VERORDENING (EU) 2019/881 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 17 april 2019

inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (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 ([1]),

Gezien het advies van het Comité van de Regio's ([2]),

Handelend volgens de gewone wetgevingsprocedure ([3]),

Overwegende hetgeen volgt:

(1) Netwerk- en informatiesystemen alsmede elektronischecommunicatienetwerken en -diensten spelen een cruciale rol in de maatschappij en zijn de ruggengraat van de economische groei geworden. Informatie- en communicatietechnologie (ICT) vormt de basis van de complexe systemen die dagelijkse 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, organisaties en ondernemingen in de hele Unie maken alom gebruik van netwerk- en informatiesystemen. Digitalisering en connectiviteit zijn cruciale kenmerken aan het worden van steeds meer producten en diensten, en door de opkomst van het internet der dingen (IoT) zal naar verwachting de volgende tien jaar in de hele Unie een uitermate groot aantal 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 die context toe dat individuele gebruikers en gebruikers binnen organisaties en ondernemingen te weinig informatie hebben over de cyberbeveiligingskenmerken van ICT-producten, -diensten en -processen, hetgeen schadelijk is voor het vertrouwen in digitale oplossingen. Netwerk- en informatiesystemen zijn in staat om alle aspecten van ons leven te ondersteunen en zij vormen de motor van de economische groei in de Unie. Zij vormen de hoeksteen om de digitale eengemaakte markt tot stand te kunnen brengen.

(3) De toenemende digitalisering en connectiviteit verhogen cyberbeveiligingsrisico's, waardoor de maatschappij als geheel kwetsbaarder wordt voor cyberdreigingen en waardoor de gevaren waaraan individuen, waaronder kwetsbare personen zoals kinderen, zijn blootgesteld worden verergerd. Om die risico's te beperken, moeten alle noodzakelijke maatregelen worden genomen om de cyberbeveiliging in de Unie te versterken, zodat netwerk- en informatiesystemen, communicatienetwerken, digitale producten, diensten en toestellen die worden gebruikt door burgers, organisaties en bedrijven — van kleine en middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie ([4]) tot exploitanten van cruciale infrastructuurvoorzieningen — beter beschermd worden tegen cyberdreigingen.

([1]) PB C 227 van 28.6.2018, blz. 86.
([2]) PB C 176 van 23.5.2018, blz. 29.
([3]) Standpunt van het Europees Parlement van 12 maart 2019 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 9 april 2019.
([4]) Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (OJ L 124, 20.5.2003, blz. 36).

(4) Door de relevante informatie openbaar te maken, draagt het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa), zoals opgericht bij Verordening (EU) nr. 526/2013 van het Europees Parlement en de Raad ([5]), bij aan de ontwikkeling van de cyberbeveiligingssector in de Unie, met name kleine en middelgrote ondernemingen en startende bedrijven. Enisa moet streven naar een nauwere samenwerking met universiteiten en onderzoekscentra, om de afhankelijkheid van cyberbeveiligingsproducten en -diensten van buiten de Unie te helpen verminderen en toeleveringsketens binnen de Unie te versterken.

(5) 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 plaatsvinden, zijn de bevoegdheden en beleidsmaatregelen van cyberbeveiligingsautoriteiten en rechtshandhavingsinstanties voornamelijk nationaal. Grootschalige incidenten kunnen de voorziening van essentiële diensten in de gehele Unie verstoren. Dit vereist een doeltreffend en gecoördineerd antwoord en crisisbeheer op Unieniveau, voortbouwend op specifiek beleid en bredere instrumenten voor Europese solidariteit en wederzijdse bijstand. Voorts zijn een regelmatige beoordeling van de staat van de cyberbeveiliging en -weerbaarheid in de Unie, op basis van betrouwbare Uniegegevens, alsmede systematische prognoses van toekomstige ontwikkelingen, uitdagingen en dreigingen, op Unie- en mondiaal niveau, belangrijk voor de beleidmakers, het bedrijfsleven en de gebruikers.

(6) Gezien de toegenomen cyberbeveiligingsuitdagingen waarmee de Unie wordt geconfronteerd, moet een uitvoerige reeks maatregelen worden genomen die voortbouwen op eerdere Uniemaatregelen en die moeten bijdragen tot doelstellingen die elkaar wederzijds versterken. Zo moeten de capaciteiten en paraatheid van de lidstaten en het bedrijfsleven verder worden versterkt en moet de samenwerking, het delen van informatie en de coördinatie tussen de lidstaten en de instellingen, organen, en instanties van de Unie worden verbeterd. Gezien de grenzeloze aard van cyberdreigingen moet, in aanvulling op het optreden van de lidstaten, de capaciteiten op Unieniveau worden versterkt, met name in geval van grootschalige grensoverschrijdende incidenten en crises, waarbij het belang van handhaving en verdere versterking van de nationale capaciteiten om te kunnen reageren op cyberdreigingen van elke omvang in aanmerking moet worden genomen.

