Raad van de
Europese Unie

Brussel, 29 mei 2018
(OR. en)

9350/18

Interinstitutioneel dossier:
2017/0225 (COD)

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

NOTA

van:	het voorzitterschap
aan:	de Raad
nr. vorig doc.:	8834/18
Nr. Comdoc.:	12183/17
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") - Algemene oriëntatie

I. INLEIDING

1. Op 13 september 2017 heeft de Commissie bovengenoemd voorstel[1] met artikel 114 VWEU als rechtsgrond in het kader van haar strategie voor een digitale eengemaakte markt aangenomen en aan de Raad en het Europees Parlement voorgelegd. Het voorstel maakt deel uit van het zogenoemd cyberbeveiligingspakket en moet leiden tot een hoog niveau van cyberbeveiliging, cyberveerkracht en vertrouwen binnen de Unie opdat de interne markt goed functioneert.

2. De voorgestelde verordening bepaalt de doelstellingen, taken en organisatorische aspecten van Enisa, het agentschap van de Europese Unie voor cyberbeveiliging, en schept een kader voor het opzetten van Europese regelingen voor cyberbeveiligingscertificering om te zorgen voor een passend cyberbeveiligingsniveau van ICT-producten en diensten in de Unie. Het Commissievoorstel gaat vergezeld van een effectbeoordeling, waarin een verzameling van acht beleidsopties nader wordt bezien, onder meer de evaluatie van Enisa en de cyber-beveiligingscertificering voor ICT-producten en -diensten.

3. Het verordeningsvoorstel bevat twee hoofdonderdelen:

   - een permanent mandaat voor het agentschap met een afgebakende werkingssfeer die is afgestemd op de behoeften in het kader van de nieuwe beleidsprioriteiten en -instrumenten, en een vernieuwd pakket van taken en functies voor het agentschap, dat het in staat stelt doeltreffende en efficiënte steun te verlenen aan de inspanningen van de lidstaten, de EU-instellingen en andere belanghebbenden om een veilige cyberspace te waarborgen;

   - een Europees kader voor de cyberbeveiligingscertificering van ICT-producten en -diensten en regels voor Europese regelingen voor cyberbeveiligingscertificering, zodat certificaten in het kader van die regelingen in alle lidstaten geldig zijn en worden erkend en zodat de huidige versnippering van de markt wordt tegengegaan.

[1] Doc. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. De Europese Raad pleitte er in oktober 2017 voor dat[2] de Commissievoorstellen inzake cyberbeveiliging op een holistische wijze worden ontwikkeld, tijdig worden ingediend en onverwijld worden behandeld, in overeenstemming met een door de Raad op te stellen actieplan.

5. De Raad Algemene Zaken hechtte op 12 december 2017 zijn goedkeuring aan het actieplan[3] voor de uitvoering van de conclusies van de Raad[4] over de gezamenlijke mededeling[5] aan het Europees Parlement en de Raad: "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU". Het actieplan vormde een weerspiegeling van de ambitie van de Raad om tegen juni 2018 met een algemene oriëntatie over het voorstel te komen.

6. In het Europees Parlement is mevrouw Angelika NIEBLER (ITRE, EPP) als rapporteur aangewezen. De stemming in de Commissie ITRE over haar verslag is gepland op 19 juni 2018.

7. Het Europees Economisch en Sociaal Comité heeft zijn advies op 14 februari 2018 vastgesteld.

II. BESPREKINGEN IN DE RAAD

8. De Commissie heeft haar voorstel en effectbeoordeling op 26 september 2017 voorgelegd aan de Groep cybervraagstukken (hierna "de groep" genoemd), die de effectbeoordeling op 20 oktober 2017 heeft besproken. Tijdens de daaropvolgende besprekingen is aandacht besteed aan de operationele capaciteit van het agentschap en de reikwijdte van de wisselwerking met de nationale bevoegde instanties, alsmede aan de gevolgen van het certificeringskader voor de markt en het concurrentievermogen van bedrijven. In het algemeen is zowel de effectbeoordeling als het voorstel gunstig onthaald door de delegaties.

---

2 EUCO 14/17, punt 11.
3 Doc. 15748/17.
4 Doc. 14435/17.
5 Doc. 12211/17.

9. De groep startte de bespreking van het voorstel zelf in november 2017 onder het Estse voorzitterschap en zette die onder het Bulgaarse voorzitterschap voort. Over het voorstel zijn 12 vergaderingen georganiseerd, die resulteerden in acht opeenvolgende herziene versies van het voorstel met het oog op overeenstemming over een algemene oriëntatie tijdens de Raad TTE op 8 juni 2018.

10. Het resultaat van de besprekingen in de groep tijdens de vergadering van 14 en 15 mei 2018 en de herziene compromistekst van het voorzitterschap staan in de bijlage bij deze nota. De overwegingen zijn gewijzigd om rekening te houden met de wijzigingen in de materiële bepalingen. Alle wijzigingen ten opzichte van het Commissievoorstel zijn **vetgedrukt** en met […] weergegeven. De wijzigingen in vergelijking met het meest recente document van de groep, namelijk ST 8834/18, zijn **vetgedrukt en onderstreept** en alle schrappingen zijn aangegeven met **[...]**.

III. CONCLUSIE

11. De compromistekst van het voorzitterschap in bijlage dezes weerspiegelt de inspanningen van het voorzitterschap en de lidstaten om in de tekst een juist evenwicht te vinden.

12. Het Comité van permanente vertegenwoordigers heeft op 25 mei 2018 overeenstemming bereikt over de compromistekst van het voorzitterschap, onder voorbehoud van de in de bijlage opgenomen wijzigingen in artikel 19, lid 5, en artikel 48, lid 5.

13. De Raad wordt derhalve verzocht tijdens zijn zitting op 8 juni een algemene oriëntatie vast te stellen en het voorzitterschap het mandaat te verlenen om over dit dossier met de vertegenwoordigers van het Europees Parlement en de Europese Commissie te onderhandelen.

BIJLAGE

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[6],

Gezien het advies van het Comité van de Regio's[7],

Handelend volgens de gewone wetgevingsprocedure,

[6] PB C , blz.
[7] PB C , blz.

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 cyber-beveiligingskenmerken 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 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. Voorts 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 cyber–dreigingen 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 doordat transparante informatie wordt verstrekt 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[8] 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[9] vastgesteld, waarbij het mandaat van het Agentschap werd verlengd tot maart 2012. Bij Verordening (EU) nr. 580/2011[10] werd het mandaat van het Agentschap tot 13 september 2013 verlengd. In 2013 hebben het Europees Parlement en de Raad Verordening (EU) nr. 526/2013[11] inzake Enisa en tot intrekking van (EG) nr. 460/2004 vastgesteld, waarbij het mandaat van het Agentschap tot juni 2020 werd verlengd

---

8 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).

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

10 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).

11 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 (PB L 165 van 18.6.2013, blz. 41).

(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. Opdat 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 digitaledienstaanbieders (zoekmachines, cloudcomputingdiensten en onlinemarktplaatsen). Aan Enisa werd een cruciale rol toegewezen bij 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 Enisa worden herzien teneinde de rol ervan 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 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 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 Europese instellingen, instanties 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 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 werven 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 **nationale inspanningen ondersteunen en** proactief bijdragen tot nationale en EU-inspanningen en daarbij zijn taken uitvoeren in nauwe samenwerking met de instellingen, organen **en** instanties [...] van de Unie en de lidstaten. Voorts 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 [...] **en haar sectorspecifieke aspecten teneinde EU-beleid en -recht met een cyberveiligings-dimensie relevanter te maken en te zorgen voor een consistente tenuitvoerlegging ervan op nationaal niveau**. 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, instanties **en organen** [...] van de Unie assisteren bij hun inspanningen om vermogens en paraatheid te ontwikkelen en te vergroten om problemen en incidenten op het gebied van cyber[...]**dreigingen** 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 opdat deze in de Unie een hoog gemeenschappelijk maturiteitsniveau bereiken. **Door Enisa verrichte activiteiten in verband met de operationele vermogens van de lidstaten moeten alleen complementair zijn met de door de lidstaten ondernomen eigen acties ter nakoming van hun verplichtingen uit hoofde van de NIS-richtlijn en mogen daarvoor niet in de plaats komen.**[...]

(15a) Het Agentschap moet ook helpen bij het ontwikkelen en actualiseren van strategieën van de EU en, op verzoek, van 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 het ontwikkelen 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) Ter bevordering van de samenwerking tussen de overheidssector en de particuliere sector enerzijds, en binnen de particuliere sector anderzijds, [...] moet het Agentschap **informatie-uitwisseling in en tussen sectoren, en met name die vermeld in bijlage II bij Richtlijn (EU) 2016/1148, ondersteunen door te voorzien in beste praktijken en richtsnoeren over beschikbare instrumenten en procedures, evenals richtsnoeren over de manier waarop problemen op regelgevingsgebied in verband met informatie-uitwisseling kunnen worden opgelost, onder meer door** [...] het instellen van sectorale centra voor informatie-uitwisseling en analyse (ISAC's) te stimuleren[...].

(18) Het Agentschap moet **vrijwillige uitgewisselde** nationale verslagen van de CSIRT's en CERT-EU verzamelen en analyseren **om de lidstaten te assisteren bij het invoeren van** [...] gemeenschappelijke [...] **procedures**, een taalregeling en terminologie voor de uitwisseling van informatie. Het Agentschap moet verder zorgen voor betrokkenheid van de particuliere sector, binnen het kader van de NIS-richtlijn die [...] de basis heeft gelegd voor de vrijwillige uitwisseling van technische informatie op operationeel niveau **binnen het CSIRT-netwerk**.

(19) Het Agentschap moet bijdragen tot een reactie op EU-niveau in het geval van grootschalige grensoverschrijdende cyberbeveiligingsincidenten en -crises. Deze functie moet **in overeenstemming met het mandaat van het Agentschap uit hoofde van deze verordening worden uitgevoerd en de lidstaten moeten een aanpak overeenkomen in het kader van de aanbeveling van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.** Tot **die aanpak** [...] behoren **mogelijk** 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 dat proces ondersteunen door de modaliteiten van een dergelijke samenwerking in het kader van **regelmatige** [...] cyberbeveiligingsoefeningen te testen.

(20) [...] Bij **het ondersteunen van de** operationele **samenwerking** [...] moet het Agentschap gebruikmaken van de **technische en operationele** expertise van CERT-EU door middel van een gestructureerde samenwerking [...]. [...] Wanneer passend moeten specifieke regelingen tussen de twee organisaties worden vastgesteld teneinde de praktische uitvoering van een dergelijke samenwerking te bepalen **en dubbel werk te voorkomen**.

(21) Overeenkomstig zijn [...] taken **ter ondersteuning van operationele samenwerking binnen het CSIRT-netwerk** moet het Agentschap in staat zijn ondersteuning te bieden aan de lidstaten **indien zij daarom verzoeken**, bijvoorbeeld door advies te geven omtrent het **vergroten van hun vermogen om incidenten te voorkomen, op te sporen en aan te pakken** [...], **door de** technische [...] **afhandeling van incidenten met aanzienlijke of substantiële gevolgen** te faciliteren of **door** te zorgen voor analyses van dreigingen en incidenten. **Als onderdeel van het faciliteren van de technische afhandeling van incidenten met aanzienlijke of substantiële gevolgen [...] moet Enisa met name steun verlenen aan de vrijwillige uitwisseling van technische oplossingen tussen lidstaten of gecombineerde technische informatie opstellen, waaronder door de lidstaten vrijwillig uitgewisselde technische oplossingen.** In de aanbeveling van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises wordt aanbevolen dat de lidstaten te goeder trouw samenwerken en zowel onderling als met Enisa onverwijld informatie uitwisselen betreffende grootschalige cyberincidenten en -crises. Die informatie moet Enisa verder helpen bij het [...] **ondersteunen van operationele samenwerking**.

