsniveau substantieel, en wordt toegekend onder verwijzing naar technische

specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben cyberincidenten te voorkomen.

Artikel 47

Elementen van Europese regelingen voor cyberbeveiligingscertificering

1. Een Europese regeling voor cyberbeveiligingscertificering omvat de volgende elementen:

   (a) het onderwerp en het toepassingsgebied van de certificering, met inbegrip van het type of de categorieën van ICT-producten en -diensten die hieronder vallen;

   (b) gedetailleerde specificatie van de voorschriften voor cyberbeveiliging op basis waarvan de specifieke ICT-producten en -diensten worden beoordeeld, bijvoorbeeld door verwijzing naar Europese of internationale normen of technische specificaties;

   (c) in voorkomend geval, één of meer zekerheidsniveaus;

   (d) de specifieke evaluatiecriteria en -methoden, met inbegrip van soorten evaluaties, die worden gebruikt om aan te tonen dat de in artikel 45 genoemde specifieke doelstellingen worden verwezenlijkt;

   (e) de door een aanvrager aan de conformiteitsbeoordelingsinstantie te verstrekken informatie die nodig is voor certificering;

   (f) indien de regeling voorziet in merktekens of labels, de voorwaarden waaronder dergelijke merktekens of labels mogen worden gebruikt;

   (g) indien toezicht onderdeel uitmaakt van de regeling, de regels voor het toezicht op de naleving van de certificeringseisen, met inbegrip van mechanismen om de blijvende naleving van de gespecificeerde cyberbeveiligingseisen aan te tonen;

   (h) voorwaarden voor de toekenning, handhaving, voortzetting, uitbreiding en beperking van het toepassingsgebied van de certificering;

   (i) regels over de gevolgen wanneer gecertificeerde ICT-producten en -diensten niet voldoen aan de certificeringseisen;

   (j) regels over de manier waarop voorheen onopgemerkte zwakke punten in de cyberbeveiliging van ICT-producten en -diensten moeten worden gemeld en aangepakt;

   (k) regels over het bewaren van gegevens door conformiteitsbeoordelingsinstanties;

   (l) identificatie van nationale regelingen voor cyberbeveiligingscertificering die betrekking hebben op hetzelfde type of dezelfde categorieën van ICT-producten en -diensten;

   (m) de inhoud van het afgegeven certificaat.

2. De specifieke eisen van de regeling zijn niet in strijd met de toepasselijke wettelijke voorschriften, met name voorschriften die voortvloeien uit geharmoniseerde Uniewetgeving.

3. Indien een specifieke handeling van de Unie daarin voorziet, kan certificering in het kader van een Europese regeling voor cyberbeveiligingscertificering worden gebruikt om het vermoeden van conformiteit met de vereisten van die handeling aan te tonen.

4. In gevallen waarin geharmoniseerde Uniewetgeving ontbreekt, kan in nationale wetgeving ook worden bepaald dat een Europese regeling voor cyberbeveiligingscertificering kan worden gebruikt om het vermoeden van conformiteit met de wettelijke eisen vast te stellen.

Artikel 48

Cyberbeveiligingscertificering

1. ICT-producten en -diensten die zijn gecertificeerd in het kader van een overeenkomstig artikel 44 vastgestelde Europese regeling voor cyberbeveiligingscertificering, worden geacht te voldoen aan de vereisten van een dergelijke regeling.

2. De certificering gebeurt vrijwillig, tenzij anders is gespecificeerd in de wetgeving van de Unie.

3. Een Europees cyberbeveiligingscertificaat als bedoeld in dit artikel wordt afgegeven door de in artikel 51 bedoelde conformiteitsbeoordelingsinstanties op basis van de criteria in de overeenkomstig artikel 44 vastgestelde Europese regeling voor cyberbeveiligingscertificering.

4. In afwijking van lid 3 en in naar behoren gemotiveerde gevallen kan een bepaalde Europese regeling voor cyberbeveiliging erin voorzien dat een Europees cyberbeveiligingscertificaat dat voortvloeit uit die regeling alleen door een overheidsinstantie kan worden afgegeven. Die overheidsinstantie is een van de volgende organen:

   (a) een nationale autoriteit voor certificeringstoezicht als bedoeld in artikel 50, lid 1;

   (b) een orgaan dat als conformiteitsbeoordelingsinstantie overeenkomstig artikel 51, lid 1, is geaccrediteerd; of

   (c) een orgaan dat is opgericht bij wetten, wettelijke regelingen of andere officiële administratieve procedures van een betrokken lidstaat en dat voldoet aan de eisen voor instanties die producten, processen en diensten certificeren overeenkomstig ISO/IEC 17065:2012.

5. De natuurlijke persoon of rechtspersoon die zijn ICT-producten of -diensten aan het certificeringsmechanisme onderwerpt, geeft de in artikel 51 bedoelde conformiteitsbeoordelingsinstantie alle informatie die nodig is om de certificeringsprocedure uit te voeren.

6. Certificaten worden afgegeven voor een maximumperiode van drie jaar en kunnen onder dezelfde voorwaarden worden verlengd, mits nog steeds aan de desbetreffende eisen wordt voldaan.

7. Een op grond van dit artikel afgegeven Europees cyberbeveiligingscertificaat wordt in alle lidstaten erkend.

Artikel 49

Nationale regelingen en certificaten voor cyberbeveiligingscertificering

1. Onverminderd lid 3 hebben nationale regelingen voor cyberbeveiligingscertificering en de daaraan verbonden procedures voor ICT-producten en -diensten die onder een Europese regeling voor cyberbeveiligingscertificering vallen, niet langer gevolgen vanaf de datum die wordt bepaald in de overeenkomstig artikel 44, lid 4, vastgestelde uitvoeringshandeling. Bestaande nationale regelingen voor cyberbeveiligingscertificering en de daaraan verbonden procedures voor ICT-producten en -diensten die niet onder een Europese regeling voor cyberbeveiligingscertificering vallen, blijven bestaan.
2. De lidstaten voeren geen nieuwe nationale regelingen voor cyberbeveiligingscertificering in voor ICT-producten en -diensten die onder een van kracht zijnde Europese regeling voor cyberbeveiligingscertificering vallen.
3. Bestaande certificaten die zijn afgegeven op grond van nationale regelingen voor cyberbeveiligingscertificering, blijven geldig tot hun vervaldatum.

Artikel 50

Nationale autoriteiten voor certificeringstoezicht

1. Iedere lidstaat wijst een nationale autoriteit voor certificeringstoezicht aan.
2. Elke lidstaat stelt de Commissie in kennis van de identiteit van de aangewezen autoriteit.
3. Elke nationale autoriteit voor certificeringstoezicht is op het vlak van haar organisatie, financieringsbeslissingen, rechtsstructuur en besluitvorming onafhankelijk van de entiteiten waarop zij toezicht houdt.
4. De lidstaten zien erop toe dat de nationale autoriteiten voor certificeringstoezicht over voldoende middelen beschikken om hun bevoegdheden uit te oefenen en de hun toegewezen taken op een doeltreffende en doelmatige wijze uit te voeren.
5. Met het oog op de effectieve uitvoering van deze verordening is het wenselijk dat deze autoriteiten op een actieve, effectieve, efficiënte en betrouwbare manier deelnemen aan de overeenkomstig artikel 53 ingestelde Europese Groep voor cyberbeveiligingscertificering.
6. Nationale autoriteiten voor certificeringstoezicht:
   (a) monitoren en handhaven de toepassing van de bepalingen van deze titel op nationaal niveau en zien erop toe dat de certificaten die zijn afgegeven door conformiteitsbeoordelingsinstanties die op hun respectieve grondgebieden zijn gevestigd, voldoen aan de vereisten van deze titel en de betrokken Europese regeling voor cyberbeveiligingscertificering;
   (b) monitoren en houden toezicht op de werkzaamheden van de conformiteitsbeoordelingsinstanties voor de toepassing van deze verordening, onder meer met betrekking tot de aanmelding van conformiteitsbeoordelingsinstanties en de daarmee verband houdende taken als bedoeld in artikel 52 van deze verordening;
   (c) behandelen klachten van natuurlijke of rechtspersonen over certificaten die zijn afgegeven door op hun grondgebied gevestigde

conformiteitsbeoordelingsinstanties, onderzoeken de inhoud van de klacht in de mate waarin dat gepast is, en stellen de klager binnen een redelijke termijn in kennis van de vooruitgang en het resultaat van het onderzoek;

(d) werken samen met andere nationale autoriteiten voor certificeringstoezicht of andere overheidsinstanties, onder meer door informatie uit te wisselen over de mogelijke niet-overeenstemming van ICT-producten en -diensten met de vereisten van deze verordening of met specifieke Europese regelingen voor cyberbeveiliging;

(e) volgen de relevante ontwikkelingen op het gebied van cyberbeveiligingscertificering.