(7) Er moeten ook meer inspanningen worden geleverd om de burgers, organisaties en ondernemingen bewuster te maken van cyberbeveiligingsvraagstukken. Aangezien incidenten het vertrouwen in digitaledienstverleners en in de digitale eengemaakte markt zelf ondermijnen, in het bijzonder bij consumenten, moet het vertrouwen in de digitale eengemaakte markt verder worden versterkt door over het beveiligingsniveau van ICT-producten, -diensten en -processen op transparante wijze informatie te verstrekken waarin wordt benadrukt dat zelfs een hoog niveau van cyberbeveiligingscertificering niet kan garanderen dat een ICT-product, -dienst of -proces volkomen beveiligd is. Een toename van het vertrouwen kan worden bevorderd door middel van een Uniebrede certificering die voorziet in gemeenschappelijke cyberbeveiligingsvoorschriften en evaluatiecriteria, ongeacht de nationale markten en sectoren.

(8) Cyberbeveiliging is niet alleen maar een technologievraagstuk; het menselijk gedrag is even belangrijk. Daarom moet „cyberhygiëne" sterk worden aangemoedigd, namelijk eenvoudige routinemaatregelen die, indien zij regelmatig door burgers, organisaties en bedrijven worden toegepast en uitgevoerd, hun blootstelling aan risico's van cyberdreigingen tot een minimum beperken.

(9) Ter versterking van cyberbeveiligingsstructuren in de Unie is het van belang dat de capaciteiten van de lidstaten om uitgebreid te reageren op cyberdreigingen, met inbegrip van grensoverschrijdende incidenten, worden gehandhaafd en ontwikkeld.

(10) Bedrijven en individuele consumenten moeten beschikken over nauwkeurige informatie met betrekking tot het zekerheidsniveau waarop hun ICT-producten, -diensten en -processen zijn gecertificeerd. Tegelijkertijd is geen enkel ICT-product en geen enkele ICT-dienst volledig cyberbeveiligd en moeten de basisregels van cyberhygiëne worden bevorderd en moeten zij prioriteit krijgen. Gezien de toenemende beschikbaarheid van IoT-apparaten kan de particuliere sector een reeks vrijwillige maatregelen treffen om het vertrouwen in de beveiliging van ICT-producten, -diensten en -processen te vergroten.

(11) Moderne ICT-producten en -systemen maken vaak gebruik van technologieën en onderdelen die door een of meer derde partijen worden geleverd, zoals softwaremodules, bibliotheekprogramma's of applicatieprogramma-interfaces, en steunen daarop. Deze omstandigheid, die „afhankelijkheid" wordt genoemd, kan een aanvullend cyberbeveiligingsrisico inhouden, aangezien kwetsbaarheden in onderdelen van derde partijen ook de veiligheid van de ICT-producten, -diensten en -processen kunnen aantasten. In veel gevallen stelt de identificatie en documentatie van dergelijke afhankelijkheden de eindgebruikers van ICT-producten, -diensten en -processen in staat om de cyberbeveiligingsrisico's beter te beheersen door bijvoorbeeld het beleid en de herstelprocedures van de gebruikers inzake kwetsbaarheden van de cyberbeveiliging te verbeteren.

([5]) 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).

(12) Bij het ontwerp en de ontwikkeling van ICT-producten, -diensten en -processen betrokken organisaties, fabrikanten en aanbieders moeten ertoe worden aangespoord om al in de eerste fase van ontwerp en ontwikkeling maatregelen te treffen om ervoor te zorgen dat het beveiligingsniveau van ICT-producten, -diensten en -processen zo hoog mogelijk is, zodat cyberaanvallen zijn ingecalculeerd en de gevolgen daarvan zijn ingeschat en tot een minimum beperkt („beveiliging door ontwerp"). Beveiliging moet tijdens de gehele levensduur van het ICT-product, de ICT-dienst of het ICT-proces worden gewaarborgd door middel van ontwerp- en ontwikkelingsprocessen die constant evolueren om het risico op schade door kwaadwillig gebruik te verminderen.