(22) In het kader van de regelmatige samenwerking op technisch niveau ter ondersteuning van het situatiebewustzijn van de Unie, moet het Agentschap regelmatig **en in nauwe samenwerking met de lidstaten** het technisch situatieverslag inzake EU-cyberbeveiliging (EU Cybersecurity Technical Situation Report) 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 [...] of de bij de NIS-richtlijn opgerichte centrale contactpunten **(beide op vrijwillige basis)**, 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) **De door het Agentschap verleende steun aan** [...]technische ex-post**onderzoeken** van incidenten met aanzienlijke gevolgen [...] op verzoek van [...] de **betrokken** lidstaten[...] dient te zijn gericht op de preventie van toekomstige incidenten [...]. **De betrokken lidstaten moeten de nodige informatie verstrekken opdat het Agentschap die technische onderzoeken effectief kan steunen.**

24) [...]

25) De lidstaten kunnen de bij het incident betrokken ondernemingen verzoeken medewerking te verlenen door het Agentschap de nodige informatie en assistentie 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 andere entiteiten, relevante **voor iedereen beschikbare of vrijwillig uitgewisselde** 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 Unie-instellingen, -agentschappen en -organen door middel van dreigings- en incidentanalyse ondersteunen bij het constateren van nieuwe tendensen en het voorkomen van [...] cyberbeveiligings**incidenten**.

27) Om de weerbaarheid van de Unie te versterken, moet het Agentschap in staat zijn top-prestaties te leveren op het gebied van de **cyber**beveiliging **van infrastructuren door middel van steun aan met name de sectoren die worden genoemd in bijlage II van de NIS-richtlijn en de infrastructuren die worden gebruikt door de digitaledienst-aanbieders die worden genoemd in bijlage III van die richtlijn** [...] en wel 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 instand-houding 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 moet richtsnoeren verstrekken inzake goede praktijken voor afzonderlijke gebruikers, gericht tot 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 Unie-instellingen, [...] -agentschappen **en -organen** [...], tot 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 gegevens-beschermingsadvies 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 cyber-beveiligingsoplossingen 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), het **Agentschap van het Europese wereldwijde satellietnavigatiesysteem (GNSS-agentschap)** en alle andere EU-agentschappen die bij cyberbeveiliging zijn betrokken. Het moet overleggen met autoriteiten die zich bezighouden 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 moet, **in zijn rol** van [...] secretariaat van het CSIRT-netwerk [...], de CSIRT's van de lidstaten en CERT-EU ondersteunen wat betreft de operationele samenwerking in verband met alle relevante 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 voorts 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 [...] **regelmatig** cyberbeveiligingsoefeningen op Unieniveau 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 Unie-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 Unie-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 assisteren bij 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 dienstaanbieders stimuleren hun algemene veiligheids-normen 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 dienstaanbieders en fabrikanten van producten deze intrekken of recyclen. In samenwerking met de bevoegde autoriteiten kan 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 te verbeteren.

36) Het Agentschap moet volledig rekening houden met de lopende activiteiten op het gebied van onderzoek, ontwikkeling en technologiebeoordeling, en in het bijzonder de activiteiten van de verschillende onderzoeksinitiatieven van de Unie om de instellingen, [...] agentschappen **en organen** van de Unie en in voorkomend geval de lidstaten, op hun verzoek, te adviseren over onderzoeksbehoeften op het gebied van [...] cyberbeveiliging. **Om te bepalen welke onderzoeksbehoeften en -prioriteiten er zijn, moet het Agentschap ook de relevante gebruikersgroepen raadplegen.**

37) **Bedreigingen** van [...] cyberbeveiliging zijn wereldwijde problemen. Er is dan ook behoefte aan nauwere internationale samenwerking om de **cyber**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 verdergaande betrokkenheid van de Unie bij en samenwerking met derde landen en internationale organisaties ondersteunen door, voor zover van toepassing, de betrokken instellingen, [...] agentschappen **en organen** van de Unie van de noodzakelijke expertise en analyses te voorzien.

38) Het Agentschap moet kunnen reageren op ad-hocverzoeken om advies en assistentie 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, waar passend, 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) Met het oog op 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 respectieve vertegenwoordigers in de raad van bestuur te beperken met het oog op de continuïteit in de werkzaamheden.

42) Voor het goed functioneren van het Agentschap is het noodzakelijk dat de uitvoerend directeur wordt benoemd op grond van zowel verdiensten en aantoonbare administratieve en bestuurskundige vaardigheden, als 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 over onder andere **de uitvoering van het jaarlijkse werkprogramma van het Agentschap**, 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 voorts over de mogelijkheid beschikken om adhocwerkgroepen 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 adhocwerkgroepen 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 het doeltreffend functioneren 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 verkennen alsmede advies en oplossingen bieden ter voorbereiding van 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 toepasselijke bepalingen van de Unie inzake publieke toegang tot documenten toepassen, zoals vervat in Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad[12]. 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[13]. 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.

---

12 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).

13 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 meren–deel van het personeel van het Agentschap moet rechtstreeks worden ingezet voor de operationele tenuitvoerlegging van het mandaat van het Agentschap. De lidstaat van vestiging of om enige andere lidstaat mag een vrijwillige bijdrage leveren aan de inkomsten van het Agentschap. De Unie-begrotingsprocedure blijft van toepassing op eventuele subsidies die ten laste van de algemene begroting van de Unie komen. Voorts controleert de Rekenkamer de rekeningen van het Agentschap teneinde transparantie en verantwoording zeker te stellen.

47) [...]

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 automatisering 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 is het ontbreken van interoperabele oplossingen (technische normen), praktijken en EU-wijde certificerings-mechanismen een manco van de eengemaakte markt voor cyberbeveiliging. 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-**processen** 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 cyberbeveiligings-autoriteit 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 cyber-beveiliging, bijvoorbeeld op het gebied van het internet der dingen. Bestaande regelingen vertonen 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 geleverd 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 SOG-IS omvat slechts een deel van de Unie-lidstaten. 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 **en EU-verklaringen van overeenstemming** 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 **[...] Europese** 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-**processen**, -producten en -diensten vast te stellen. De uitvoering van en het toezicht op deze regelingen moeten worden verricht door de nationale autoriteiten voor **cyberbeveiligings**certificering [...] 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 toegepast, moeten buiten het toepassingsgebied van de verordening vallen. De organisaties die dergelijke regelingen toepassen, 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 (AVG) bepalingen betreffende het instellen van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens ter bevestiging van de naleving van die verordening bij verwerkingen door verwerkingsverantwoordelijken en verwerkers. Met behulp van dergelijke certificeringsmechanismen en gegevensbeschermingszegels en -merktekens dienen betrokkenen snel te kunnen 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**-processen**, -producten en -diensten die door middel van een dergelijke regeling zijn gecertificeerd, aan gespecificeerde vereisten voldoen [...] **met als doel** de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of verzonden gegevens of de daaraan gerelateerde diensten die via deze producten, processen, diensten en systemen worden aangeboden of toegankelijk zijn, **[...] te beschermen gedurende hun levenscyclus** in de zin van deze verordening. Het is niet mogelijk om in deze verordening de vereisten inzake cyberbeveiliging voor alle ICT-**processen**, -producten en -diensten in detail op te nemen. ICT-**processen**, -producten en -diensten en de daarmee verband houdende behoeften inzake cyberbeveiliging lopen zo sterk uiteen 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**-processen**, -producten en -diensten moet vervolgens verder worden gepreciseerd op het niveau van de specifieke, door de Commissie vastgestelde certificeringsregeling, bijvoorbeeld door middel van verwijzing naar normen of technische specificaties **wanneer er geen passende normen beschikbaar zijn.**

(55a) De technische specificaties voor gebruik in een Europese regeling voor cyber-beveiligingscertificering moeten worden opgesteld met inachtneming van de beginselen die zijn vastgelegd in bijlage II bij Verordening (EU) nr. 1025/2012. Sommige afwijkingen van deze beginselen kunnen evenwel in naar behoren gemotiveerde gevallen noodzakelijk worden geacht wanneer deze technische specificaties moeten worden gebruikt in een Europese regeling voor cyber-beveiligingscertificering waarin zekerheidsniveau "hoog" wordt vermeld. De redenen voor dergelijke afwijkingen moeten openbaar worden gemaakt.

(55b) De gecertificeerde conformiteitsbeoordeling is het proces waarbij wordt geëvalueerd of er is voldaan aan gespecificeerde vereisten inzake een ICT-proces, -product of -dienst. Deze evaluatie geschiedt door een onafhankelijke derde partij die niet de fabrikant van het product of de dienstverlener is. Na een succesvolle evaluatie van een ICT-proces, -product of -dienst wordt een certificaat afgegeven. Dat moet worden gezien als een bevestiging dat de betrokken evaluatie correct is uitgevoerd. Afhankelijk van het niveau van zekerheid moet in de Europese regeling voor cyberbeveiliging worden aangegeven of het certificaat wordt afgegeven door een particuliere of een openbare instantie. Een conformiteitsbeoordeling en een certificering bieden geen absolute garantie 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.

(55c) De keuze, door de gebruikers van certificaten, van het passende niveau van certificering en de bijbehorende beveiligingseisen moet worden gebaseerd op een risicoanalyse van het gebruik van het ICT-proces of -product of de ICT-dienst. Het niveau van zekerheid moet daarom in verhouding staan tot het niveau van het risico dat verbonden is aan het beoogde gebruik van een ICT-proces, -product of -dienst.

(55d) In een Europese regeling voor cyberbeveiligingscertificering zou kunnen worden bepaald dat een conformiteitsbeoordeling wordt uitgevoerd onder de uitsluitende verantwoordelijkheid van de fabrikant of leverancier van ICT-producten en -diensten (conformiteitszelfbeoordeling). In dergelijke gevallen volstaat het dat de fabrikant of de dienstverlener zelf alle inspecties uitvoert om te zorgen voor de conformiteit van het ICT-proces, de ICT-producten of -diensten met de certificeringsregeling. Dit soort conformiteitsbeoordeling moet geschikt worden geacht voor ICT-producten en -diensten met een geringe complexiteit (bv. eenvoudig ontwerp- en productiemechanisme) die een laag risico voor het openbaar belang opleveren. Voorts zouden alleen ICT-producten en -diensten met zekerheidsniveau "basis" in aanmerking kunnen komen voor een conformiteitszelfbeoordeling.

(55e) Een Europese regeling voor cyberbeveiligingscertificering zou de mogelijkheid kunnen bieden van zowel certificering als conformiteitszelfbeoordeling van ICT-producten en -diensten. In dit geval moet de regeling de consumenten of andere gebruikers duidelijke en begrijpelijke middelen aanreiken waarmee zij een onderscheid kunnen maken tussen producten en diensten die onder de verantwoordelijkheid van de fabrikant of dienstverlener zijn beoordeeld en producten en diensten die door een derde partij zijn gecertificeerd.

(55f) De fabrikant of leverancier van ICT-producten en -diensten die een conformiteitszelfbeoordeling uitvoert moet, als onderdeel van de conformiteitsbeoordelingsprocedure, de EU-verklaring van overeenstemming opstellen en ondertekenen. De EU-verklaring van overeenstemming is het document waarin staat dat een bepaald ICT-product of een bepaalde ICT-dienst voldoet aan de voorschriften van de regeling. Door de EU-verklaring van overeenstemming op te stellen en te ondertekenen verklaart de fabrikant of de dienstverlener zich verantwoordelijk voor de naleving, door het ICT-product of de ICT-dienst, van de wettelijke voorschriften van de regeling. Van de EU-verklaring van overeenstemming moet een exemplaar bij de nationale autoriteit voor cyberbeveiligingscertificering en bij Enisa worden ingediend.