7. Elke nationale autoriteit voor certificeringstoezicht beschikt ten minste over de volgende bevoegdheden:

(a) conformiteitsbeoordelingsinstanties en houders van Europese cyberbeveiligingscertificaten vragen om alle informatie te verstrekken die zij nodig heeft voor de uitvoering van haar taken;

(b) onderzoeken verrichten in de vorm van audits van conformiteitsbeoordelingsinstanties en houders van Europese cyberbeveiligingscertificaten om de naleving van de bepalingen van titel III te verifiëren;

(c) passende maatregelen nemen, overeenkomstig het nationale recht, om ervoor te zorgen dat conformiteitsbeoordelingsinstanties en houders van Europese cyberbeveiligingscertificaten deze verordening of een Europese regeling voor cyberbeveiligingscertificering naleven;

(d) toegang verkrijgen tot alle gebouwen en terreinen van conformiteitsbeoordelingsinstanties en houders van Europese cyberbeveiligingscertificaten voor het verrichten van onderzoeken in overeenstemming met het Unierecht of het lidstatelijke procesrecht;

(e) certificaten die niet in overeenstemming zijn met deze verordening of een Europese regeling voor cyberbeveiligingscertificering intrekken conform het nationale recht;

(f) overeenkomstig het nationale recht sancties opleggen als bedoeld in artikel 54 en eisen dat onmiddellijk een einde wordt gemaakt aan de niet-nakoming van de verplichtingen van deze verordening.

8. Nationale autoriteiten voor certificeringstoezicht werken samen met elkaar en met de Commissie en wisselen met name informatie, ervaringen en goede praktijken uit op het vlak van cyberbeveiligingscertificering en technische kwesties met betrekking tot de cyberbeveiliging van ICT-producten en -diensten.

Artikel 51

Conformiteitsbeoordelingsinstanties

1. De conformiteitsbeoordelingsinstanties worden alleen door de op grond van Verordening (EG) nr. 765/2008 aangewezen nationale accreditatie-instantie geaccrediteerd als zij voldoen aan de vereisten die zijn vastgesteld in de bijlage bij deze verordening.

2. De accreditatie wordt afgegeven voor een maximumperiode van vijf jaar en kan onder dezelfde voorwaarden worden verlengd, mits de conformiteitsbeoordelingsinstantie aan de in dit artikel gestelde eisen voldoet. Accreditatie-instanties trekken de accreditatie van een conformiteitsbeoordelingsinstantie, als bedoeld in lid 1 van dit artikel, in wanneer niet of niet meer aan de voorwaarden voor de accreditatie wordt voldaan of wanneer door een conformiteitsbeoordelingsinstantie ondernomen acties indruisen tegen deze verordening.

Artikel 52
Aanmelding

1. Voor elke overeenkomstig artikel 44 vastgestelde Europese regeling voor cyberbeveiligingscertificering stellen de nationale autoriteiten voor certificeringstoezicht de Commissie in kennis van de conformiteitsbeoordelingsinstanties die geaccrediteerd zijn om certificaten af te geven voor gespecificeerde zekerheidsniveaus als bedoeld in artikel 46 en, onverwijld, van alle latere wijzigingen met betrekking daartoe.
2. Eén jaar na de inwerkingtreding van een Europese regeling voor cyberbeveiligingscertificering publiceert de Commissie in het Publicatieblad van de Europese Unie een lijst van aangemelde conformiteitsbeoordelingsinstanties.
3. Indien de Commissie een aanmelding ontvangt nadat de in lid 2 bedoelde periode is verstreken, maakt zij binnen twee maanden na de datum van ontvangst van die aanmelding in het Publicatieblad van de Europese Unie de wijzigingen van de in lid 2 bedoelde lijst bekend.
4. Een nationale autoriteit voor certificeringstoezicht kan bij de Commissie een verzoek indienen om een door die nationale autoriteit voor certificeringstoezicht aangemelde conformiteitsbeoordelingsinstantie te verwijderen van de in lid 2 van dit artikel bedoelde lijst. Binnen één maand na de datum van ontvangst van het verzoek van de nationale autoriteit voor certificeringstoezicht maakt de Commissie de overeenkomstige wijzigingen van de lijst bekend in het Publicatieblad van de Europese Unie.
5. De Commissie kan door middel van uitvoeringshandelingen de omstandigheden, formaten en procedures van de in lid 1 van dit artikel bedoelde aanmeldingen vaststellen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 55, lid 2, bedoelde onderzoeksprocedure.

Artikel 53
Europese Groep voor cyberbeveiligingscertificering

1. De Europese Groep voor cyberbeveiligingscertificering (hierna “de Groep” genoemd) wordt opgericht.
2. De groep bestaat uit de nationale autoriteiten voor certificeringstoezicht. De autoriteiten worden vertegenwoordigd door de hoofden of andere hooggeplaatste vertegenwoordigers van de nationale autoriteiten voor certificeringstoezicht.
3. De groep heeft de volgende taken:

(a) de Commissie adviseren en bijstaan in haar werkzaamheden met het oog op een consistente tenuitvoerlegging en toepassing van de bepalingen van deze titel, met name met betrekking tot beleidsvraagstukken over cyberbeveiligingscertificering, de coördinatie van beleidsbenaderingen en de voorbereiding van Europese regelingen voor cyberbeveiligingscertificering;

(b) bijstand en advies verlenen aan en samenwerken met het Enisa in het kader van de voorbereiding van een potentiële regeling overeenkomstig artikel 44 van deze verordening;

(c) de Commissie voorstellen dat zij het Enisa vraagt een potentiële Europese regeling voor cyberbeveiligingscertificering voor te bereiden overeenkomstig artikel 44 van deze verordening;

(d) aan de Commissie gerichte adviezen uitbrengen met betrekking tot het onderhoud en de herziening van bestaande Europese regelingen voor cyberbeveiligingscertificering;

(e) de relevante ontwikkelingen op het gebied van cyberbeveiligingscertificering bestuderen en goede praktijken op het gebied van regelingen voor cyberbeveiligingscertificering uitwisselen;

(f) de samenwerking tussen de nationale autoriteiten voor certificeringstoezicht uit hoofde van deze titel vergemakkelijken door middel van informatie-uitwisseling, met name door de vaststelling van methoden voor de efficiënte uitwisseling van informatie over alle aangelegenheden die verband houden met cyberbeveiligingscertificering.

4. De Commissie zit de groep voor en verzorgt het secretariaat, bijgestaan door het Enisa overeenkomstig artikel 8, onder a).

Artikel 54
Sancties

De lidstaten stellen voorschriften vast voor de bestraffing van overtredingen van deze titel en van Europese regelingen voor cyberbeveiligingscertificering en treffen alle nodige maatregelen om erop toe te zien dat die sancties ook worden toegepast. De vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend. De lidstaten stellen de Commissie [uiterlijk op .../onverwijld] van deze voorschriften en deze maatregelen in kennis en doen dit eveneens bij alle eventuele latere wijzigingen ervan.

TITEL IV
SLOTBEPALINGEN

Artikel 55
Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.
2. Wanneer naar dit lid wordt verwezen, is artikel 4 van Verordening (EU) nr. 182/2011 van toepassing.

Artikel 56
Evaluatie en toetsing

1. Uiterlijk vijf jaar na de in artikel 58 bedoelde datum en vervolgens om de vijf jaar beoordeelt de Commissie de impact, doeltreffendheid en doelmatigheid van het Agentschap, zijn werkmethoden, de eventuele noodzaak om het mandaat van het Agentschap te wijzigen en de financiële gevolgen van een dergelijke wijziging. Bij de evaluatie wordt rekening gehouden met feedback die aan het Agentschap is gegeven naar aanleiding van zijn activiteiten. Als de Commissie van oordeel is dat het voortbestaan van het Agentschap niet langer gerechtvaardigd is in het licht van zijn doelstellingen, mandaat en taken, kan zij voorstellen om de bepalingen van deze verordening die betrekking hebben op het Agentschap, te wijzigen.
2. Bij de evaluatie wordt ook gekeken naar de impact, doeltreffendheid en doelmatigheid van de bepalingen van titel III met betrekking tot de doelstellingen om een passend niveau van cyberbeveiliging van ICT-producten en -diensten in de Unie te waarborgen en de werking van de interne markt te verbeteren.
3. De Commissie stuurt het evaluatieverslag en haar conclusies toe aan het Europees Parlement, de Raad en de raad van bestuur. De bevindingen van het evaluatieverslag worden openbaar gemaakt.

Artikel 57
Intrekking en opvolging

1. Verordening (EU) nr. 526/2013 wordt met ingang van [...] ingetrokken.
2. Verwijzingen naar Verordening (EU) nr. 526/2013 en naar het Enisa gelden als verwijzingen naar deze verordening en naar het Agentschap.
3. Het Agentschap volgt het bij Verordening (EU) nr. 526/2013 opgerichte agentschap op voor wat alle eigendommen, overeenkomsten, wettelijke verplichtingen, arbeidsovereenkomsten, financiële verbintenissen en verplichtingen betreft. Alle bestaande besluiten van de raad van bestuur en het dagelijks bestuur blijven geldig, mits zij niet in strijd zijn met de bepalingen van deze verordening.
4. Het Agentschap wordt met ingang van [...] voor onbepaalde tijd opgericht.

5. De overeenkomstig artikel 24, lid 4, van Verordening (EU) nr. 526/2013 aangewezen uitvoerend directeur wordt de uitvoerend directeur van het Agentschap voor het resterende gedeelte van zijn ambtstermijn.

6. De overeenkomstig artikel 6 van Verordening (EU) nr. 526/2013 aangewezen leden van de raad van bestuur en hun plaatsvervangers worden de leden van de raad van bestuur van het Agentschap en hun plaatsvervangers voor het resterende gedeelte van hun ambtstermijn.

Artikel 58

1. Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het Publicatieblad van de Europese Unie.

2. Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

FINANCIEEL MEMORANDUM

1. KADER VAN HET VOORSTEL/INITIATIEF

1.1. Benaming van het voorstel/initiatief

Voorstel voor een verordening van het Europees Parlement en de Raad inzake Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, tot intrekking van Verordening (EU) nr. 526/2013, en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie ("de cyberbeveiligingsverordening")

1.2. Betrokken beleidsterrein(en)

Beleidsterrein: 09 Communicatienetwerken, inhoud en technologie

Activiteit: 09 02 Digitale eengemaakte markt

1.3. Aard van het voorstel/initiatief

☒ Het voorstel/initiatief betreft **een nieuwe actie (Titel III – Certificering)**

☐ Het voorstel/initiatief betreft **een nieuwe actie na een proefproject/een voorbereidende actie**[43]

☒Het voorstel/initiatief betreft **de verlenging van een bestaande actie** (**Titel II – Mandaat van het Enisa)**

☐ Het voorstel/initiatief betreft **een actie die wordt omgebogen naar een nieuwe actie**

1.4. Doelstelling(en)

1.4.1. De met het voorstel/initiatief beoogde strategische meerjarendoelstelling(en) van de Commissie

1. De weerbaarheid van de lidstaten, het bedrijfsleven en de EU als geheel versterken

2. De goede werking van de interne markt van de EU voor ICT-producten en -diensten waarborgen

3. Het mondiale concurrentievermogen van ondernemingen in de EU die actief zijn op het gebied van ICT vergroten

4. De wettelijke en bestuursrechtelijke bepalingen van de lidstaten waarvoor cyberbeveiliging is vereist onderling aanpassen

1.4.2. Specifieke doelstelling(en)

In het licht van de algemene doelstellingen en in de bredere context van de herziene strategie voor cyberbeveiliging wordt, door de reikwijdte en het mandaat van het Enisa af te bakenen en een Europees certificeringskader voor ICT-producten en -diensten op te zetten, beoogd de volgende specifieke doelstellingen te verwezenlijken met het instrument:

1. De **vermogens en paraatheid** van de lidstaten en het bedrijfsleven verhogen.
2. De **samenwerking en coördinatie** tussen de lidstaten en de EU-instellingen, -agentschappen en -organen verbeteren.
3. De **vermogens op EU-niveau ter aanvulling op maatregelen van de lidstaten**, met name in het geval van grensoverschrijdende cybercrises, versterken.

[43] In de zin van artikel 54, lid 2, onder a) of b), van het Financieel Reglement.

4. Het **bewustzijn** van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties versterken.
5. Het vertrouwen in de digitale eengemaakte markt en in digitale innovatie versterken door de algehele **transparantie van de zekerheid inzake cyberbeveiliging**[44] van ICT-producten en -diensten te verbeteren.

Het Enisa zal bijdragen tot de verwezenlijking van bovenstaande doelstellingen door middel van:

Versterkte ondersteuning van de beleidsvorming – richtsnoeren en advies verstrekken aan de Commissie en de lidstaten met het oog op de actualisering en ontwikkeling van een alomvattend normatief kader op het gebied van cyberbeveiliging, alsook sectorspecifieke beleids- en wetgevingsinitiatieven die verband houden met cyberbeveiliging; bijdragen tot de werkzaamheden van de samenwerkingsgroep (artikel 11 van Richtlijn (EU) 2016/1148) door expertise en bijstand te verstrekken; de ontwikkeling en uitvoering van beleid op het gebied van elektronische identiteits- en vertrouwensdiensten ondersteunen; bevorderen van de uitwisseling van beste praktijken tussen bevoegde autoriteiten;

Ondersteuning van versterkte capaciteitsopbouw – ondersteuning verlenen aan de lidstaten, de EU-instellingen, -organen, -instanties en -agentschappen om de preventie, de opsporing en de analyse van, en het vermogen te reageren op, problemen en incidenten betreffende cyberbeveiliging te ontwikkelen en te verbeteren; bijstand verlenen aan de lidstaten, op hun verzoek, bij de ontwikkeling van nationale CSIRT's en nationale cyberbeveiligingsstrategieën; bijstand verlenen aan de EU-instellingen bij de ontwikkeling en evaluatie van EU-strategieën inzake cyberbeveiliging; organiseren van opleidingen op het gebied van cyberbeveiliging; bijstand verlenen aan de lidstaten in het kader van de samenwerkingsgroep bij de uitwisseling van beste praktijken; vergemakkelijken van de oprichting van sectorale centra voor informatie-uitwisseling en -analyse (ISAC's).

Ondersteuning van de operationele samenwerking en crisisbeheersing – ondersteunen van de samenwerking tussen bevoegde overheidsinstanties, en tussen belanghebbenden, door een systematische samenwerking tot stand te brengen tussen de EU-instellingen, -organen, -instanties en -agentschappen die zich bezighouden met cyberbeveiliging, cybercriminaliteit en de bescherming van de persoonlijke levenssfeer en persoonsgegevens; voor het secretariaat van het CSIRT-netwerk zorgen (artikel 12, lid 2, van Richtlijn (EU) 2016/1148) en bijdragen aan de operationele samenwerking binnen het netwerk door in samenwerking met CERT-EU ondersteuning te verlenen aan de lidstaten op hun verzoek; organiseren van regelmatige cyberbeveiligingsoefeningen; bijdragen tot de ontwikkeling van een gezamenlijke respons op grootschalige grensoverschrijdende cyberincidenten en -crises; uitvoeren van technisch ex-postonderzoek van significante incidenten in samenwerking met het CSIRT-netwerk en uitvaardigen van vervolgaanbevelingen;

Marktgerelateerde taken (normalisatie, certificering) – een aantal functies uitvoeren die specifiek zijn bedoeld voor het ondersteunen van de interne markt: voorzien in een waarnemingspost cyberbeveiliging, door relevante trends op de cyberbeveiligingsmarkt te analyseren teneinde vraag en aanbod beter op elkaar af te stemmen; ondersteunen en bevorderen van de ontwikkeling en uitvoering van het EU-beleid inzake cyberbeveiligingscertificering van ICT-producten en -diensten door potentiële Europese

[44] Transparantie van de zekerheid inzake cyberbeveiliging houdt in dat de gebruikers worden voorzien van voldoende informatie over cyberbeveiligingseigenschappen, waardoor zij in staat zijn het beveiligingsniveau van elk ICT-product, -dienst of -proces objectief te bepalen.

regelingen voor cyberbeveiligingscertificering voor ICT-producten en -diensten voor te bereiden, het secretariaat voor de Europese Groep voor cyberbeveiligingscertificering te verzorgen, en richtsnoeren en beste praktijken te verschaffen in verband met de beveiligingsvereisten van ICT-producten en -diensten, in samenwerking met de nationale autoriteiten voor certificeringstoezicht en de branche; **Ondersteuning van verbeterde kennis, informatie en bewustmaking** – bijstand verlenen en advies verstrekken aan de Commissie en de lidstaten om in de hele Unie een hoog niveau van kennis te bereiken over kwesties die verband houden met netwerk- en informatiebeveiliging en de toepassing ervan op de belanghebbenden uit de sector. Dit houdt ook in dat informatie over de beveiliging van netwerk- en informatiesystemen [of cyberbeveiliging] wordt gebundeld, georganiseerd en openbaar wordt gemaakt. Bewustmakingsactiviteiten en op het brede publiek gerichte voorlichtingscampagnes over cyberbeveiligingsrisico's vormen een ander belangrijk element.

Versterkte ondersteuning van onderzoek en innovatie – advies verschaffen over onderzoeksbehoeften en het stellen van prioriteiten op het gebied van cyberbeveiliging;

Ondersteuning van internationale samenwerking – de inspanningen van de Unie om samen te werken met derde landen en internationale organisaties ondersteunen teneinde de internationale samenwerking op het gebied van cyberbeveiliging te bevorderen.

CERTIFICERING

Het certificeringskader zal bijdragen tot de verwezenlijking van de doelstellingen door de algehele transparantie van de cyberbeveiligingszekerheid[45] van ICT-producten en -diensten te verhogen en daarmee het vertrouwen in de digitale interne markt en digitale innovatie te versterken. Hiermee moet ook worden voorkomen dat de certificeringsregelingen in de EU en de daarmee samenhangende beveiligingseisen en evaluatiecriteria in alle lidstaten en sectoren versnipperen.

1.4.3. Verwacht resultaat/verwachte resultaten en gevolg(en)

Vermeld de gevolgen die het voorstel/initiatief zou moeten hebben voor de begunstigden/doelgroepen.

Het versterkte Enisa (waarmee de vermogens, preventie, samenwerking en bewustmaking op EU-niveau worden ondersteund teneinde de algehele cyberweerbaarheid van de EU te versterken), en de ondersteuning van het Europese certificeringskader voor ICT-producten en -diensten zullen naar verwachting de volgende gevolgen hebben (niet-limitatieve lijst):

Algemene gevolgen:

- Algemene positieve gevolgen voor de interne markt dankzij de teruggedrongen marktversnippering en het vergroten van het vertrouwen in digitale technologieën door middel van betere samenwerking, een meer geharmoniseerde aanpak van het EU-beleid op het gebied van cyberbeveiliging en grotere vermogens op EU-niveau. Dit moet een positief economisch effect sorteren door er mee voor te zorgen dat cyberbeveiligings- of cybercriminaliteitsincidenten, waarvan de economische impact in de Unie momenteel naar schatting 0,41 % van het bbp van de EU bedraagt (ongeveer 55 miljard EUR), minder kosten veroorzaken.

Specifieke resultaten:

[45] Transparantie van de zekerheid inzake cyberbeveiliging houdt in dat de gebruikers worden voorzien van voldoende informatie over cyberbeveiligingseigenschappen, waardoor zij in staat zijn het beveiligingsniveau van elk ICT-product, -dienst of -proces objectief te bepalen.