(13) Ondernemingen, organisaties en overheidsinstanties dienen de door hen ontworpen ICT-producten, -diensten of -processen zodanig te configureren dat een hoger beveiligingsniveau is gewaarborgd, waarbij de eerste gebruiker de meest beveiligde instelling wordt aangeboden („beveiliging door standaardinstellingen"), waardoor het voor gebruikers minder lastig wordt om een ICT-product, -dienst of -proces geschikt te configureren. De beveiliging door standaardinstellingen moet eenvoudig en betrouwbaar werken zonder dat daarvoor een uitvoerige configuratie, specifiek technisch inzicht of niet voor de hand liggende handelingen van de gebruiker vereist zijn. Als uit een risico- en bruikbaarheidsanalyse per geval blijkt dat een dergelijke standaardinstelling niet haalbaar is, moeten gebruikers ertoe worden aangespoord voor de meest beveiligde instelling te kiezen.

(14) Bij Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad ([6]) is Enisa opgericht teneinde bij te dragen tot een hoog en doeltreffend netwerk- en informatiebeveiligingsniveau in de Unie, en tot de ontwikkeling van een netwerk- en informatiebeveiligingscultuur ten bate van burgers, consumenten, ondernemingen en overheidsdiensten. Bij Verordening (EG) nr. 1007/2008 van het Europees Parlement en de Raad ([7]) is het mandaat van Enisa tot en met maart 2012 verlengd. Bij Verordening (EU) nr. 580/2011 van het Europees Parlement en de Raad ([8]) is het mandaat van Enisa nog eens verlengd tot en met 13 september 2013. Bij Verordening (EU) nr. 526/2013 is het mandaat van Enisa tot en met 19 juni 2020 verlengd.

(15) De Unie heeft reeds belangrijke maatregelen genomen om voor cyberbeveiliging te zorgen en om het vertrouwen in digitale technologieën te vergroten. In 2013 werd de strategie inzake cyberbeveiliging van de Europese Unie goedgekeurd als leidraad voor de beleidsreactie van de Unie op cyberdreigingen en -risico's. Om de burgers online beter te beschermen, werd in 2016 de eerste rechtshandeling van de Unie inzake cyberbeveiliging in de vorm van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([9]) vastgesteld. Bij Richtlijn (EU) 2016/1148 werden eisen vastgesteld betreffende nationale capaciteiten 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, levering en distributie van drinkwater, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, digitale infrastructuur en belangrijke digitaledienstverleners (zoekmachines, cloudcomputingdiensten en onlinemarktplaatsen).

Aan Enisa werd een sleutelrol toebedeeld bij het ondersteunen van de uitvoering van die richtlijn. Daarnaast is de doeltreffende bestrijding van cybercriminaliteit een belangrijke prioriteit in de Europese veiligheidsagenda, die bijdraagt tot de algemene doelstelling om een hoog cyberbeveiligingsniveau tot stand te brengen. Andere rechtshandelingen zoals Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([10]) en de Richtlijnen 2002/58/EG ([11]) en (EU) 2018/1972 ([12]) van het Europees Parlement en de Raad, dragen eveneens bij tot een hoog cyberbeveiligingsniveau in de digitale eengemaakte markt.

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016, blz. 1).

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

([11]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

([12]) Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (PB L 321 van 17 december 2018, blz. 36).

(16) Sinds de strategie inzake cyberbeveiliging van de Europese Unie in 2013 werd vastgesteld en het mandaat van Enisa de laatste keer werd herzien, is de algehele beleidscontext aanzienlijk veranderd doordat de mondiale omgeving onzekerder en onveiliger is geworden. Tegen die achtergrond en in het licht van de positieve ontwikkeling van de rol die Enisa speelt als referentiepunt voor advies en expertise, als bemiddelaar van samenwerking en capaciteitsopbouw, evenals binnen het kader van het nieuwe cyberbeveiligingsbeleid van de Unie, moet het mandaat van Enisa worden herzien teneinde de rol van Enisa in de veranderde cyberbeveiligingsomgeving te bepalen en te waarborgen dat het op doeltreffende wijze bijdraagt tot de respons van de Unie op cyberbeveiligingsuitdagingen die voortvloeien uit het radicaal gewijzigde cyberdreigingslandschap, waarvoor, zoals gedurende de evaluatie van Enisa is gebleken, het huidige mandaat niet toereikend is.

(17) Enisa, zoals bij deze verordening opgericht, moet Enisa, zoals opgericht bij Verordening (EG) nr. 526/2013, opvolgen. Enisa moet de taken uitvoeren die hem bij deze verordening en rechtshandelingen van de Unie op het gebied van cyberbeveiliging aan worden toegewezen, onder meer door advies en expertise te verstrekken en te fungeren als informatie- en kenniscentrum van de Unie. Enisa moet de uitwisseling van beste praktijken tussen de lidstaten en particuliere belanghebbenden bevorderen, beleidsaanbevelingen doen aan de Commissie en de lidstaten, fungeren als referentiepunt voor sectorale beleidsinitiatieven van de Unie inzake cyberbeveiligingsvraagstukken, en de operationele samenwerking tussen de lidstaten onderling en tussen de lidstaten en instellingen, organen en instanties van de Unie bevorderen.