(55g) De fabrikant of leverancier van ICT-producten en -diensten moet de EU-verklaring van overeenstemming en de technische documentatie van alle relevante informatie met betrekking tot de conformiteit van de ICT-producten of -diensten met een regeling ter beschikking van de bevoegde nationale autoriteit voor cyberbeveiligingscertificering houden, en wel gedurende een in de specifieke Europese regeling voor cyber-beveiligingscertificering bepaalde periode. In de technische documentatie moeten de toepasselijke vereisten worden vermeld en moeten, voor zover relevant voor de beoordeling, het ontwerp, de fabricage en de werking van het ICT-product of de ICT-dienst worden bestreken. De technische documentatie moet zodanig worden opgesteld dat kan worden beoordeeld of een ICT-product of -dienst voldoet aan de toepasselijke vereisten.

(55h) Lidstaten en geïnteresseerde organisaties van belanghebbenden moeten de mogelijkheid hebben bij de Europese Groep voor cyberbeveiligingscertificering een voorstel in dienen voor het opstellen van een mogelijke regeling. Geïnteresseerde organisaties van belanghebbenden zijn het bedrijfsleven of consumentenorganisaties, met inbegrip van vertegenwoordigers van kmo/mkb-organisaties die een geldig belang hebben bij de ontwikkeling van een specifieke Europese regeling voor cyberbeveiligingscertificering. Deze voorstellen moeten worden onderzocht in het licht van de criteria die zijn ontwikkeld door de Europese Groep voor cyberbeveiligingscertificering op grond van richtsnoeren die gebaseerd zijn op de beginselen transparantie, openheid, onpartijdigheid, consensus, effectiviteit, relevantie en coherentie.

(56) De Commissie **en de Groep** moeten de bevoegdheid krijgen om Enisa te vragen om **onverwijld** potentiële regelingen voor specifieke ICT-**processen**, -producten of -diensten op te stellen. De Commissie moet de bevoegdheid krijgen om vervolgens, op basis van de door Enisa voorgestelde potentiële regeling, de Europese regeling voor cyberbeveiligings-certificering bij uitvoeringshandeling 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 minimumreeks elementen worden vermeld die betrekking hebben op het onderwerp, het toepassingsgebied en het functioneren van de afzonderlijke regeling. Daartoe moeten onder meer het toepassingsgebied en het onderwerp van de cyberbeveiligingscertificering behoren, met inbegrip van de betrokken categorieën ICT-**processen**, -producten en -diensten, de gedetailleerde specificatie van de eisen inzake cyberbeveiliging, bijvoorbeeld onder verwijzing naar normen of technische specificaties, de specifieke evaluatiecriteria en -methoden alsmede het beoogde zekerheidsniveau (dat wil zeggen basis, substantieel en/of hoog) **en de evaluatieniveaus, indien van toepassing.**

(56a) De zekerheid van een Europese certificeringsregeling is de grond voor het vertrouwen dat een ICT-proces, -product of -dienst voldoet aan de beveiligingsvoorschriften van een specifieke Europese regeling voor cyberbeveiligingscertificering. Teneinde te zorgen voor samenhang van het kader betreffende gecertificeerde ICT-processen, -producten en -diensten zouden in een Europese certificeringsregeling zekerheids-niveaus kunnen worden aangegeven voor Europese cyberbeveiligingscertificaten en EU-verklaringen van overeenstemming die in het kader van die regeling worden afgegeven. In elk certificaat zou kunnen worden verwezen naar de zekerheidsniveaus "basis", "substantieel" of "hoog", terwijl in de EU-verklaring van overeenstemming alleen melding zou kunnen worden gemaakt van zekerheidsniveau "basis". De zeker-heidsniveaus bieden een overeenkomstige gradatie van inspanningen voor de evaluatie [...] en worden aangeduid met verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles, die tot doel hebben cyberbeveiligingsincidenten beperkt te houden of te voorkomen. Elk zeker-heidsniveau dient in overeenstemming te zijn met de diverse sectorale domeinen waar certificering wordt toegepast.

(56b) In een Europese regeling voor cyberbeveiligingscertificering kunnen verscheidene evaluatieniveaus worden vermeld, afhankelijk van de vraag hoe strikt en diepgaand de gebruikte evaluatiemethode is; deze methode moet overeenkomen met één van de zekerheidsniveaus en moet gepaard gaan met een passende combinatie van zekerheids-componenten. Voor alle zekerheidsniveaus moet het ICT-product of de ICT-dienst een aantal veilige functies bevatten, zoals omschreven door de regeling, zoals standaard-configuratie, ondertekende code, beveiligde update, bescherming tegen exploit, en volledige bescherming van het stack/heapgeheugen. Deze functies moeten worden ontwikkeld en onderhouden met op beveiliging gerichte benaderingen inzake ontwikkeling en de bijbehorende instrumenten waardoor wordt gewaarborgd dat er doeltreffende mechanismen (zowel software als hardware) op betrouwbare wijze in orden verwerkt. Voor het zekerheidsniveau "basis" moet de evaluatie worden gestuurd door ten minste de volgende zekerheidscomponenten: de evaluatie moet ten minste een beoordeling inhouden van de technische documentaties van het ICT-product of de ICT-dienst door de conformiteitsbeoordelingsinstantie. Indien de certificering ook ICT-processen omvat, moet de technische beoordeling ook betrekking hebben op het proces dat wordt gebruikt voor het ontwerpen, ontwikkelen en in stand houden van een ICT-product of -dienst. In gevallen waarin een Europese regeling voor cyberbeveiligingscertificering de mogelijk biedt van conformiteits-zelfbeoordeling, moet het voldoende zijn als de fabrikant of leverancier zelf heeft beoordeeld of het ICT-proces, de ICT-producten of -diensten voldoen aan de certificeringsregeling. Voor zekerheidsheidsniveau "substantieel" moet de evaluatie, in aanvulling op zekerheidsniveau "basis", worden gestuurd door ten minste de verificatie van de conformiteit van de beveiligingsfuncties van het ICT-product of de ICT-dienst aan de technische documentatie ervan. Voor zekerheidsheidsniveau "hoog" moet de evaluatie, in aanvulling op zekerheidsniveau "substantieel", worden gestuurd door ten minste een test van de efficiëntie waarbij wordt beoordeeld of de beveiligings-functies van een ICT-product of -dienst bestand zijn tegen mensen die vergaande cyberaanvallen uitvoeren en over aanzienlijke vaardigheden en middelen beschikken.

(56c) Bij het opstellen van een mogelijke regeling moet Enisa overleg plegen met alle relevante belanghebbenden, zoals de Europese normalisatieorganisaties, de bevoegde nationale autoriteiten, organisaties op basis van overeenkomsten voor wederzijdse erkenning zoals SOG-IS MRA, kmo's/mkb, consumentenorganisaties en belanghebbenden op sociaal en milieugebied.

(56d) Enisa moet een website aanhouden met voorlichting en publiciteit over Europese regelingen voor cyberbeveiligingscertificering, met aandacht voor, onder meer, de verzoeken voor de opstelling van een mogelijke Europese regeling voor cyberbeveiligingscertificering en voor de feedback die wordt ontvangen tijdens het raadplegingsproces dat Enisa in de voorbereidingsfase uitvoert. De website moet ook informatie geven over certificaten en EU-verklaringen van overeenstemming die uit hoofde van deze verordening worden afgegeven.

(57) De toepassing van Europese regelingen voor cyberbeveiligingscertificering **en de EU-verklaring van overeenstemming** moet vrijwillig blijven, tenzij anders is bepaald in Unie-wetgeving of in nationale wetgeving **die in overeenstemming met Unie-wetgeving is aangenomen. Bij ontstentenis van geharmoniseerde wetgeving mogen de lidstaten in overeenstemming met Richtlijn (EU) 2015/1535 nationale technische voorschriften vaststellen tot instelling van een verplichte certificering uit hoofde van een Europese regeling voor cyberbeveiligingcertificering. De lidstaten zouden tevens gebruik kunnen maken van de Europese cyberbeveiligingscertificering in het kader van overheidsopdrachten en Richtlijn 2014/214/EU.[...]**

(57a) Om de doelstellingen van deze verordening te verwezenlijken en de versnippering van de interne markt te voorkomen, mogen 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. Voorts moeten de lidstaten geen nieuwe nationale regelingen invoeren voor cyberbeveiligings-certificering van ICT-producten en -diensten die reeds onder een bestaande Europese regeling voor cyberbeveiligingscertificering vallen. Niets mag echter de lidstaten beletten nationale certificeringsregelingen vast te stellen of te handhaven met het oog op de nationale veiligheid.

(58) Zodra een Europese regeling voor cyberbeveiligingscertificering is vastgesteld, moeten fabrikanten van ICT-producten of verleners van ICT-diensten bij een conformiteits-beoordelingsinstantie 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 maximum-periode 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 **beperken, opschorten of** 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) [...] De lidstaten **moeten** [...] één autoriteit **of meerdere** autoriteiten aanwijzen voor cyberbeveiligingscertificering[...] die erop toeziet/toezien dat wordt voldaan **aan de uit deze verordening voortvloeiende verplichtingen. Indien een lidstaat zulks passend acht, kunnen de taken ook worden toegewezen aan reeds bestaande instanties. De lidstaten moeten eveneens kunnen besluiten om, in onderlinge overeenstemming met een andere lidstaat, een toezichthoudende autoriteit of toezichthoudende autoriteiten aan te wijzen op het grondgebied van die andere lidstaat. De autoriteit moet in het bijzonder toezicht houden op en de handhaving verzekeren van de verplichtingen van de fabrikant of leverancier van ICT-producten en -diensten, gevestigd op hun respectieve grondgebieden, ten aanzien van de EU-verklaring van overeenstemming; zij moet de nationale accreditatie-instanties bijstaan bij het volgen van en toezien op activiteiten van conformiteitsbeoordelingsinstanties door hen te voorzien van deskundigheid en relevante informatie; en zij moet conformiteitsbeoordelingsinstanties toestaan hun taken uit te voeren wanneer zij voldoen aan de aanvullende vereisten in een regeling, en relevante ontwikkelingen volgen op het gebied van cyberbeveiligingscertificering [...].** De nationale autoriteiten voor **cyberbeveiliging**scertificering [...] moeten klachten behandelen die natuurlijke of rechtspersonen hebben ingediend over **door hen** afgegeven certificaten **of over certificaten die zijn afgegeven door conformiteitsbeoordelingsinstanties met zekerheidsniveau "hoog"**[...], moeten de inhoud van de klacht in passende mate onderzoeken 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 **cyberbeveiliging**scertificering[...] 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 **vertegenwoordigers van** de nationale autoriteiten voor **cyberbeveiligings**certificering[...] **of andere relevante nationale autoriteiten.** De voornaamste taken van de Groep moeten bestaan uit het adviseren en assisteren van de Commissie bij haar werkzaamheden ter waarborging van een samenhangende uitvoering en toepassing van het Europees kader voor cyberbeveiligingscertificering; het assisteren van, en nauw samenwerken met, het Agentschap bij het opstellen van potentiële regelingen voor cyberbeveiligingscertificering; aanbevelen dat de Commissie het Agentschap verzoekt om een potentiële Europese regeling voor cyberbeveiligingscertificering op te stellen; en aan **het Agentschap** adviezen uitbrengen **over mogelijke regelingen en aan** de Commissie adviezen uitbrengen met betrekking tot het onderhoud en de herziening van bestaande Europese regelingen voor cyberbeveiligingscertificering.