Versterkte vermogens en paraatheid van de lidstaten en het bedrijfsleven inzake cyberbeveiliging

- Versterkte vermogens en paraatheid van de lidstaten inzake cyberbeveiliging (dankzij strategische langetermijnanalyses van cyberbeveiligingsdreigingen en -incidenten, richtsnoeren en verslagen, expertise en goede praktijken, de beschikbaarheid van opleidingen en opleidingsmateriaal, versterkt door CyberEurope-oefeningen).

- Versterkte vermogens van particuliere actoren dankzij de ondersteuning van de oprichting van centra voor informatie-uitwisseling en -analyse (ISAC's) in diverse sectoren.

- Versterkte paraatheid van de EU en de lidstaten inzake cyberbeveiliging dankzij het feit dat er goed ingeoefende en overeengekomen plannen beschikbaar zijn in geval van grootschalige grensoverschrijdende incidenten die zijn getest in het kader van CyberEurope-oefeningen;

Verbeterde samenwerking en coördinatie tussen de lidstaten en de EU-instellingen, -agentschappen en -organen

- Verbeterde samenwerking zowel binnen als tussen de publieke en de particuliere sector;

- Consistentere aanpak van de uitvoering van de NIS-richtlijn over de grenzen heen en in alle sectoren;

- Verbeterde samenwerking op het gebied van certificering dankzij een institutioneel kader voor de ontwikkeling van Europese regelingen voor cyberbeveiligingscertificering en de ontwikkeling van een gemeenschappelijk beleid op dit gebied.

Versterkte vermogens op EU-niveau ter aanvulling van het optreden van de lidstaten

- Verbeterde "operationele capaciteit van de EU" ter aanvulling en ondersteuning van het optreden van de lidstaten, op verzoek en met betrekking tot beperkte en vooraf bepaalde diensten; Dit zal naar verwachting een positief effect hebben op het succes van de preventie en opsporing van, alsmede de reactie op, incidenten, zowel op het niveau van de lidstaten als van de Unie;

Versterkt bewustzijn van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties

- Versterkt algemeen bewustzijn van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties

- Verbeterd vermogen om weloverwogen aankoopbeslissingen te nemen op het vlak van ICT-producten en -diensten dankzij cyberbeveiligingscertificering

Versterkt vertrouwen in de digitale eengemaakte markt en in digitale innovatie door de betere transparantie van de zekerheid inzake cyberbeveiliging van ICT-producten en -diensten

- Betere transparantie van de zekerheid inzake cyberbeveiliging[46] van ICT-producten en -diensten dankzij vereenvoudigde procedures voor beveiligingscertificering door middel van een EU-kader

- Meer zekerheid over de beveiligingseigenschappen van ICT-producten en -diensten

[46] Transparantie van de zekerheid inzake cyberbeveiliging houdt in dat de gebruikers worden voorzien van voldoende informatie over cyberbeveiligingseigenschappen, waardoor zij in staat zijn het beveiligingsniveau van elk ICT-product, -dienst of -proces objectief te bepalen.

- Toegenomen gebruik van beveiligingscertificering, gestimuleerd door vereenvoudigde procedures, lagere kosten en het vooruitzicht op zakelijke mogelijkheden in de hele EU die niet worden belemmerd door marktversnippering

- Sterker concurrentievermogen op de EU-markt voor cyberbeveiliging door de verminderde kosten en administratieve lasten voor kleine en middelgrote ondernemingen en door het wegnemen van mogelijke belemmeringen voor toetreding tot de markt als gevolg van de vele nationale certificeringsregelingen

Andere

- Voor geen enkele doelstelling wordt een significant milieueffect verwacht.

- Wat de EU-begroting betreft, worden efficiëntiewinsten verwacht door de intensievere samenwerking en coördinatie van de activiteiten tussen de EU-instellingen, -agentschappen en -organen

1.4.4. Resultaat- en effectindicatoren

Vermeld de indicatoren aan de hand waarvan kan worden nagegaan in hoeverre het voorstel/initiatief is uitgevoerd.

(a)

Doelstelling: De vermogens en paraatheid van de lidstaten en het bedrijfsleven verhogen:

- Aantal opleidingen georganiseerd door het Enisa
- Geografische spreiding (aantal landen en gebieden) van de rechtstreekse steun van het Enisa
- Niveau van paraatheid van de lidstaten wat betreft de maturiteit van de CSIRT's en het toezicht op regelgevingsmaatregelen in verband met cyberbeveiliging
- Aantal EU-brede goede praktijken voor kritieke infrastructuurvoorzieningen die worden verstrekt door het Enisa
- Aantal EU-brede goede praktijken voor kleine en middelgrote ondernemingen die worden verstrekt door het Enisa
- Bekendmaking door het Enisa van jaarlijkse strategische analyses van cyberdreigingen en -incidenten om nieuwe trends te constateren
- Regelmatige bijdrage van Enisa aan de werkzaamheden van de werkgroepen cyberbeveiliging van de Europese normalisatieorganisaties (ENO's)

Doelstelling: De samenwerking en de coördinatie tussen de lidstaten en de EU-instellingen, -agentschappen en -organen verbeteren:

- Aantal lidstaten dat bij het opstellen van hun beleid gebruik heeft gemaakt van de aanbevelingen en adviezen van het Enisa
- Aantal EU-instellingen, -agentschappen en -organen dat bij het opstellen van hun beleid gebruik heeft gemaakt van de aanbevelingen en adviezen van het Enisa
- Regelmatige uitvoering van het werkprogramma van het CSIRT-netwerk en de goede werking van de IT-infrastructuur en de communicatiekanalen van het

CSIRT-netwerk

- Aantal technische verslagen dat ter beschikking wordt gesteld aan en wordt gebruikt door de samenwerkingsgroep
- Consistente aanpak van de uitvoering van de NIS-richtlijn over de grenzen heen en in alle sectoren
- Aantal door het Enisa uitgevoerde beoordelingen van de naleving van de regelgeving
- Aantal opgerichte ISAC's in verschillende sectoren, met name voor kritieke infrastructuurvoorzieningen
- Oprichting en regelmatige toepassing van het informatieplatform waarmee informatie inzake cyberveiligheid wordt verspreid die afkomstig is van de EU-instellingen, agentschappen en andere organen
- Regelmatige bijdragen tot de voorbereiding van de werkprogramma's van de EU op het gebied van onderzoek en innovatie
- Samenwerkingsovereenkomst tussen het Enisa, EC3 en CERT-EU in werking
- Aantal door middel van het kader ontwikkelde certificeringsregelingen

Doelstelling: De vermogens op EU-niveau versterken ter aanvulling op maatregelen van de lidstaten, met name in het geval van grensoverschrijdende cybercrises:

- Bekendmaking door het Enisa van jaarlijkse strategische analyses van cyberdreigingen en -incidenten om nieuwe trends te constateren
- Bekendmaking van gebundelde informatie betreffende overeenkomstig de NIS-richtlijn bij het Enisa gemelde incidenten
- Aantal door het Agentschap gecoördineerde pan-Europese oefeningen en aantal daarbij betrokken lidstaten en organisaties.
- Aantal verzoeken om ondersteuning voor noodmaatregelen door de lidstaten aan het Enisa, waaraan het Agentschap gevolg heeft gegeven
- Aantal door het Enisa in samenwerking met CERT-EU uitgevoerde analyses van kwetsbare punten, artefacten en incidenten.
- Beschikbaarheid van EU-brede situatieverslagen die zijn gebaseerd op informatie die de lidstaten en andere entiteiten aan het Enisa ter beschikking hebben gesteld in het geval van grootschalige grensoverschrijdende cyberincidenten.

Doelstelling: Versterkt bewustzijn van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties:

- Regelmatige uitvoering van EU-brede en nationale voorlichtingscampagnes en regelmatig bijwerken van de onderwerpen daarvan naargelang van leerbehoeften die ontstaan.
- Versterken van het bewustzijn betreffende cyberkwesties bij de EU-burgers.
- Regelmatige uitvoering van een quiz met betrekking tot het bewustzijn van cyberbeveiliging en na verloop van tijd verhoging van het percentage juiste antwoorden.
- Regelmatige bekendmaking van goede praktijken op het gebied van cyberbeveiliging en cyberhygiëne, gericht op werknemers en organisaties.