(60a) De Groep moet de uitwisseling mogelijk maken van goede praktijken en expertise tussen de nationale autoriteiten voor cyberbeveiligingscertificering die verantwoordelijk zijn oor de toelating van conformiteitsbeoordelingsinstanties en voor de afgifte van certificaten. De Groep moet bijdragen tot de ontwikkeling van een mechanisme voor collegiale toetsing in het kader van de opstelling van een mogelijke regeling en de uitvoering ervan voor instanties die Europese cyberbeveiligingscertificaten afgeven met zekerheidsniveau "hoog". Bij dergelijke collegiale toetsingen moet in het bijzonder worden nagegaan of de betrokken instanties beschikken over de juiste deskundigheid en of zij hun taken op geharmoniseerde wijze uitvoeren. De resultaten van de collegiale toetsingen moeten openbaar worden gemaakt. Deze instanties kunnen passende maatregelen nemen om hun praktijken en expertise aan te passen.

(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.

(61a) Ter verdere bevordering van de handel en in het besef dat ICT-voorzieningsketens mondiaal zijn, kan de Unie in overeenstemming met artikel 218 VWEU overeenkomsten sluiten inzake wederzijdse erkenning met betrekking tot certificaten die zijn afgegeven via regelingen die zijn ingesteld krachtens het Europees kader voor cyberbeveiligingscertificering. De Commissie, rekening houdend met het advies van Enisa en de Europese Groep voor cyberbeveiligingscertificering, kan aanbevelen hierover onderhandelingen te openen. Iedere regeling moet specifieke voorwaarden bevatten voor wederzijdse erkenning met derde landen.

(62) [...]

(63) [...]

(64) Aan de Commissie dienen de in deze verordening bepaalde uitvoeringsbevoegdheden te worden verleend opdat zij kan zorgen voor uniforme omstandigheden voor de tenuitvoerlegging van deze verordening. 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 inzake de omstandigheden, formaten en procedures voor kennisgeving betreffende geaccrediteerde conformiteitsbeoordelingsinstanties door de nationale autoriteiten voor **cyberbeveiligings**certificering[...] aan de Commissie.

(66) Het optreden van het Agentschap moet aan een onafhankelijke evaluatie worden onderworpen. Die moet de verwezenlijking van de doelstellingen van het Agentschap, de werkmethoden ervan en de relevantie van zijn taken betreffen. Bij de evaluatie moeten tevens het effect, 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

1. 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 Enisa, het "agentschap van de Europese Unie voor cyberbeveiliging", hierna "het Agentschap" genoemd; alsmede

b) een kader voor de vaststelling van Europese regelingen voor cyberbeveiligingscertificering met als doel het waarborgen van een toereikend cyberbeveiligingsniveau van ICT-processen, -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.

2. **Deze verordening laat 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 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 omschreven in artikel 4, punt 4), van Richtlijn (EU) 2016/1148;

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

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

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

8) "cyberdreiging": elke potentiële omstandigheid of gebeurtenis die netwerk- en informatie-systemen, de gebruikers daarvan en betrokken personen kan **schaden, kan verstoren of op andere wijze** negatief kan beïnvloeden;

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

9a) "nationale regeling voor cyberbeveiligingscertificering": een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die door een nationale overheidsinstantie zijn ontwikkeld en aangenomen en die van toepassing zijn op de certificering of conformiteitsbeoordeling van ICT-processen, -producten en -diensten die binnen het toepassingsgebied van die specifieke regeling vallen;

10) "Europees cyberbeveiligingscertificaat": een [...] document dat bevestigt dat **is beoordeeld of** een bepaald ICT-**proces of** product of een bepaalde ICT-dienst voldoet aan de specifieke, in een Europese regeling voor cyberbeveiligingscertificering vastgestelde **beveiligings**vereisten;

11) "ICT-product [...]": elk element of elke groep elementen van netwerk- en informatiesystemen;

11a) "ICT-dienst": elke dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen;

11b) "ICT-proces": een reeks activiteiten die wordt uitgevoerd om een ICT-productof - dienst te ontwerpen, te ontwikkelen, te leveren en te onderhouden;

12) "accreditatie": accreditatie als omschreven 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 omschreven in artikel 2, punt 13, van Verordening (EG) nr. 765/2008;

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

16a) "technische specificatie": een document waarin de technische vereisten zijn voorgeschreven waaraan een ICT-proces, -product of -dienst moet voldoen;

16b) "zekerheidsniveau: een basis voor de zekerheid dat een ICT-proces, -product of -dienst aan de beveiligingsvereisten van een specifieke Europese regeling voor cyberbeveiligingscertificering voldoet, die aangeeft op welk niveau het betrokken ICT-proces of -product of de betrokken ICT-dienst is geëvalueerd; het zekerheids-niveau is geen maatstaf voor de beveiliging van een ICT-proces, -product of -dienst zelf.

TITEL II

Enisa – het *[...] "agentschap van de Europese Unie voor cyberbeveiliging*"

HOOFDSTUK I

MANDAAT EN DOELSTELLINGEN *[...]*

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 [...] **in de hele** Unie, **met name door steun te verlenen aan de instellingen, instanties en organen van de Unie met het oog op betere cyberbeveiliging. Het Agentschap fungeert voor de instellingen, instanties en organen van de Unie als referentiepunt voor advies en deskundigheid op het gebied van cyberbeveiliging.**

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.

2a. Bij het uitoefenen van zijn taken treedt het Agentschap onafhankelijk op, houdt het zo veel mogelijk rekening met de nationale deskundigheid van de bevoegde autoriteiten van de lidstaten, en voorkomt het tegelijk dat er dubbel werk wordt geleverd.

3. [...]

Artikel 4

Doelstellingen

1. Het Agentschap is een expertisecentrum voor cyberbeveiliging door zijn onafhankelijkheid, de wetenschappelijke en technische kwaliteit van zijn advies en assistentie, de informatie die het verstrekt, de transparantie van zijn werkwijzen en -methoden, en de toewijding bij de uitvoering van zijn taken.

2. Het Agentschap assisteert de instellingen, instanties en organen van de Unie alsmede de lidstaten bij het ontwikkelen en uitvoeren van Uniebeleid inzake cyberbeveiliging, **waaronder sectoraal beleid op het gebied van cyberbeveiliging**.

3. Het Agentschap ondersteunt de capaciteitsopbouw en de paraatheid in de hele Unie door de **instellingen, instanties en organen** van de Unie, **alsmede** de lidstaten en publieke en particuliere belanghebbenden te assisteren teneinde de bescherming van hun netwerk- en informatiesystemen te verbeteren, **cyberveerkracht en cyberreactievermogen** te ontwikkelen **en te verbeteren**, en vaardigheden en bekwaamheden op het gebied van cyberbeveiliging **te ontwikkelen** [...].

4. Het Agentschap bevordert de samenwerking en coördinatie op EU-niveau tussen de lidstaten, de EU-instellingen, -instanties en -organen, en relevante **particuliere en publieke** belanghebbenden [...] inzake aangelegenheden op het gebied van cyberbeveiliging.

5. Het Agentschap **draagt bij tot het versterken** [...] van de vermogens inzake cyberbeveiliging op EU-niveau teneinde [...] de lidstaten **te assisteren bij het voorkomen van en reageren op cyberdreigingen**, met name in het geval van grensoverschrijdende incidenten.

6. Het Agentschap bevordert het gebruik van certificering **om versnippering van certificeringsregelingen in de EU te voorkomen**. **Het Agentschap draagt met name bij tot** [...] het tot stand brengen en handhaven van een kader voor cyberbeveiligings-certificering op EU-niveau overeenkomstig titel III van deze verordening, met het oog op een transparantere cyberbeveiligingszekerheid van ICT-producten en -diensten en zodoende een groter vertrouwen in de digitale interne markt.

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

HOOFDSTUK IA

TAKEN

Artikel 5

[...] ***Ontwikkeling en uitvoering van EU-beleid en -wetgeving***

Het Agentschap draagt bij tot het ontwikkelen en uitvoeren van EU-beleid en -wetgeving door:

1. te assisteren en te adviseren, 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 te assisteren 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 assistentie te verstrekken;

4. ondersteuning te bieden bij:

    1) het ontwikkelen en uitvoeren 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) het bevorderen 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 contactpunten van iedere lidstaat worden gerapporteerd aan 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 aanbieders van vertrouwensdiensten, door de toezichthoudende organen aan het Agentschap gerapporteerd overeenkomstig artikel 19, lid 3, van Verordening (EU) nr. 910/2014;

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

Artikel 6

[...] ***Capaciteitsopbouw***

1. Het Agentschap assisteert:

a) de lidstaten bij hun inspanningen ter verbetering van de preventie, opsporing en analyse van [...] **cyberdreigingen** en -incidenten [...], alsmede het vermogen hierop te reageren, door hen te voorzien van de noodzakelijke kennis en expertise;

b) de EU-instellingen, -instanties **en -organen** bij hun inspanningen ter verbetering van de preventie, opsporing en analyse [...] **cyberdreigingen** en -incidenten [...], alsmede het vermogen hierop te reageren, **met name** door passende ondersteuning voor het CERT voor de EU-instellingen, -instanties 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 en [...] **volgt de** uitvoering van die strategieën in de hele Unie teneinde beste praktijken te bevorderen;

e) de EU-instellingen bij de ontwikkeling en evaluatie van EU-strategieën inzake cyber-beveiliging, 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 **regelmatig** [...] 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 **bij** het [...] uitwisselen [...] van beste praktijken, met name voor het in kaart brengen 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 **bevordert de informatie-uitwisseling binnen en tussen sectoren** [...] 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

[...] ***Operationele samenwerking op EU-niveau***

1. Het Agentschap ondersteunt de operationele samenwerking tussen de **lidstaten, de instellingen, instanties en** [...] organen van de Unie en tussen belanghebbenden.

2. Het Agentschap werkt op operationeel niveau samen en brengt synergieën tot stand met de EU-instellingen, -instanties [...] **en -organen**,, 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:

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 **in deze hoedanigheid** [...] de uitwisseling van informatie en de samenwerking tussen zijn leden.

4. Het Agentschap **bevordert** [...] de operationele samenwerking binnen het CSIRT-netwerk en verleent de lidstaten **op hun verzoek** steun door:

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

b) [...] de technische **afhandeling** [...] van incidenten met aanzienlijke of substantiële gevolgen **te faciliteren**, **onder meer met name door steun te verlenen aan het vrijwillig delen van technische oplossingen tussen lidstaten**;

c) kwetsbaarheden [...] en incidenten te analyseren**;**

ca) steun te verlenen aan technische onderzoeken achteraf van incidenten met aanzienlijke of substantiële gevolgen, zulks uit hoofde van Richtlijn (EU) 2016/1148.

Bij het uitvoeren van deze taken werken het Agentschap en CERT-EU op gestructureerde wijze samen om te kunnen profiteren van synergieën **en dubbel werk te voorkomen** [...].

5. [...]

[...]

6. Het Agentschap organiseert **regelmatig** [...] cyberbeveiligingsoefeningen op EU-niveau en ondersteunt de EU-instellingen, -instanties en -organen op hun verzoek bij het organiseren van oefeningen. **Die oefeningen op EU-niveau kunnen technische, operationele of strategische onderdelen bevatten [...]. Om de twee jaar wordt een grootschalige oefening georganiseerd waarin al deze onderdelen zijn opgenomen.** Het Agentschap draagt in voorkomend geval ook bij tot sectorale cyberbeveiligingsoefeningen, en helpt deze te organiseren, samen met relevante [...] **organisaties die ook kunnen** deelnemen aan cyberbeveiligingsoefeningen op EU-niveau.

7. Het Agentschap stelt **in nauwe samenwerking met de lidstaten** 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 [...] of de bij de NIS-richtlijn opgezette centrale contactpunten (**beide op vrijwillige basis** [...]); het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol en CERT-EU.