Doelstelling: Het vertrouwen in de digitale eengemaakte markt en in digitale innovatie versterken door de algehele transparantie van de zekerheid inzake cyberbeveiliging[47] van ICT-producten en -diensten te verbeteren:

- Aantal regelingen dat voldoet aan het EU-kader
- Lagere kosten voor het verkrijgen van een certificaat betreffende ICT-beveiliging.
- Aantal conformiteitsbeoordelingsinstanties dat gespecialiseerd is in ICT-certificering, in alle lidstaten
- Oprichting van de Europese Groep voor cyberbeveiligingscertificering en organisatie van regelmatige vergaderingen
- Richtsnoeren voor certificering overeenkomstig het desbetreffende EU-kader
- Regelmatige bekendmaking van de voornaamste tendensen op de EU-markt voor cyberbeveiliging
- Aantal gecertificeerde ICT-producten en -diensten overeenkomstig de regels van het Europees kader voor ICT-cyberbeveiligingscertificering
- Toename van het aantal eindgebruikers dat zich bewust is van de beveiligingskenmerken van ICT-producten en -diensten

(b)

1.4.5. Behoefte(n) waarin op korte of lange termijn moet worden voorzien

Gezien de regelgevingsvereisten en de snelle ontwikkeling van het cyberdreigingslandschap moet het mandaat van het Enisa worden herzien en wordt een hernieuwde reeks taken en functies vastgesteld, met als doel doeltreffende en efficiënte ondersteuning van de inspanningen van de lidstaten, de EU-instellingen en andere belanghebbenden met betrekking tot het waarborgen van een veilige cyberspace in de Europese Unie. De voorgestelde werkingssfeer van het mandaat wordt afgebakend, waarbij de gebieden worden versterkt waarop het Agentschap blijk heeft gegeven van een duidelijke meerwaarde en nieuwe gebieden worden toegevoegd waarop ondersteuning nodig is gezien de nieuwe beleidsprioriteiten en instrumenten, met name de NIS-richtlijn, de herziening van de EU-cyberbeveiligingsstrategie, de blauwdruk voor de EU-cyberbeveiliging in verband met de samenwerking bij cybercrises alsmede de ICT-beveiligingscertificering. Met het nieuwe, in dit voorstel opgenomen mandaat wordt beoogd aan het Agentschap een sterkere en meer centrale rol toe te kennen, door onder meer de lidstaten actiever te ondersteunen door specifieke dreigingen aan te pakken (operationele capaciteit) en door een kenniscentrum te worden dat de lidstaten en de Commissie ondersteunt op het gebied van de certificering van cyberbeveiliging.

Tegelijkertijd wordt met de voorstellen een Europees kader voor cyberbeveiligingscertificering voor ICT-producten en -diensten tot stand gebracht en worden de essentiële functies en taken van het Enisa op het gebied van cyberbeveiligingscertificering gespecificeerd. Het kader omvat gemeenschappelijke bepalingen en procedures voor de totstandbrenging van EU-brede regelingen voor cyberbeveiligingscertificering voor specifieke ICT-producten/-diensten of cyberbeveiligingsrisico's. Europese regelingen voor cyberbeveiligingscertificering die in

[47] Transparantie van de zekerheid inzake cyberbeveiliging houdt in dat de gebruikers worden voorzien van voldoende informatie over cyberbeveiligingseigenschappen, waardoor zij in staat zijn het beveiligingsniveau van elk ICT-product, -dienst of -proces objectief te bepalen.

overeenstemming met het kader worden opgezet, zorgen ervoor dat volgens deze regelingen afgegeven certificaten in alle lidstaten geldig zijn en erkend worden en dat de huidige versnippering van de markt wordt aangepakt.

1.4.6. Toegevoegde waarde van de betrokkenheid van de Unie

Cyberbeveiliging is een daadwerkelijk mondiaal vraagstuk dat van nature grensoverschrijdend is en in steeds grotere mate sectoroverschrijdend wordt vanwege de onderlinge afhankelijkheid van netwerken en informatiesystemen. Het aantal cyberbeveiligingsincidenten, de complexiteit en de omvang ervan, alsmede de impact op de economie en de samenleving nemen steeds meer toe, en deze stijging wordt naar verwachting voortgezet naargelang van de technologische ontwikkelingen, bijvoorbeeld de verspreiding van het internet der dingen. Het kan derhalve niet worden verwacht dat de noodzaak van meer gemeenschappelijke inspanningen van de lidstaten, de EU-instellingen en particuliere belanghebbenden om cyberbeveiligingsdreigingen aan te pakken, in de toekomst afneemt.

Sinds het Enisa in 2004 is opgericht, heeft het zich gericht op de bevordering van de samenwerking tussen de lidstaten en de NIS-belanghebbenden, onder meer door ondersteuning te verlenen aan publiek-private samenwerking. De ondersteuning ten behoeve van samenwerking omvatte de technische werkzaamheden voor de totstandbrenging van een EU-breed overzicht van het dreigingslandschap, het opzetten van deskundigengroepen en de organisatie van pan-Europese oefeningen betreffende cyberincidenten en crisisbeheersing voor de overheids- en de particuliere sector (in het bijzonder "Cyber Europe"). Bij de NIS-richtlijn werden aan het Enisa bijkomende taken toevertrouwd, waaronder het verzorgen van het secretariaat voor het CSIRT-netwerk voor operationele samenwerking tussen de lidstaten.

De toegevoegde waarde van actie op EU-niveau, met name ter versterking van de samenwerking tussen de lidstaten, maar ook tussen de netwerk- en informatiebeveiligingsgemeenschappen, is erkend in de conclusies van de Raad van 2016[48] en blijkt duidelijk uit de evaluatie van het Enisa van 2017, waaruit blijkt dat de toegevoegde waarde van het Agentschap voornamelijk is dat het in staat is de samenwerking tussen deze belanghebbenden te versterken. Op EU-niveau is er geen andere actor die de samenwerking van een dergelijke variatie aan belanghebbenden op het gebied van netwerk- en informatiebeveiliging ondersteunt.

De toegevoegde waarde van het Enisa wat betreft het samenbrengen van cyberbeveiligingsgemeenschappen en belanghebbenden geldt ook op het gebied van certificering. Door de toename van cybercriminaliteit en beveiligingsdreigingen zijn nationale initiatieven tot stand gekomen op basis waarvan cyberbeveiligings- en certificeringseisen van hoog niveau worden vastgesteld voor ICT-componenten in traditionele infrastructuur. Hoewel deze initiatieven belangrijk zijn, bestaat het risico dat deze leiden tot versnippering van de interne markt en tot belemmeringen voor de interoperabiliteit. Een ICT-leverancier moet wellicht meerdere certificeringsprocedures doorlopen teneinde zijn producten in meerdere lidstaten te kunnen verkopen. Indien de EU niet optreedt, is het onwaarschijnlijk dat de inefficiëntie van de huidige certificeringsregelingen wordt weggewerkt. Indien maatregelen uitblijven, neemt de versnippering van de markt naar alle waarschijnlijkheid op middellange termijn (de

[48] Conclusies van de Raad over het versterken van het Europese cyberbeveiligingssysteem en het bevorderen van een concurrerende en innovatieve cyberbeveiligingsbranche - 15 november 2016.

volgende 5 tot 10 jaar) toe naarmate nieuwe certificeringsregelingen ontstaan. Het gebrek aan coördinatie en interoperabiliteit binnen dergelijke regelingen, is een element waardoor het potentieel van de digitale eengemaakte markt niet volledig wordt benut. Dat toont de toegevoegde waarde aan van het opzetten van een Europees kader voor cyberbeveiligingscertificering van ICT-producten en -diensten, waarmee de juiste voorwaarden worden geschapen voor een doeltreffende aanpak van de problemen in verband met het bestaan van meerdere certificeringsprocedures in de verschillende lidstaten, en de kosten voor certificering worden verlaagd, zodat certificering in de EU in het algemeen aantrekkelijker wordt vanuit commercieel en concurrentieel oogpunt.

1.4.7. Nuttige ervaring die bij soortgelijke activiteiten in het verleden is opgedaan

Overeenkomstig de rechtsgrondslag van het Enisa heeft de Commissie een evaluatie van het Agentschap verricht, waarbij een onafhankelijke studie en een openbare raadpleging zijn uitgevoerd. In de evaluatie werd geconcludeerd de doelstellingen van het Enisa nog steeds relevant zijn. In een klimaat van technologische ontwikkelingen en veranderende dreigingen, en van een grote behoefte aan versterkte netwerk- en informatiebeveiliging in de EU, is technische expertise op het gebied van de ontwikkeling van kwesties betreffende netwerk- en informatiebeveiliging van groot belang. De capaciteit in de lidstaten moet worden opgebouwd, zodat dreigingen juist worden ingeschat en er adequaat op wordt gereageerd, en de belanghebbenden moeten over de grenzen van thematische gebieden en instellingen heen samenwerken.

Het Agentschap heeft met succes bijgedragen tot het verbeteren van de netwerk- en informatiebeveiliging in Europa door capaciteitsopbouw in 28 lidstaten aan te bieden, te zorgen voor nauwere samenwerking tussen de lidstaten en de belanghebbenden op het gebied van netwerk- en informatiebeveiliging, en te voorzien in expertise, gemeenschapsopbouw en ondersteuning van de ontwikkeling van beleid.

Het Enisa is er weliswaar in geslaagd enige resultaten te boeken op het omvangrijke gebied van de netwerk- en informatiebeveiliging, maar het is er niet volledig in geslaagd een sterke merknaam te vestigen en voldoende bekendheid te verwerven om te worden erkend als het expertisecentrum in Europa bij uitstek. Dat is het gevolg van het feit dat het Enisa een breed mandaat heeft, maar niet beschikt over voldoende middelen. Daarnaast heeft het Enisa als enige EU-agentschap een tijdelijk mandaat, waardoor het slechts in beperkte mate een langetermijnvisie kan ontwikkelen en de belanghebbenden op duurzame wijze kan ondersteunen. Hiermee wordt afgeweken van de NIS-richtlijn, waarin is bepaald dat aan het Enisa taken zonder einddatum worden toevertrouwd.

Wat betreft cyberbeveiligingscertificering voor ICT-producten en -diensten bestaat er momenteel geen Europees kader. Door de toename van cybercriminaliteit en beveiligingsdreigingen zijn nationale initiatieven tot stand gekomen die het risico op versnippering van de eengemaakte markt met zich meebrengen.