8. Het Agentschap draagt bij tot het ontwikkelen 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) **op vrijwillige basis gedeelde** verslagen van nationale bronnen te bundelen om tot het tot stand brengen van een gemeenschappelijk situatiebewustzijn bij te dragen;

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

c) [...] **op verzoek van de lidstaten** de technische afhandeling van een incident of crisis **te faciliteren**, onder meer **met name** [...] door **steun te verlenen aan het vrijwillig delen van technische oplossingen tussen lidstaten**;

d) **steun te verlenen aan de EU-instellingen, -instanties en -organen en, op verzoek, de lidstaten bij de communicatie met het publiek over het incident of de crisis;**

e) **op verzoek steun te verlenen aan de lidstaten** om de plannen voor samenwerking bij het reageren op dergelijke incidenten of crises te toetsen.

Artikel 8

[...] ***Markt, cyberbeveiligingscertificering en normalisatie***

Het Agentschap:

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

1) potentiële Europese regelingen voor cyberbeveiligingscertificering voor ICT-**processen**, -producten en -diensten **in samenwerking met de sector en** overeenkomstig artikel 44 van deze verordening op te stellen;

2) de Commissie te assisteren 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 **cyberbeveiligingscertificering** [...] en de sector;

3a) passende technische specificaties aan te bevelen voor het gebruik van de ontwikkeling van Europese regelingen voor cyberbeveiligingscertificering als bedoeld in artikel 47, lid 1, onder b), in gevallen waarin geen normen beschikbaar zijn;

3b) bij te dragen tot de opbouw van voldoende capaciteit voor evaluatie- en certificeringsprocessen door richtsnoeren te verzamelen en te publiceren en door op verzoek steun te verlenen aan de lidstaten;

b) faciliteert het opstellen en toepassen van Europese en internationale normen voor risicobeheersing en voor de beveiliging van ICT-**processen**-, -producten en diensten [...];

ba) 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

[...] ***Kennis* en *informatie*** [...]

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 in kaart te brengen en [...] **cyberbeveiligingsincidenten** te helpen 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 [...] infrastructuurvoorzieningen die de in bijlage II bij Richtlijn (EU) 2016/1148 genoemde sectoren ondersteunen **en die welke worden gebruikt door de in bijlage III van die richtlijn genoemde digitaledienstaanbieders**;

d) bundelt en organiseert door middel van een hiervoor bestemd portaal informatie over cyberbeveiliging die door de EU-instellingen, -instanties en -organen en **op vrijwillige basis door de lidstaten en publieke en particuliere belanghebbenden wordt verstrekt**, en maakt deze openbaar;

e) [...]

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) [...].

Artikel 9a

Bewustmaking en voorlichting

Het Agentschap:

a) draagt bij tot de bewustmaking van het publiek omtrent risico's inzake cyber-beveiliging en verstrekt richtsnoeren inzake goede praktijken voor afzonderlijke gebruikers, te weten burgers en organisaties;

b) organiseert, in samenwerking met de lidstaten en de EU-instellingen, -organen, -instanties en de sector, regelmatig publieke voorlichtingscampagnes teneinde de cyberbeveiliging in de Unie te versterken en zichtbaarder te maken;

c) assisteert de lidstaten bij hun inspanningen met het oog op de bewustmaking omtrent cyberbeveiliging en verleent steun aan voorlichting inzake cyberbeveiliging;

d) ondersteunt nauwere coördinatie en de uitwisseling van beste praktijken tussen de lidstaten met betrekking tot de voorlichting en bewustmaking inzake cyberbeveiliging door het tot stand brengen en onderhouden van een netwerk van nationale voorlichtingscontactpunten te faciliteren.

Artikel 10

[...] ***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 doeltreffend 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 doeltreffend 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

[...] ***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) de uitwisseling van beste praktijken te faciliteren **binnen de toepasselijke internationale samenwerkingsverbanden** [...].

c) de Commissie, op verzoek, van expertise te voorzien**;**

ca) in samenwerking met de op grond van artikel 53 ingestelde Europese Groep voor cyberbeveiligingscertificering advies en steun aan de Commissie te verlenen inzake aangelegenheden in verband met overeenkomsten met derde landen betreffende wederzijdse erkenning van cyberbeveiligingscertificaten.

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 beschreven taken uitvoert;

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

c) een uitvoerend directeur, die de in artikel 19 genoemde verantwoordelijkheden uitoefent; [...]

d) een permanente groep van belanghebbenden, die de in artikel 20 beschreven taken uitvoert**;**

da) een netwerk van nationale verbindingsfunctionarissen dat de in artikel 20a beschreven 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 en in het licht 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

Taken 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;

ca) oefent toezicht uit op de uitvoering van de meerjarige en jaarlijkse programmering die in het enig programmeringsdocument is opgenomen;

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 en op basis van artikel 2, lid 1, van het Statuut alsmede op basis van artikel 6 van de Regeling die van toepassing is op de andere personeelsleden, een beslissing waarbij 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 assisteren door adviseurs of deskundigen.

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

Artikel 17

Stemregels in de raad van beheer

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 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 de uitvoerend directeur bij de uitvoering van de besluiten van de raad van bestuur aangaande administratieve en budgettaire aangelegenheden, zulks onverminderd de in artikel 19 genoemde verantwoordelijkheden van de uitvoerend directeur;

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. [...]

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 opstellen van het geconsolideerde jaarverslag over de activiteiten van het Agentschap, **waaronder de uitvoering van het jaarlijkse werkprogramma**, en dat ter beoordeling en goedkeuring 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 in voorkomend geval effectieve, evenredige en afschrikkende administratieve en geldelijke sancties op te leggen;

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

l) het leggen en onderhouden van contacten met het bedrijfsleven en consumenten-organisaties om een regelmatige dialoog met de belanghebbenden te waarborgen;

(la) het regelmatige overleg met de instellingen, instanties en organen van de Unie over hun cyberbeveiligingsactiviteiten om te zorgen voor samenhang in de ontwikkeling en uitvoering van het EU-beleid;

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 instellen, samengesteld uit deskundigen, onder meer afkomstig 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 kan, indien nodig voor het efficiënt en doeltreffend uitvoeren van de taken van het Agentschap en op basis van een passende kosten-batenanalyse** besluiten [...] in een of meer lidstaten **een of meer lokale kantoren op te zetten.** Voordat de uitvoerend directeur besluit een lokaal kantoor op te zetten, **vraagt hij het advies van de betrokken lidstaten (lidstaten), onder meer de lidstaat waar de zetel van het Agentschap zich bevindt, en** verkrijgt hij daarvoor voorafgaande toestemming van de Commissie **en** de raad van bestuur [...]. **Indien tijdens het overleg tussen de uitvoerend directeur en de betrokken lidstaten geen overeenstemming kan worden bereikt, wordt de kwestie ter bespreking aan de Raad voorgelegd.** Het besluit vermeldt het toepassingsgebied van de activiteiten die in het lokale kantoor moeten worden uitgevoerd, opdat onnodige kosten en verdubbeling van administratieve functies van het Agentschap worden vermeden. [...]**Het aantal personeelsleden in alle lokale kantoren wordt tot een minimum beperkt en maakt <u>in totaal</u> maximaal 40 % uit van het [...] personeel <u>in de lidstaat waar de zetel van het Agentschap zich bevindt</u>. Het aantal personeelsleden in elk lokaal kantoor maakt maximaal 10 % uit van het [...] aantal personeelsleden <u>in de lidstaat waar de zetel van het Agentschap zich bevindt.</u>**

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-sector, aanbieders van openbare elektronische communicatienetwerken of -diensten, **aanbieders van essentiële 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, alsmede 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 voor 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 bij het opstellen 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.

5a. De permanente groep van belanghebbenden informeert de raad van bestuur op gezette tijden over haar activiteiten.

AFDELING 4A

NETWERK VAN NATIONALE VERBINDINGSFUNCTIONARISSEN

Artikel 20a

Netwerk van nationale verbindingsfunctionarissen

1. De raad van bestuur zet op voorstel van de uitvoerend directeur een netwerk van nationale verbindingsfunctionarissen op dat is samengesteld uit vertegenwoordigers van de lidstaten.

2. Het netwerk van nationale verbindingsfunctionarissen bestaat uit vertegenwoordigers van alle lidstaten. Elke lidstaat wijst één vertegenwoordiger aan. De vergaderingen van het netwerk kunnen in verschillende samenstellingen van deskundigen worden gehouden.

3. Het netwerk van nationale verbindingsfunctionarissen faciliteert met name de uitwisseling van informatie tussen het Agentschap en de lidstaten. Het verleent met name steun aan het Agentschap bij het verspreiden van zijn activiteiten, bevindingen en aanbevelingen in de hele EU aan de relevante belanghebbenden.

4. De nationale verbindingsfunctionarissen fungeren als contactpunt op nationaal niveau om de samenwerking tussen het Agentschap en nationale deskundigen in het kader van de uitvoering van het werkprogramma van het Agentschap te faciliteren.

5. Hoewel de nationale verbindingsfunctionarissen nauw moeten samenwerken met de vertegenwoordigers van hun respectieve landen in de raad van bestuur, dupliceert het netwerk zelf noch de werkzaamheden van de raad van bestuur, noch die van andere EU-fora.

6. De taken en procedures voor het netwerk van nationale verbindingsfunctionarissen worden in het huishoudelijk reglement van het Agentschap vastgesteld en gepubliceerd.

HOOFDSTUK 5
WERKING

Artikel 21

Enig programmeringsdocument

1. Het Agentschap voert zijn werkzaamheden uit overeenkomstig een enig programmerings-document, 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[14] 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.

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 activiteits-gestuurde 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.

---

[14] 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).

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 geactualiseerd. 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 vervatte 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-hoc-werkgroepen en de personeelsleden van het Agentschap, met inbegrip van de door de lidstaten tijdelijk gedetacheerde ambtenaren, houden zich ook na het beëindigen van hun functie aan de geheimhoudingsplicht uit hoofde van artikel 339 van het Verdrag betreffende de werking van de Europese Unie (VWEU).

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[15] en Besluit (EU, Euratom) 2015/444[16] worden toegepast. Dit reglement omvat onder meer bepalingen betreffende de uitwisseling, de verwerking en de opslag van gerubriceerde gegevens.

---

[15] 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).

[16] 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.

TITEL III

VASTSTELLING EN STRUCTUUR VAN DE BEGROTING

Artikel 26

Vaststelling 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-hoc-subsidies 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 regels

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[17] 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 passende, 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.

[17] 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).

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[18] 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 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. Samenwerkingsovereenkomsten met derde landen en internationale organisaties, contracten, subsidieovereenkomsten en subsidiebesluiten van het Agentschap bevatten, onverminderd de leden 1, 2 en 3, 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.

---

[18] 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).

Artikel 32

Voorrechten en immuniteit

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 bedraagt **vier** [...] 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 **vier** [...] 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 enkel uit zijn ambt worden ontheven door een besluit van de raad van bestuur [...].

Artikel 34

Gedetacheerde nationale deskundigen en andere personeelsleden

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 [...].

3. Het Agentschap wordt vertegenwoordigd door zijn uitvoerend directeur.

Artikel 36

Aansprakelijkheid van het Bureau

1. De contractuele aansprakelijkheid van het Agentschap valt onder het recht dat van toepassing is op de betrokken 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[19]. 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[20] 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.

---

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

[20] 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).