1.4.8. Verenigbaarheid en eventuele synergie met andere passende instrumenten

Het initiatief is in hoge mate in overeenstemming met het bestaande beleid, met name op het gebied van de interne markt. De opzet ervan sluit aan op de algemene aanpak van cyberbeveiliging die is omschreven in de evaluatie van de strategie voor de digitale eengemaakte markt, ter aanvulling van een uitgebreid pakket aan maatregelen, zoals de herziening van de cyberbeveiligingsstrategie van de EU, de blauwdruk voor de samenwerking bij cybercrises en de initiatieven ter bestrijding van cybercriminaliteit. Het initiatief waarborgt aanpassing aan de bepalingen van de bestaande wetgeving inzake

cyberbeveiliging en bouwt erop voort, met name op de NIS-richtlijn, teneinde de cyberweerbaarheid van de EU te verbeteren door middel van versterkte vermogens, samenwerking, risicobeheer en cyberbewustzijn.

De voorgestelde certificeringsmaatregelen dienen de potentiële versnippering als gevolg van bestaande en nieuwe nationale certificeringsregelingen aan te pakken en daardoor bij te dragen tot de ontwikkeling van de digitale eengemaakte markt. Het initiatief dient verder als ondersteuning van en aanvulling op de uitvoering van de NIS-richtlijn doordat de aan de richtlijn onderworpen ondernemingen de beschikking krijgen over een instrument voor het aantonen van de naleving van de NIS-vereisten in de hele Unie.

Het voorgestelde Europees kader voor ICT-cyberbeveiligingscertificering doet geen afbreuk aan de algemene verordening gegevensbescherming[49], en met name niet aan de relevante bepalingen inzake certificering[50] aangezien deze van toepassing zijn op de beveiliging van de verwerking van persoonsgegevens. Tot slot moeten de regelingen van het toekomstige Europees kader zoveel mogelijk steunen op internationale normen om het ontstaan van handelsbelemmeringen te vermijden en samenhang met internationale initiatieven te waarborgen.

[49] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

[50] Zoals de artikelen 42 (certificering) en 43 (certificeringsorganen) alsmede de artikelen 57, 58 en 70 betreffende respectievelijk de relevante taken en bevoegdheden van de onafhankelijke toezichthoudende autoriteiten en de taken van het Europees Comité voor gegevensbescherming.

1.5. Duur en financiële gevolgen

☐ Voorstel/initiatief met een **beperkte geldigheidsduur**

– ☐ Voorstel/initiatief is van kracht vanaf [DD/MM]JJJJ tot en met [DD/MM]JJJJ

– ☐ Financiële gevolgen vanaf JJJJ tot en met JJJJ

☒ Voorstel/initiatief met een **onbeperkte geldigheidsduur**

– Uitvoering met een opstartperiode vanaf 2019 tot en met 2020,

– gevolgd door een volledige uitvoering.

1.6. Beheersvorm(en)[51]

☒ **Direct beheer** door de Commissie (titel III – Certificering)

– ☐ uitvoerende agentschappen

☐ **Gedeeld beheer** met de lidstaten

☒ **Indirect beheer** door begrotingsuitvoeringstaken te delegeren aan:

☐ internationale organisaties en hun agentschappen (geef aan welke);

☐ de EIB en het Europees Investeringsfonds;

☒ de in de artikelen 208 en 209 bedoelde organen (titel II – Enisa);

☐ publiekrechtelijke organen;

☐ privaatrechtelijke organen met een openbaredienstverleningstaak, voor zover zij voldoende financiële garanties bieden;

☐ privaatrechtelijke organen van een lidstaat, waaraan de uitvoering van een publiek-privaat partnerschap is toevertrouwd en die voldoende financiële garanties bieden;

☐ personen aan wie de uitvoering van specifieke maatregelen op het gebied van het GBVB in het kader van titel V van het VEU is toevertrouwd en die worden genoemd in de betrokken basishandeling.

Opmerkingen

De verordening heeft betrekking op:

- In titel II van de voorgestelde verordening wordt het mandaat van het European Union Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) herzien en krijgt het een belangrijke rol op het gebied van certificering.

- In titel III wordt een kader vastgesteld voor de totstandbrenging van Europese regelingen voor cyberbeveiligingscertificering van ICT-producten en -diensten, waarbij het Enisa een cruciale rol speelt.

[51] Nadere gegevens over de beheersvormen en verwijzingen naar het Financieel Reglement zijn beschikbaar op BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. BEHEERSMAATREGELEN

2.1. Regels inzake het toezicht en de verslagen

Vermeld frequentie en voorwaarden.

Het toezicht zal meteen na de vaststelling van het rechtsinstrument van start gaan en het accent zal liggen op de toepassing ervan. De Commissie zal bijeenkomsten met het Enisa, vertegenwoordigers van de lidstaten (bijv. groep van deskundigen) en de relevante belanghebbenden organiseren, met name om de uitvoering van de regels inzake certificering te vergemakkelijken, zoals de oprichting van de raad van bestuur.

De eerste evaluatie zal vijf jaar na de inwerkingtreding van het rechtsinstrument plaatsvinden, mits er voldoende gegevens beschikbaar zijn. In het rechtsinstrument is een expliciete clausule inzake toetsing en evaluatie [artikel XXX] opgenomen, op grond waarvan de Commissie een onafhankelijke evaluatie zal uitvoeren. De Commissie zal vervolgens aan het Europees Parlement en de Raad verslag uitbrengen over haar evaluatie en wanneer passend een voorstel voor herziening doen, teneinde de gevolgen van de verordening en de toegevoegde waarde ervan te meten. Verdere evaluaties zullen om de vijf jaar plaatsvinden. De evaluatiemethodiek van de Commissie inzake betere regelgeving zal worden toegepast. Deze evaluaties zullen worden verricht met behulp van doelgerichte discussies onder deskundigen, studies en brede raadplegingen van de belanghebbenden.

De uitvoerend directeur van het Enisa om de twee jaar een ex-postevaluatie van de activiteiten van het Enisa aan de raad van bestuur verstrekken. Het Agentschap moet verder een actieplan als follow-up van ex-postevaluaties en om de twee jaar een voortgangsrapportage aan de Commissie opstellen. De raad van bestuur zal verantwoordelijk zijn voor het toezicht op de follow-up van dergelijke conclusies.

Overeenkomstig de bepalingen van artikel 228 van het Verdrag kunnen vermeende gevallen van wanbeheer bij de activiteiten van het Agentschap worden onderzocht door de Europese Ombudsman.

De gegevensbronnen voor het geplande toezicht zijn voornamelijk het Enisa, de Europese Groep voor cyberbeveiligingscertificering, de samenwerkingsgroep, het CSIRT-netwerk en de autoriteiten van de lidstaten. Naast de gegevens afkomstig uit de verslagen (waaronder de jaarlijkse activiteitenverslagen) van het Enisa, de Europese Groep voor cyberbeveiligingscertificering, de samenwerkingsgroep en het CSIRT-netwerk, zullen indien nodig specifieke instrumenten voor het verzamelen van gegevens worden gebruikt (bijvoorbeeld enquêtes door nationale autoriteiten, Eurobarometer-enquêtes en verslagen van de maand van de cyberbeveiliging en de pan-Europese oefeningen).

2.2. Beheers- en controlesysteem

2.2.1. Mogelijke risico's

De geïdentificeerde risico’s zijn beperkt: er bestaat reeds een EU-agentschap en het mandaat ervan zal worden afgebakend, waarbij de gebieden worden versterkt waarop het Agentschap blijk heeft gegeven van een duidelijke meerwaarde en nieuwe gebieden worden toegevoegd waarop ondersteuning nodig is gezien de nieuwe beleidsprioriteiten en -instrumenten, met

name de NIS-richtlijn, de herziening van de EU-cyberbeveiligingsstrategie, de op stapel staande blauwdruk voor de EU-cyberbeveiliging in verband met de samenwerking bij cybercrises alsmede de ICT-beveiligingscertificering.

Het voorstel omvat derhalve details over de functies van het Agentschap, en het leidt tot efficiëntieverbeteringen. De uitbreiding van de operationele bevoegdheden en taken vormt geen reëel risico, aangezien hierdoor het optreden van de lidstaten, op hun verzoek en enkel met betrekking tot beperkte en vooraf bepaalde diensten, wordt aangevuld en ondersteund.

Bovendien wordt, overeenkomstig de gemeenschappelijke aanpak, door het voorgestelde model van het agentschap gewaarborgd dat er afdoende controle plaatsvindt om ervoor te zorgen dat het Enisa zijn doelstellingen nastreeft. De operationele en financiële risico's van de voorgestelde wijzigingen lijken beperkt te zijn.

Tegelijkertijd moet worden gezorgd voor adequate financiële middelen, zodat het Enisa de taken kan uitvoeren die op grond van het nieuwe mandaat aan hem zijn toevertrouwd, waaronder op het gebied van certificering.

2.2.2. Controlemiddel(en)

De rekeningen van het Agentschap worden ter goedkeuring aan de Rekenkamer voorgelegd en worden onderworpen aan de kwijtingsprocedure. Er zullen audits plaatsvinden.

De activiteiten van het Agentschap staan onder toezicht van de Ombudsman overeenkomstig de bepalingen van artikel 228 van het Verdrag.

Zie tevens de punten 2.1 en 2.2.1 hierboven.

2.3. Maatregelen ter voorkoming van fraude en onregelmatigheden

Vermeld de bestaande en geplande preventie- en beschermingsmaatregelen.