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 werkzaamheden van het Agentschap, met inbegrip van bepalingen betreffende de deelname aan de initiatieven van het Agentschap en betreffende 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 voor de bescherming van gerubriceerde informatie en gevoelige niet-gerubriceerde informatie

Het Agentschap stelt in overleg met de Commissie zijn beveiligingsvoorschriften vast en past daarbij de beveiligingsbeginselen toe die zijn vervat 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

Zetelovereenkomst 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 schept [...] de voorwaarden voor het goed functioneren van het Agentschap, 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

Administratief toezicht

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

TITEL III
KADER VOOR CYBERBEVEILIGINGSCERTIFICERING

Artikel 43

Kader *voor Europese cijferbeveiligingscertificering [...]*

1. **Er wordt een kader voor Europese cyberbeveiligingscertificering ingesteld teneinde door een hoger niveau van cyberbeveiliging in de Unie, de voorwaarden voor het functioneren van de interne markt te verbeteren. Het behelst een bestuursmodel waarmee op EU-niveau een geharmoniseerde aanpak van de regelingen voor Europese cyberbeveiligingscertificering kan worden gevolgd, met het oog op de totstandbrenging van een digitale eengemaakte markt voor ICT-processen, -producten en -diensten.**

2. **Binnen het kader voor Europese cyberbeveiligingscertificering wordt een mechanisme omschreven voor de totstandbrenging van [...]** Europese regelingen voor cyberbeveiligingscertificering [...] **alsmede om** te waarborgen dat ICT**-processen**, -producten en -diensten die door middel van een dergelijke regeling zijn **geëvalueerd**, aan gespecificeerde **beveiligings**vereisten voldoen [...] **met als doel** de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of verzonden gegevens of de daaraan gerelateerde diensten die via deze producten, processen en **diensten** [...] worden aangeboden of toegankelijk zijn, **[...] te beschermen gedurende hun gehele levenscyclus**.

Artikel 44

Opstelling en vaststelling van een Europese regeling voor cyberbeveiligingscertificering

1. Naar aanleiding van een verzoek van de Commissie **of van de krachtens artikel 53 opgerichte Europese Groep voor cyberbeveiligingscertificering ("de Groep")**, stelt Enisa een potentiële Europese regeling voor cyberbeveiligingscertificering op die voldoet aan de voorschriften van de artikelen 45, 46 en 47 van deze verordening.

1a. De lidstaten of organisaties van belanghebbenden kunnen aan de Groep voorstellen dat zij een potentiële Europese regeling voor cyberbeveiligingscertificering opstellen. De Groep evalueert deze voorstellen aan de hand van criteria die de Groep omschrijft door middel van richtsnoeren als bedoeld in artikel 53, lid 3, punt ca), en kan Enisa verzoeken een potentiële Europese regeling voor cyberbeveiligingscertificering op te stellen.

2. Bij het opstellen van potentiële regelingen als bedoeld in lid 1 van dit artikel, raadpleegt Enisa **door middel van transparante raadplegingsprocedures** alle betrokken partijen en werkt het nauw samen met de Groep. De Groep verstrekt Enisa assistentie en deskundig advies [...] met betrekking tot het opstellen van de potentiële regeling, **en brengt over de potentiële regeling advies uit voordat zij aan de Commissie wordt voorgelegd [...]. Enisa zorgt ervoor dat de potentiële regelingen in overeenstemming zijn met de toepasselijke geharmoniseerde norm voor de accreditatie van de conformiteits-beoordelingsinstantie.**

3. Enisa **houdt zoveel mogelijk rekening met het advies van de Groep voordat** [...] de in overeenstemming met lid 2 van dit artikel opgestelde potentiële regeling aan de Commissie [...] **wordt toegezonden**.

4. Op basis van de door Enisa voorgestelde potentiële regeling kan de Commissie uitvoeringshandelingen vaststellen overeenkomstig artikel 55, lid 2, om te voorzien in Europese regelingen voor cyberbeveiligingscertificering van ICT-**processen**, -producten en -diensten die voldoen aan de vereisten van de artikelen 45, 46 en 47 van deze verordening.

5. [...]

Artikel 44a

Beheer van een Europese regeling voor cyberbeveiligingscertificering

1. Het Agentschap beheert een specifieke website met informatie en publiciteit over Europese regelingen voor cyberbeveiligingscertificering, certificaten en uit hoofde van artikel 47a afgegeven EU-verklaringen van overeenstemming.

2. Het Agentschap evalueert in nauwe samenwerking met de Groep ten minste elke vijf jaar de vastgestelde Europese regelingen voor cyberbeveiligingscertificering en houdt hierbij rekening met de feedback die het ontvangt van belanghebbenden. Indien nodig kan de Commissie of de Groep het Agentschap verzoeken de procedure te beginnen voor het ontwikkelen van een herziene potentiele regeling overeenkomstig artikel 44, leden 2 en 3.

Artikel 45

Beveiligingsdoelstellingen van Europese regelingen voor cyberbeveiligingscertificering

De opzet van een Europese regeling voor cyberbeveiligingscertificering is **van dien aard** dat, voor zover van toepassing, **minstens** de volgende beveiligingsdoelstellingen [...] worden verwezenlijkt.

a) opgeslagen, doorgegeven of anderszins verwerkte gegevens **gedurende het gehele proces en de gehele levensduur van het product of dienst** worden beschermd tegen accidentele of onbevoegde opslag, verwerking, toegang of openbaarmaking;

b)

opgeslagen, doorgegeven of anderszins verwerkte gegevens **gedurende het gehele proces en de gehele levensduur van het product of dienst** worden beschermd tegen accidentele of onbevoegde vernietiging, [...] verlies of wijziging, **of gebrekkige beschikbaarheid**;

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

d) registreerd wordt op welk tijdstip en door wie tot gegevens, functies of diensten [...] **toegang is verkregen, daarvan gebruik is gemaakt of die anderszins verwerkt zijn**;

e) het is mogelijk na te gaan op welk tijdstip en door wie gegevens, functies of diensten [...] zijn ingezien, [...] gebruikt of **anderszins verwerkt**;

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

g) ICT-**processen**, -producten en -diensten worden geleverd met geüpdatete software en **hard-ware** die geen [...] **algemeen** bekende kwetsbaarheden bevatten, en met mechanismen voor veilige [...] updates.

ga) ICT-processen, -producten en -diensten worden ontwikkeld, vervaardigd en geleverd overeenkomstig de beveiligingsvoorschriften van de betrokken regeling.

Artikel 46

Zekerheidsniveaus van Europese regelingen voor cyberbeveiligingscertificering

1. In een Europese regeling voor cyberbeveiligingscertificering kunnen voor ICT-**processen**, -producten en -diensten een of meer van de volgende zekerheidsniveaus worden gespecificeerd: basis, substantieel en/of hoog [...]. **Het zekerheidsniveau staat in verhouding tot het niveau van het risico dat verbonden is aan het beoogde gebruik van een ICT-proces, -product of -dienst.**

2. Aan de zekerheidsniveaus basis, substantieel en/of hoog **is een certificaat of een in het kader van een Europese regeling voor cyberbeveiligingscertificering afgegeven EU-verklaring van overeenstemming verbonden, waarin voor elk zekerheidsniveau de respectieve beveiligingsvoorschriften zijn vermeld, onder meer voor beveiligingsfuncties, en het overeenkomstige inspanningsniveau voor de evaluatie van een ICT-proces, -product of -dienst**. **Het certificaat of de EU-verklaring van overeenstemming wordt gekenmerkt door daaraan gerelateerde technische specificaties, normen en procedures, onder meer technische controles, die tot doel hebben als volgt het risico van cyberbeveiligingsincidenten te verminderen of die incidenten te voorkomen:**

a) **een Europees cyberbeveiligingscertificaat of een EU-verklaring van overeenstemming voor het** zekerheidsniveau "basis"**, biedt de zekerheid dat de ICT-processen, -producten en -diensten voldoen aan de betrokken beveiligingsvoorschriften, onder meer voor beveiligingsfuncties, en dat zij geëvalueerd zijn tot en met het niveau dat tot doel heeft de bekende basisrisico's van cyberincidenten en cyberaanvallen tot een minimum te beperken**. **De evaluatiewerkzaamheden behelzen ten minste een toetsing van technische documenten dan wel, indien het voorgaande niet van toepassing is, gelijkwaardige werkzaamheden** [...];.

b) **een Europees cyberbeveiligingscertificaat voor het** zekerheidsniveau "substantieel"**, biedt de zekerheid dat de ICT-processen, -producten en -diensten voldoen aan de respectieve beveiligingsvoorschriften, onder meer voor beveiligingsfuncties, en dat zij geëvalueerd zijn tot en met het niveau dat tot doel heeft de bekende cyberrisico's, cyberincidenten en cyberaanvallen door actoren met beperkte vaardigheden en middelen, tot een minimum te beperken**. **De evaluatiewerkzaamheden behelzen ten minste: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, en testen of bij de ICT-processen, -producten en -diensten de benodigde beveiligingsfuncties correct worden toegepast; of, indien het voorgaande niet van toepassing is, gelijkwaardige werkzaamheden [...]**;.

c) **een Europees cyberbeveiligingscertificaat voor het** zekerheidsniveau "hoog"**, biedt de zekerheid dat de ICT-processen, -producten en -diensten voldoen aan de respectieve beveiligingsvoorschriften, onder meer voor beveiligingsfuncties, en dat zij geëvalueerd zijn tot en met het niveau dat tot doel heeft het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken**. **De evaluatiewerkzaamheden behelzen ten minste: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, controleren dat bij de ICT-processen, -producten en -diensten de beveiligingsfuncties correct, volgens de huidige stand van de techniek, worden toegepast, en het testen van hun weerbaarheid tegen deskundige aanvallers door middel van penetratietests; of, indien het voorgaande niet van toepassing is, gelijkwaardige werkzaamheden [...]**.

2a. In een Europese regeling voor cyberbeveiligingscertificering kunnen verscheidene evaluatieniveaus worden vastgelegd, afhankelijk van de grondigheid en de diepgang van de evaluatiemethode. Elk evaluatieniveau komt overeen met een van de zekerheidsniveaus en kan door middel van een passende combinatie van zekerheidscomponenten worden omschreven.

Artikel 47

Elementen van Europese regelingen voor cyberbeveiligingscertificering

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

a) het onderwerp en het toepassingsgebied van de certificering**regeling**, met inbegrip van het type of de categorieën van ICT-**processen**, -producten en -diensten die hieronder vallen, **evenals een beschrijving van de wijze waarop de certificeringsregeling tegemoetkomt aan de behoeften van de verwachte doelgroepen**;

b) [...] een vermelding van [...] de internationale, **Europese of nationale** norm **die bij de evaluatie wordt gevolgd**. **Indien geen normen beschikbaar zijn, worden de** [...]technische specificaties vermeld **die voldoen aan de voorschriften van bijlage II bij Verordening (EU) nr. 1025/2012, of, indien deze niet beschikbaar zijn, de technische specificaties of andere cyberbeveiligingsvoorschrifen van de regeling**;

c) indien van toepassing, één of meer zekerheidsniveaus;

ca) indien van toepassing, specifieke of aanvullende voorschriften voor conformiteits-beoordelingsinstanties, om te waarborgen dat zij beschikken over de technische competentie om de cyberbeveiligingsvoorschriften te evalueren;

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) **indien van toepassing**, de door een aanvrager aan de conformiteitsbeoordelingsinstanties te verstrekken **of anderszins beschikbaar te stellen** 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) [...] de regels voor het toezicht op de naleving van de certificaten **of van de EU-verklaring van overeenstemming**, met inbegrip van mechanismen om aan te tonen dat de vermelde cyberbeveiligingsvoorschriften onverminderd worden nageleefd;

h) **indien van toepassing**, de voorwaarden voor de toekenning, **verlenging**, handhaving, voortzetting, uitbreiding **en** beperking van het toepassingsgebied **van de certificering**;

i) regels over de gevolgen wanneer gecertificeerde of **zelf-geëvalueerde** ICT-producten en -diensten niet voldoen aan de voorschriften **van de regeling**;

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

k) **indien van toepassing**, regels over het bewaren van gegevens door conformiteitsbeoordelingsinstanties;

l) een overzicht van nationale **of internationale** regelingen voor cyberbeveiligingscertificering die betrekking hebben op hetzelfde type of dezelfde categorieën van ICT-**processen**, -producten en -diensten, **beveiligingsvoorschriften en toetsingscriteria en -methoden**;

m) de inhoud van het afgegeven certificaat of van de afgegeven **EU-verklaring van overeenstemming**.

ma) de bewaartermijn die de fabrikant of aanbieder van ICT-producten en -diensten in acht moet nemen voor de EU-verklaring van overeenstemming en de technische documentatie over alle betrokken informatie;

mb[...]) de maximale geldigheidsduur van certificaten;

mc[...]) het beleid inzake de openbaarmaking van afgegeven, gewijzigde en ingetrokken certificaten;

md[...]) de voorwaarden voor de wederzijdse erkenning van certificeringsregelingen met derde landen;

me[...]) indien van toepassing, regels met betrekking tot een mechanisme voor collegiale toetsing voor instanties die krachtens artikel 48, lid 4a, Europese cyberbeveiligings-certificaten afgeven met zekerheidsniveau "hoog" [...];

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

3. Indien een specifieke handeling van de Unie daarin voorziet, kan certificering **of de EU-verklaring van overeenstemming** op grond van een Europese regeling voor cyber-beveiligingscertificering, 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 voorschriften vast te stellen.