De preventie- en beschermingsmaatregelen van het Enisa zullen van toepassing zijn, met name:

- De rekeningen voor alle uitbestede diensten en studies worden door het personeel van het Agentschap vóór de feitelijke uitbetaling gecontroleerd, met inachtneming van eventuele contractuele verplichtingen, economische beginselen en goede financiële of beheerspraktijken. In alle overeenkomsten en contracten tussen het Agentschap en de begunstigden van eventuele betalingen worden fraudebestrijdingsbepalingen (eisen ten aanzien van toezicht, verslaglegging enz.) opgenomen.

- Met het oog op de bestrijding van fraude, corruptie en andere illegale handelingen zijn de bepalingen van Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad van 25 mei 1999 betreffende onderzoeken door het Europees Bureau voor fraudebestrijding (OLAF) onverminderd van toepassing.

- Het Agentschap zal binnen zes maanden vanaf de datum van inwerkingtreding van deze verordening toetreden tot het Interinstitutioneel Akkoord van 25 mei 1999 tussen het Europees Parlement, de Raad van de Europese Unie en de Commissie van de Europese Gemeenschappen betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF) en stelt onverwijld de passende voorschriften vast die van toepassing zijn op alle medewerkers van het Agentschap.

3. GERAAMDE FINANCIËLE GEVOLGEN VAN HET VOORSTEL/INITIATIEF

3.1. Rubriek(en) van het meerjarig financieel kader en betrokken begrotingsonderde(e)l(en) voor uitgaven

- Bestaande begrotingsonderdelen

In volgorde van de rubrieken van het meerjarig financieel kader en de begrotingsonderdelen.

Rubriek van het meerjarig financieel kader	Begrotingsonderdeel	Soort krediet	Bijdrage			
		GK/NGK[52]	van EVA-landen[53]	van kandidaat-lidstaten[54]	van derde landen	in de zin van artikel 21, lid 2, onder b), van het Financieel Reglement
1a Concurrentievermogen ter bevordering van groei en werkgelegenheid	09.0203 Enisa en Veiligheidscertificering van informatie- en communicatietechnologie	GK	JA	NEE	NEE	NEE
5 Administratieve uitgaven	09 01 01 Uitgaven voor personeel in actieve dienst voor het beleidsterrein Communicatienetwerken, inhoud en technologie 09 01 02 Uitgaven voor extern personeel in actieve dienst voor het	NGK	NEE	NEE	NEE	NEE

[52] GK = gesplitste kredieten/NGK = niet-gesplitste kredieten.
[53] EVA: Europese Vrijhandelsassociatie.
[54] Kandidaat-lidstaten en, in voorkomend geval, potentiële kandidaten van de Westelijke Balkan.

	beleidsterrein Communicatienetwerken, inhoud en technologie 09 01 02 11 Andere beheersuitgaven					

3.2. Geraamde gevolgen voor de uitgaven

3.2.1. Samenvatting van de geraamde gevolgen voor de uitgaven

in miljoenen euro's (tot op drie decimalen)

Rubriek van het meerjarig financieel kader	1a	Concurrentievermogen ter bevordering van groei en werkgelegenheid

Enisa			**Basisscenario** 2017 (31.12.2016)	**2019** *(vanaf 1.7.2019)*	**2020**	**2021**	**2022**	**TOTAAL**
Titel 1: Personeelsuitgaven *(met inbegrip van uitgaven in verband met de aanwerving van personeel, opleiding, infrastructuur van medisch-sociale aard en externe dienstverlening)*	Vastleggingen	(1)	6,387	9,899	12,082	13,349	13,894	**49,224**
	Betalingen	(2)	6,387	9,899	12,082	13,349	13,894	**49,224**
Titel 2: Infrastructuur- en operationele uitgaven	Vastleggingen	(1a)	1,770	1,957	2,232	2,461	2,565	**9,215**
	Betalingen	(2a)	1,770	1,957	2,232	2,461	2,565	**9,215**
Titel 3: Operationele uitgaven	Vastleggingen	(3a)	3,086	4,694	6,332	6,438	6,564	**24,028**
	Betalingen	(3b)	3,086	4,694	6,332	6,438	6,564	**24,028**
TOTAAL kredieten voor het Enisa	Vastleggingen	=1+1a +3a	**11,244**	16,550	20,646	22,248	23,023	**82,467**
	Betalingen	=2+2a +3b	**11,244**	**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Rubriek van het meerjarig financieel kader	**5**	"Administratieve uitgaven"

in miljoenen euro's (tot op drie decimalen)

		2019 *(vanaf 1.7.2019)*	**2020**	**2021**	**2022**	**TOTAAL**
DG: CNECT						
• Personele middelen		0,216	0,846	0,846	0,846	**2,754**
• Andere administratieve uitgaven		0,102	0,235	0,238	0,242	**0,817**
TOTAAL DG CNECT	Kredieten	0,318	1,081	1,084	1,088	**3,571**

De personeelskosten zijn berekend op basis van de geplande datum van indiensttreding (tewerkstelling is gepland vanaf 1.7.2019).

De vooruitzichten voor deze middelen voor de periode na 2020 zijn indicatief en onder voorbehoud van de voorstellen van de Commissie voor het meerjarig financieel kader voor de periode na 2020.

TOTAAL kredieten onder RUBRIEK 5 van het meerjarig financieel kader	(totaal vastleggingen = totaal betalingen)	0,318	1,081	1,084	1,088	**3,571**

in miljoenen euro's (tot op drie decimalen)

	2019	**2020**	**2021**	**2022**	**TOTAAL**

TOTAAL kredieten onder de RUBRIEKEN 1 tot en met 5 van het meerjarig financieel kader	Vastleggingen	16,868	21,727	23,332	24,11	**86,038**
	Betalingen	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Geraamde gevolgen voor de kredieten van het Agentschap

– ☐ Voor het voorstel/initiatief zijn geen beleidskredieten nodig

– ☒ Voor het voorstel/initiatief zijn beleidskredieten nodig, zoals hieronder nader wordt beschreven:

Vastleggingskredieten, in miljoenen euro's (tot op drie decimalen)

Vermeld doelstellingen en outputs[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTAAL**
De vermogens en paraatheid van de lidstaten en het bedrijfsleven verhogen	1,408	1,900	1,931	1,969	7,208
De samenwerking en de coördinatie tussen de lidstaten en de EU-instellingen, -agentschappen en -organen verbeteren.	0,939	1,266	1,288	1,313	4,806
De vermogens op EU-niveau versterken ter aanvulling op maatregelen van de lidstaten, met name in het geval van grensoverschrijdende cybercrises.	0,704	0,950	0,965	0,985	3,604
Het bewustzijn van de burgers en het bedrijfsleven met betrekking tot cyberbeveiligingskwesties versterken.	0,704	0,950	0,965	0,985	3,604
Het vertrouwen in de digitale eengemaakte markt en in digitale innovatie versterken door de algehele transparantie van de zekerheid inzake cyberbeveiliging van ICT-producten en -diensten te verbeteren.	0,939	1,266	1,288	1,313	4,806
TOTALE KOSTEN	4,694	6,332	6,437	6,565	24,028

[55] In deze tabel worden alleen de operationele uitgaven van titel 3 weergegeven.

3.2.3. Geraamde gevolgen voor het personeel van het Agentschap

3.2.3.1. Samenvatting

– ☐ Voor het voorstel/initiatief zijn geen administratieve kredieten nodig

– ☒ Voor het voorstel/initiatief zijn administratieve kredieten nodig, zoals hieronder nader wordt beschreven:

in miljoenen euro's (tot op drie decimalen)

	K3/4 2019	**2020**	**2021**	**2022**
Tijdelijke functionarissen (AD)	4,242	5,695	6,381	6,709
Tijdelijke functionarissen (AST)	1,601	1,998	2,217	2,217
Arbeidscontractanten	2,041	2,041	2,041	2,041
Gedetacheerde nationale deskundigen	0,306	0,447	0,656	0,796
TOTAAL	**8,190**	**10,181**	**11,295**	**11,763**

De personeelskosten zijn berekend op basis van de geplande datum van indiensttreding (voor het huidige personeel van het Enisa werd uitgegaan van een volledige tewerkstelling vanaf 1.1.2019). Voor het nieuwe personeel werd uitgegaan van een geleidelijke tewerkstelling vanaf 1.7.2019 en een volledige tewerkstelling in 2022. De vooruitzichten voor deze middelen voor de periode na 2020 zijn indicatief en onder voorbehoud van de voorstellen van de Commissie voor het meerjarige financiële kader voor de periode na 2020.