Artikel 47a

Conformiteitszelfbeoordeling

1. In een Europese regeling voor cyberbeveiligingscertificering kan worden bepaald dat een conformiteitsbeoordeling uitsluitend onder de verantwoordelijkheid van de fabrikant of leverancier van ICT-producten en -diensten kan worden uitgevoerd. Dit soort conformiteitsbeoordeling geldt uitsluitend voor ICT-producten en -diensten met een laag risico en met zekerheidsniveau "basis".

2. De fabrikant of aanbieder van ICT-producten en -diensten kan een EU-verklaring van overeenstemming afgeven waarin wordt verklaard dat is aangetoond dat aan de voorschriften van de regeling is voldaan. Door een dergelijke verklaring op te stellen aanvaardt de fabrikant of aanbieder van ICT-producten en -diensten verantwoordelijkheid voor de conformiteit van het ICT-product of -dienst met de in de regeling opgenomen voorschriften.

3. De fabrikant of aanbieder van ICT-producten en -diensten houdt de EU-verklaring van overeenstemming en de technische documenten betreffende alle dienstige informatie over de overeenstemming van de ICT-producten en -diensten met een regeling, ter beschikking van de in artikel 50, lid 1, bedoelde nationale autoriteiten voor cyberbeveiligingscertificering gedurende een termijn die is vastgesteld in de betrokken Europese regeling voor cyberbeveiligingscertificering. Aan de nationale instantie voor cyberbeveiligingscertificering en aan Enisa wordt een kopie van de EU-verklaring van overeenstemming voorgelegd.

4. De afgifte van de EU-verklaring van overeenstemming geschiedt vrijwillig, tenzij in de wetgeving van de Unie of de lidstaten anders is bepaald.

5. Een op grond van dit artikel afgegeven EU-verklaring van overeenstemming wordt in alle lidstaten erkend.

Artikel 48

Cyberbeveiligingscertificering

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

2. De certificering geschiedt vrijwillig, tenzij in de wetgeving van de Unie **of de lidstaten** anders is bepaald**.**

3. Een in dit artikel bedoeld Europees cyberbeveiligingscertificaat **voor zekerheidsniveau "basis" of "substantieel"** wordt afgegeven door de in artikel 51 bedoelde conformiteits-beoordelingsinstanties 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 cyberbeveiligings**certificering** erin voorzien dat een uit die regeling voortvloeiend Europees cyberbeveiligingscertificaat alleen door een overheids-instantie kan worden afgegeven. Die [...]instantie is een van de volgende organen:

a) een nationale autoriteit voor **cyberbeveiligings**certificering[...] als bedoeld in artikel 50, lid 1;

b) en **overheids**orgaan dat als conformiteitsbeoordelingsinstantie overeenkomstig artikel 51, lid 1, is geaccrediteerd; of

c) [...].

4a. Indien een Europese regeling voor cyberbeveiligingscertificering als bedoeld in artikel 44 een zekerheidsniveau "hoog" voorschrijft, kan het certificaat uitsluitend worden afgegeven door een in artikel 50, lid 1, bedoelde nationale autoriteit voor cyberbeveiligingscertificering, of, onder de volgende voorwaarden, door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 51:

a) nadat de nationale autoriteit voor cyberbeveiligingscertificering elk door de conformiteitsbeoordelingsinstantie afgegeven individueel certificaat heeft goedgekeurd; of

b) nadat de nationale autoriteit voor cyberbeveiligingscertificering deze taak volledig aan een conformiteitsbeoordelingsinstantie heeft overgedragen.

5. De natuurlijke persoon of rechtspersoon die zijn ICT-**processen**, -producten of -diensten aan het certificeringsmechanisme onderwerpt, **stelt** aan de in artikel 51 bedoelde conformiteitsbeoordelingsinstantie of **aan de in artikel 50 bedoelde nationale autoriteit voor cyberbeveiligingscertificering**, **indien deze autoriteit het certificaat afgeeft**, alle informatie **ter beschikking** die nodig is om de certificeringsprocedure uit te voeren.

5a. De houder van een certificaat stelt de instantie die het certificaat afgeeft in kennis van kwetsbaarheden of onregelmatigheden in verband met de beveiliging van gecertificeerde ICT-processen, -producten of -diensten die achteraf zijn vastgesteld en die gevolgen kunnen hebben voor de certificeringsvoorschriften. Deze instantie stuur deze informatie onverwijld door naar de nationale autoriteit voor cyber-beveiligingscertificering.

6. Certificaten worden afgegeven voor de **[...]periode die is vastgesteld in de betrokken certificeringsregeling** en kunnen worden verlengd, [...] mits nog steeds aan de desbetreffende voorschriften 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**-processen,** -producten en -diensten die onder een Europese regeling voor cyberbeveiligingscertificering vallen, niet langer gevolgen vanaf de datum die is vastgelegd in de overeenkomstig artikel 44, lid 4, vastgestelde uitvoeringshandeling. [...]**N**ationale regelingen voor cyberbeveiligingscertificering en de daaraan verbonden procedures voor ICT**-processen**, -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**-procressen,** -producten en -diensten die onder een van kracht zijnde Europese regeling voor cyberbeveiligingscertificering vallen.

3. Bestaande certificaten die op grond van nationale regelingen voor cyberbeveiligingscertificering zijn afgegeven **en onder een Europese regeling voor cyberbeveiligingscertificering vallen**, blijven geldig tot hun vervaldatum.

Artikel 50

Nationale autoriteiten voor* cyberbeveiligings*certificering[...]

1. Iedere lidstaat wijst **één** [...] nationale autoriteit [...] **of meerdere nationale autoriteiten** voor cyberbeveiligings**certificering**[...] **op zijn grondgebied** aan**, of wijst, in onderlinge overeenstemming met een andere lidstaat, een of meerdere in die andere lidstaat gevestigde autoriteiten aan die verantwoordelijk worden voor de toezichthoudende taken in de aanwijzende lidstaat**.

2. Elke lidstaat stelt de Commissie in kennis van de identiteit **en de toegewezen taken** van de aangewezen autoriteit**en**.

3. **Onverminderd het bepaalde in artikel 48, lid 4, onder a), en artikel 48, lid 4a, is** [...]**e**lke nationale autoriteit voor cyberbeveiligingscertificering[...] op het vlak van haar organisatie, financieringsbeslissingen, rechtsstructuur en besluitvorming onafhankelijk van de entiteiten waarop zij toezicht houdt.

3a. De lidstaten zorgen ervoor dat de werkzaamheden van de nationale autoriteit voor cyberbeveiligingscertificering met betrekking tot de afgifte van certificaten overeenkomstig artikel 48, lid 4, onder a), en artikel 48, lid 4a, worden verricht onder een strikte scheiding tussen de functies en verantwoordelijkheden, enerzijds, en de in dit artikel bedoelde toezichthoudende werkzaamheden, anderzijds, en dat beide werkzaamheden onafhankelijk van elkaar worden verricht.

4. De lidstaten zien erop toe dat de nationale autoriteiten voor **cyberbeveiligings**certificering[...] 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 **cyberbeveiligings**certificering[...]:

a) [...]

aa) monitoren en handhaven de verplichtingen van fabrikanten of leveranciers van ICT-producten en -diensten die gevestigd zijn op hun respectieve grondgebieden als bedoeld in artikel 47 bis, leden 2 en 3, en in de overeenkomstige Europese regeling voor cyberbeveiligingscertificering;

b) [...] **assisteren de nationale accreditatie-instanties bij de monitoring van en het toezicht op** de werkzaamheden van de conformiteitsbeoordelingsinstanties voor de toepassing van deze verordening, [...] **onverminderd artikel 51, lid 1b**;

ba) monitoren en houden toezicht op de werkzaamheden van de in artikel 48, lid 4, bedoelde instanties;

bb) verlenen vergunningen aan de in artikel 51, lid 1b, bedoelde conformiteitsbeoordelings-instanties en gaan over tot het beperken, opschorten of intrekken van bestaande vergunningen indien zij niet aan de in deze verordening neergelegde vereisten voldoen;

c) behandelen klachten van natuurlijke of rechtspersonen over certificaten die zijn afgegeven door [...] **de nationale autoriteit voor cyberbeveiligingscertificering of, overeenkomstig artikel 48, lid 4a, door conformiteitsbeoordelingsinstanties**, onderzoeken in passende mate de inhoud van de klacht 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 **cyberbeveiligings**certificering[...]of andere overheidsinstanties, onder meer door informatie uit te wisselen over de mogelijke niet-overeenstemming van ICT**-processen,** -producten en -diensten met de voorschriften van deze verordening of met specifieke Europese regelingen voor cyberbeveiligingscertificering;

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

7. Elke nationale autoriteit voor **cyberbeveiligings**certificering[...] beschikt ten minste over de volgende bevoegdheden:

a) conformiteitsbeoordelingsinstanties**,** [...] houders van Europese cyberbeveiligingscertificaten **en afgevers van EU-verklaringen van overeenstemming** 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**,** [...] houders van Europese cyberbeveiligingscertificaten **en afgevers van EU-verklaringen van overeenstemming** 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**,** [...] houders van Europese cyberbeveiligingscertificaten **en afgevers van EU-verklaringen van overeenstemming** 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) intrekken, conform het nationale recht, van **door de nationale autoriteit voor cyber-beveiligingscertificering of, overeenkomstig artikel 48, lid 4a, door conformiteits-beoordelingsinstanties afgegeven** certificaten die niet in overeenstemming zijn met deze verordening of een Europese regeling voor cyberbeveiligingscertificering;

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 **cyberbeveiligings**certificering[...] 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**-processen,** -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.

1a. Indien een Europees cyberveiligheidscertificaat is afgegeven door een nationale autoriteit voor cyberbeveiligingscertificering overeenkomstig artikel 48, lid 4, onder a), en artikel 48, lid 4a, wordt de certificeringsinstantie van de nationale autoriteit voor cyberbeveiligingscertificering geaccrediteerd als conformiteitsbeoordelings-instantie uit hoofde van lid 1 van dit artikel.

1b. In voorkomend geval worden de conformiteitsbeoordelingsinstanties door de nationale autoriteit voor cyberbeveiligingscertificering gemachtigd om haar taken uit te voeren indien deze instanties voldoen aan specifieke of aanvullende voorschriften van de Europese certificeringsregeling overeenkomstig artikel 47, lid 1, onder ca).

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 **nemen binnen een redelijke termijn alle passende maatregelen om** [...] de accreditatie van een conformiteits-beoordelingsinstantie, als bedoeld in lid 1 van dit artikel, **te beperken, op te schorten of** in **te trekken** 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 **cyberbeveiligings-**certificering[...] de Commissie in kennis van de conformiteitsbeoordelingsinstanties die geaccrediteerd **en, in voorkomend geval, overeenkomstig artikel 51, lid 1b gemachtigd** zijn om certificaten af te geven voor gespecificeerde zekerheidsniveaus als vastgelegd in artikel 46 alsmede, 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 **cyberbeveiligings**certificering[...] kan bij de Commissie een verzoek indienen om een door die lidstaat 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 **cyberbeveiligings-**certificering[...] 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") wordt opgericht.

2. De groep bestaat uit **vertegenwoordigers van** de nationale autoriteiten voor **cyber-beveiligings**certificering[...] **of van andere relevante nationale autoriteiten**. [...] **Elk lid van de groep kan niet meer dan één andere lidstaat vertegenwoordigen.**

3. De groep heeft de volgende taken:

a) de Commissie adviseren en assisteren 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 beleids-benaderingen en de opstelling van Europese regelingen voor cyberbeveiligingscertificering;

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

ba) een advies uitbrengen over de potentiële regeling overeenkomstig artikel 44 van deze verordening;

c) [...] Enisa [...] **vragen** een potentiële Europese regeling voor cyberbeveiligingscertificering op te stellen overeenkomstig artikel 44 van deze verordening;

ca) opstellen en aannemen van richtsnoeren over criteria voor de beoordeling van voorstellen voor het opstellen van een potentiële regeling die bij de [...] groep zijn ingediend overeenkomstig artikel 44, lid 1a;

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

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

f) de samenwerking tussen de nationale autoriteiten voor **cyberbeveiligings**certificering[...] uit hoofde van deze titel vergemakkelijken door middel van **capaciteitsopbouw,** informatie-uitwisseling, met name door de vaststelling van methoden voor de efficiënte uitwisseling van informatie over alle aangelegenheden die verband houden met cyberbeveiligingscertificering**;**

fa) ondersteunen van **de uitvoering van het mechanisme voor collegiale toetsing volgens de regels die zijn vastgesteld in een Europese regeling voor cyberbeveiligingscertificering overeenkomstig artikel 47, lid 1, onder md) van deze verordening**.

4. De Commissie zit de groep voor **in de hoedanigheid van bemiddelaar** en verzorgt het secretariaat ervan, met de assistentie van Enisa overeenkomstig artikel 8, onder a).

Artikel 53 bis

Recht op het indienen van een klacht bij nationale autoriteiten voor* cyberbeveiligings*certificering

1. Natuurlijke personen of rechtspersonen hebben het recht bij de nationale autoriteit voor cyberbeveiligingscertificering een klacht in te dienen in verband met een certificaat dat is afgegeven door dezelfde autoriteit of, overeenkomstig artikel 48, lid 4a, door conformiteitsbeoordelingsinstanties.

2. De nationale autoriteit voor cyberbeveiligingscertificering waarbij de klacht is ingediend, stelt de klager in kennis van de voortgang en het resultaat van de klacht, alsmede van de mogelijke voorziening in rechte overeenkomstig artikel 53 ter.

Artikel 53 ter

Recht op een doeltreffende voorziening in rechte

1. Natuurlijke personen of rechtspersonen hebben het recht op een doeltreffende voorziening in rechte tegen een juridisch bindend besluit van een nationale autoriteit voor cyberbeveiligingscertificering dat hen aanbelangt.

2. Natuurlijke personen of rechtspersonen hebben het recht op een doeltreffende voorziening in rechte indien de nationale autoriteit voor cyberbeveiligings-certificering een klacht niet behandelt.

3. Procedures tegen een nationale autoriteit voor cyberbeveiligingscertificering worden ingesteld bij een gerechtelijke instantie van de lidstaat waar de autoriteit is gevestigd.

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, even-redig en afschrikkend. De lidstaten stellen de Commissie [uiterlijk op .../onverwijld] van deze voorschriften en deze maatregelen in kennis alsmede van 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 **5, lid 4, onder b),** 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 het effect, de doeltreffendheid en de 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 het effect, de doeltreffendheid en de 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 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 wat betreft alle eigendommen, overeenkomsten, wettelijke verplichtingen, arbeidsovereenkomsten, financiële verbintenissen en verplichtingen. 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

Inwerkingtreding

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

1a. Deze verordening is van toepassing met ingang van [...], met uitzondering van de artikelen 50, 51, 52, 53 bis, 53 ter en 54, die van toepassing zijn met ingang van [24 maanden na de datum van bekendmaking 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*

VEREISTEN WAARAAN CONFORMITEITSBEOORDELINGSINSTANTIES MOETEN VOLDOEN

Conformiteitsbeoordelingsinstanties die wensen te worden geaccrediteerd, moeten aan de volgende voorwaarden voldoen:

1. Een conformiteitsbeoordelingsinstantie is naar nationaal recht opgericht en heeft rechtspersoonlijkheid.

2. Een conformiteitsbeoordelingsinstantie is een derde partij die onafhankelijk is van de door haar beoordeelde organisaties of ICT-producten of -diensten.

3. Een instantie die lid is van een organisatie van ondernemers en/of van een vakorganisatie die ondernemingen vertegenwoordigt die betrokken zijn bij het ontwerpen, vervaardigen, leveren, monteren, gebruiken of onderhouden van de door haar beoordeelde ICT-producten of -diensten, kan als conformiteitsbeoordelingsinstantie worden beschouwd op voorwaarde dat haar onafhankelijkheid en de afwezigheid van belangenconflicten aangetoond worden.

4. Een conformiteitsbeoordelingsinstantie, haar hoogste leidinggevenden en het personeel dat de conformiteitsbeoordelingstaken verricht, mogen niet de ontwerper, fabrikant, leverancier, installateur, koper, eigenaar, gebruiker of onderhouder zijn van het ICT-product of de ICT-dienst die wordt beoordeeld, noch de gemachtigde van één van deze partijen. Dit vormt echter geen beletsel voor het gebruik van beoordeelde producten die nodig zijn voor de activiteiten van de conformiteitsbeoordelingsinstantie of voor het gebruik van de producten voor persoonlijke doeleinden.

5. Een conformiteitsbeoordelingsinstantie, de hoogste leidinggevenden en het personeel dat de conformiteitsbeoordeling verricht, zijn niet rechtstreeks of als vertegenwoordiger van de betrokken partijen betrokken bij het ontwerpen, vervaardigen of bouwen, op de markt brengen, installeren, gebruiken of onderhouden van deze ICT-producten of -diensten. Zij oefenen geen activiteiten uit die hun onafhankelijk oordeel of hun integriteit met betrekking tot conformiteitsbeoordelingsactiviteiten waarvoor zij zijn aangemeld, in het gedrang kunnen brengen. Dit geldt met name voor adviesdiensten.

6. Conformiteitsbeoordelingsinstanties zorgen ervoor dat de activiteiten van hun dochterondernemingen of onderaannemers geen afbreuk doen aan de vertrouwelijkheid, objectiviteit of onpartijdigheid van hun conformiteitsbeoordelingsactiviteiten.

7. Conformiteitsbeoordelingsinstanties en hun personeel voeren de conformiteitsbeoordelingsactiviteiten uit met de grootste mate van beroepsintegriteit en met de vereiste technische bekwaamheid op het specifieke gebied en zij zijn vrij van elke druk en beïnvloeding, waaronder van financiële aard, die hun oordeel of de resultaten van hun conformiteitsbeoordelingsactiviteiten kunnen beïnvloeden, in het bijzonder van personen of groepen van personen die belang hebben bij de resultaten van deze activiteiten.

8. Een conformiteitsbeoordelingsinstantie is in staat alle taken in verband met conformiteitsbeoordeling te vervullen die haar bij deze verordening zijn toegewezen, ongeacht of deze taken door de conformiteitsbeoordelingsinstantie zelf dan wel namens haar en onder haar verantwoordelijkheid worden verricht.

9. Een conformiteitsbeoordelingsinstantie beschikt te allen tijde, voor elke conformiteitsbeoordelingsprocedure en voor elke soort, categorie of subcategorie ICT-producten of -diensten over:

a) het nodige personeel met technische kennis en voldoende passende ervaring om de conformiteitsbeoordelingstaken te verrichten;

b) de nodige beschrijvingen van de procedures voor de uitvoering van de conformiteitsbeoordeling, waarbij de transparantie en de mogelijkheid tot reproductie van deze procedures worden gewaarborgd. Zij beschikt over een gepast beleid en geschikte procedures om een onderscheid te maken tussen taken die zij als aangemelde instantie verricht en andere activiteiten;

c) de nodige procedures voor de uitoefening van haar activiteiten, die naar behoren rekening houden met de omvang van een onderneming, de sector waarin deze actief is, de structuur ervan, de relatieve complexiteit van de technologie van de betrokken ICT-producten of -diensten en het massa- of seriële karakter van het productieproces.

10. Een conformiteitsbeoordelingsinstantie beschikt over de nodige middelen om de technische en administratieve taken in verband met de conformiteitsbeoordelings-activiteiten op passende wijze uit te voeren en heeft toegang tot alle vereiste apparatuur en faciliteiten.

11. Het voor de uitvoering van de conformiteitsbeoordelingsactiviteiten verantwoordelijke personeel:

a) heeft een gedegen technische en beroepsopleiding gevolgd die alle relevante conformiteits-beoordelingsactiviteiten omvat;

b) beschikt over bevredigende kennis van de eisen inzake de beoordelingen die het verricht en voldoende bevoegdheden om deze beoordelingen uit te voeren;

c) beschikt over voldoende kennis van en inzicht in de toepasselijke eisen en beproevings-normen;

d) beschikt over de bekwaamheid om certificaten, dossiers en rapporten op te stellen die aantonen dat de beoordelingen zijn verricht.

12. De onpartijdigheid van de conformiteitsbeoordelingsinstanties, hun hoogste leiding-gevenden en het beoordelingspersoneel is gewaarborgd.

13. De beloning van de hoogste leidinggevenden en van het beoordelingspersoneel van een conformiteitsbeoordelingsinstantie hangt niet af van het aantal uitgevoerde beoordelingen of van de resultaten daarvan.

14. Conformiteitsbeoordelingsinstanties sluiten een aansprakelijkheidsverzekering af, tenzij de wettelijke aansprakelijkheid op basis van het nationale recht door de staat wordt gedekt of de lidstaat zelf rechtstreeks verantwoordelijk is voor de conformiteitsbeoordeling.

15. Het personeel van een conformiteitsbeoordelingsinstantie is gebonden aan het beroepsgeheim ten aanzien van alle informatie waarvan het kennisneemt bij de uitoefening van zijn taken uit hoofde van deze verordening of overeenkomstig bepalingen van nationaal recht die daaraan uitvoering geven, behalve ten opzichte van de bevoegde autoriteiten van de lidstaat waarin de werkzaamheden plaatsvinden.

16. Conformiteitsbeoordelingsinstanties voldoen aan de eisen van **de toepasselijke** norm **die in het kader van Verordening (EG) nr. 765/2008 is geharmoniseerd voor de accreditatie van conformiteitsbeoordelingsinstanties die processen, producten of diensten certificeren[...].**

17. Conformiteitsbeoordelingsinstanties zien erop toe dat testlaboratoria die worden gebruikt voor conformiteitsbeoordelingen voldoen aan de eisen van **de toepasselijke** norm **die in het kader van Verordening (EG) nr. 765/2008 is geharmoniseerd voor de accreditatie van laboratoria die tests uitvoeren** [...].