Geraamde gevolgen voor het personeel (aanvullende VTE) – lijst van het aantal ambten

Functiegroep en rang	2017 **Huidige Enisa**	K3/K4 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
Totaal AD	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Totaal AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Totaal AST/SC					
EINDTOTAAL	48	12	10	7	3

De taken van het extra AD/AST-personeel met het oog op de doelstellingen van het instrument, zoals beschreven in punt 1.4.2:

Taken	AD	AST	GND	Totaal
Beleids- en capaciteitsopbouw	8	1		9
Operationele samenwerking	8	1	7	16
Certificering (marktgerelateerde taken)	9	3	2	14
Kennis, informatie en bewustmaking	1	1		2
TOTAAL	26	6	9	41

Beschrijving van de uit te voeren taken:

Taken	**Vereiste bijkomende middelen**
Ontwikkeling en uitvoering van EU-beleid en capaciteitsopbouw	Hierbij gaat het om taken zoals bijstand verlenen aan de samenwerkingsgroep; de consistente uitvoering van de NIS-richtlijn over de grenzen heen ondersteunen; regelmatig verslag uitbrengen over de stand van uitvoering van het EU-wetgevingskader; een adviserende en coördinerende rol vervullen voor sectorale initiatieven op het gebied van cyberbeveiliging, onder meer met betrekking tot energie, vervoer (bv. luchtvaart/weg-/zeevervoer/ verbonden voertuigen), gezondheid, financiën; en steun

	verlenen aan de oprichting van centra voor informatie-uitwisseling en -analyse (ISAC's) in verschillende sectoren.
Operationele samenwerking en crisisbeheersing	**Hierbij gaat het om taken zoals:** Zorgen voor het secretariaat van het CSIRT-netwerk door onder meer te waarborgen dat de IT-infrastructuur en de communicatiekanalen van het CSIRT-netwerk goed werken. Zorgen voor een gestructureerde samenwerking met CERT-EU, EC3 en andere relevante EU-organen. Taken in het kader van **Cyber Europe-oefeningen**[56] organiseren met als doel de oefening jaarlijks in plaats van tweejaarlijks te organiseren en ervoor te zorgen dat een incident van begin tot einde aan bod komt tijdens de oefeningen. **Technische bijstand -** hierbij gaat het om taken zoals een gestructureerde samenwerking met CERT-EU tot stand brengen om technische bijstand te verlenen in geval van significante incidenten en de analyse van incidenten te ondersteunen. Dit houdt onder meer in dat er ondersteuning wordt geboden aan de lidstaten om incidenten aan te pakken en zwakke punten, artefacten en incidenten te analyseren. De samenwerking tussen de afzonderlijke lidstaten vergemakkelijken wat betreft de aanpak van noodmaatregelen door analyse en bundeling van nationale situatieverslagen, op basis van informatie die door de lidstaten en andere entiteiten aan het Agentschap ter beschikking wordt gesteld. **Blauwdruk voor een gecoördineerde respons op grootschalige grensoverschrijdende cyberincidenten** - het agentschap zal bijdragen tot de ontwikkeling van een gezamenlijke respons, op het niveau van de Unie en van de lidstaten, op grootschalige grensoverschrijdende incidenten of crises in verband met cyberbeveiliging door middel van een reeks taken, van het bijdragen aan de totstandbrenging van een situatiebewustzijn op Unieniveau tot het

[56] Cyber Europe is de grootste en meest uitgebreide cyberbeveiligingsoefening op EU-niveau tot dusver, waarbij meer dan 700 deskundigen op het gebied van cyberbeveiliging uit alle 28 lidstaten zijn betrokken. De oefening wordt om de twee jaar georganiseerd. Uit de evaluatie van het Enisa en de EU-strategie voor cyberbeveiliging van 2013 blijkt dat veel belanghebbenden Cyber Europe willen uitbreiden tot een jaarlijks evenement, gezien de snel veranderende aard van cyberdreigingen. Momenteel is dit echter niet haalbaar vanwege de beperkte middelen van het agentschap.

	testen van de samenwerkingsplannen voor incidenten. **Technisch ex-postonderzoek van incidenten** - technisch ex-postonderzoek van incidenten uitvoeren of hieraan bijdragen in samenwerking met het CSIRT-netwerk met als doel aanbevelingen uit te vaardigen en de vermogens te versterken in de vorm van openbare verslagen om toekomstige incidenten beter te voorkomen.
Marktgerelateerde taken (normalisatie, certificering)	Hierbij gaat het om taken zoals de verrichte werkzaamheden binnen het certificeringskader actief ondersteunen, onder meer door te voorzien in technische expertise om potentiële Europese regelingen voor cyberbeveiligingscertificering voor te bereiden. Hierbij gaat het ook om taken zoals ondersteuning bieden aan de ontwikkeling en uitvoering van het beleid van de Unie op het gebied van normalisatie, certificering en waarnemingsposten - hiervoor moet het gebruik van risicobeheernormen voor elektronische producten, netwerken en diensten worden bevorderd en moeten digitaledienstverleners worden geadviseerd over eisen inzake technische beveiliging. Hierbij gaat het ook om taken zoals de voornaamste tendensen op de markt voor cyberveiligheid analyseren.
Kennis en informatie, voorlichting:	Met het oog op het waarborgen van gemakkelijkere toegang tot beter gestructureerde informatie over cyberbeveiligingsrisico's en potentiële oplossingen wordt in het voorstel een nieuwe taak toevertrouwd aan het agentschap, namelijk de ontwikkeling en instandhouding van het "informatiecentrum" van de Unie. De taken houden onder meer in dat door de EU-instellingen, -agentschappen en -organen verstrekte informatie over de beveiliging van netwerk- en informatiesystemen, met name over cyberbeveiliging, wordt gebundeld, georganiseerd en openbaar wordt gemaakt door middel van een hiervoor bestemd portaal. Hierbij gaat het ook om taken zoals ondersteuning bieden aan de activiteiten van het Enisa op het gebied van voorlichting zodat het agentschap de inspanningen kan opvoeren.

3.2.3.2. Geraamde behoefte aan personele middelen voor het verantwoordelijke DG

– ☐ Voor het voorstel/initiatief zijn geen personele middelen nodig.

– ☒ Voor het voorstel/initiatief zijn personele middelen nodig, zoals hieronder nader wordt beschreven:

Raming in een geheel getal (of met hoogstens 1 decimaal)

		Extra personeel			
	Basisscenario 2017	K3/4 2019	2020	2021	2020
• **Posten opgenomen in de lijst van het aantal ambten (ambtenaren en tijdelijke functionarissen)**					
09 01 01 01 (zetel en vertegenwoordigingen van de Commissie)	1	2	3		
• **Extern personeel (in voltijdequivalenten - VTE)**[57]					
09 01 02 01 (AC, END, INT van de "totale financiële middelen")	1	2			
TOTAAL		**4**	**3**		

Beschrijving van de uit te voeren taken:

Ambtenaren en tijdelijk personeel	De Commissie vertegenwoordigen in de raad van bestuur van het agentschap. Het advies van de Commissie over het enig programmeringsdocument van het Enisa opstellen en toezien op de uitvoering ervan. Op de opstelling van de begroting van het agentschap toezien en de uitvoering ervan monitoren. Het agentschap bijstaan bij de ontwikkeling van zijn activiteiten in overeenstemming met het EU-beleid, onder meer door relevante vergaderingen bij te wonen. Toezien op de uitvoering van het kader voor Europese regelingen voor cyberbeveiligingscertificering van ICT-producten en -diensten. Contacten onderhouden met de lidstaten en andere relevante belanghebbenden over de inspanningen op het gebied van certificering. Samenwerken met het Enisa in verband met potentiële regelingen. Potentiële Europese regelingen voor cyberbeveiligingscertificering

[57] AC = Agent Contractuel (arbeidscontractant); AL = Agent Local (plaatselijk functionaris); END = Expert National Détaché (gedetacheerd nationaal deskundige); INT= Intérimaire (uitzendkracht); JED = Jeune Expert en Délégation (jonge deskundige in delegaties).

	voorbereiden.
Extern personeel	Zie hierboven

3.2.4. Verenigbaarheid met het huidige meerjarig financieel kader

– ☐ Het voorstel/initiatief is verenigbaar met het huidige meerjarig financieel kader

– ☒ Het voorstel/initiatief vergt herprogrammering van de betrokken rubriek van het meerjarig financieel kader

Het voorstel vergt herprogrammering van artikel 09 02 03 als gevolg van de herziening van het mandaat van het Enisa, waarbij het agentschap wordt belast met nieuwe taken, onder meer met betrekking tot de uitvoering van de NIS-richtlijn en het Europees kader voor cyberbeveiligingscertificering. De overeenkomstige bedragen:

Jaar	Gepland	Verzoek
2019	10,739	16,550
2020	10,954	20,646
2021	n.v.t.	22,248*
2022	n.v.t.	23,023*

* Dit is een raming. De EU-financiering na 2020 zal aan de orde komen in een debat in de hele Commissie over alle voorstellen voor de periode na 2020. Dit betekent dat de Commissie, zodra zij haar voorstel voor het volgende meerjarige financiële kader heeft ingediend, een gewijzigd financieel memorandum zal presenteren waarin rekening wordt gehouden met de conclusies van de effectbeoordeling[58].

– ☐ Het voorstel/initiatief vergt toepassing van het flexibiliteitsinstrument of herziening van het meerjarig financieel kader[59]

3.2.5. Bijdragen van derden

– ☐ Het voorstel/initiatief voorziet niet in medefinanciering door derden.

– ☒ Het voorstel/initiatief voorziet in medefinanciering, zoals hieronder wordt geraamd:

[58] Link naar de pagina met de effectbeoordeling.

[59] Zie de artikelen 11 en 17 van Verordening (EU, Euratom) nr. 1311/2013 van de Raad tot bepaling van het meerjarig financieel kader voor de jaren 2014-2020.

	Jaar **2019**	Jaar **2020**	Jaar **2021**	Jaar **2022**
EVA	p.m[60].	p.m.	p.m.	p.m.

3.3. Geraamde gevolgen voor de ontvangsten

– ☒ Het voorstel/initiatief heeft geen financiële gevolgen voor de ontvangsten.

– ☐ Het voorstel/initiatief heeft de hieronder beschreven financiële gevolgen:

  – ☐ voor de eigen middelen

  – ☐ voor de diverse ontvangsten

[60] Het precieze bedrag voor de volgende jaren zal bekend zijn wanneer de evenredigheidsfactor van de EVA voor het betrokken jaar wordt vastgesteld.