(18) Binnen het kader van Besluit 2004/97/EG, Euratom, in onderlinge overeenstemming genomen door de vertegenwoordigers van de lidstaten, op het niveau van de staatshoofden en regeringsleiders bijeen ([13]), 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 soepele en efficiënte werking van Enisa. Met het oog op de goede en efficiënte uitvoering van zijn taken, het werven en behouden van zijn personeel en efficiëntere netwerkactiviteiten is het noodzakelijk dat Enisa op een geschikte locatie wordt gehuisvest, waar onder meer goede vervoersverbindingen en geschikte faciliteiten voorhanden zijn voor echtgenoten en kinderen die meereizen met de leden van het personeel van Enisa. De noodzakelijke bepalingen moeten worden vastgelegd in een overeenkomst tussen Enisa en de lidstaat van vestiging, die wordt gesloten nadat de raad van bestuur van Enisa daarmee heeft ingestemd.

(19) Gezien de toenemende cyberbeveiligingsrisico's en -uitdagingen waarmee de Unie wordt geconfronteerd, moeten de financiële en personele middelen die aan Enisa worden toegewezen, worden uitgebreid om recht te doen aan zijn versterkte rol en taken en zijn cruciale positie in het ecosysteem van organisaties die het digitale ecosysteem van de Unie verdedigen, zodat Enisa de bij deze verordening toegekende taken op doeltreffende wijze kan uitvoeren.

(20) Enisa moet een hoog expertiseniveau ontwikkelen en handhaven, en fungeren als een referentiepunt dat op grond van 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 vertrouwen in de eengemaakte markt schept. Enisa moet nationale inspanningen actief ondersteunen en proactief bijdragen aan inspanningen van de Unie en daarbij zijn taken uitvoeren in volledige samenwerking met de instellingen, organen en instanties van de Unie en de lidstaten, en daarbij dubbel werk vermijden en synergie bevorderen. Daarnaast moet Enisa voortbouwen op de input van en de samenwerking met de particuliere sector en andere relevante belanghebbenden. In een reeks taken moet worden vastgesteld hoe Enisa zijn doelstellingen moet verwezenlijken en toch flexibel kan functioneren.

(21) Om gepaste ondersteuning aan de operationele samenwerking van de lidstaten te kunnen bieden, moet Enisa zijn technische en menselijke capaciteiten en vaardigheden verder versterken. Enisa moet zijn kennis en capaciteit uitbreiden. Enisa en de lidstaten zouden op vrijwillige basis programma's kunnen ontwikkelen om nationale deskundigen bij het Enisa te detacheren en aldus een groep deskundigen kunnen samenbrengen en personeel kunnen uitwisselen.

(22) Enisa moet de Commissie bijstaan met advies, standpunten en analyses over alle aangelegenheden van de Unie in verband met de ontwikkeling, actualisering en herziening van beleid en wetgeving op het gebied van cyberbeveiliging en de sectorspecifieke aspecten daarvan teneinde de relevantie van Uniebeleid en -wetgeving met een cyberbeveiligingsdimensie te vergroten en te zorgen voor een consistente uitvoering van dat beleid en die wetgeving op nationaal niveau. Enisa moet als referentiepunt voor advies en expertise fungeren ten behoeve van sectorspecifieke beleids- en wetgevingsinitiatieven van de Unie waarbij cyberbeveiligingsvraagstukken zijn betrokken. Enisa moet het Europees Parlement regelmatig van zijn werkzaamheden op de hoogte brengen.

([13]) Besluit (EG, Euratom) 2004/97, in onderlinge overeenstemming genomen door de vertegenwoordigers van de lidstaten, op het niveau van de staatshoofden en regeringsleiders bijeen, van 13 december 2003 inzake de vestigingsplaatsen van bepaalde bureaus en organen van de Europese Unie (PB L 29 van 3.2.2004, blz. 15).

(23) De openbare kern van het open internet, namelijk de belangrijkste protocollen en infrastructuur, die een mondiaal publiek goed zijn, vormen de essentiële functionaliteit van het internet als geheel en ondersteunen de normale werking ervan. Enisa dient de beveiliging van de openbare kern van het open internet en de stabiliteit van zijn werking te ondersteunen, met inbegrip van, maar niet beperkt tot, cruciale protocollen (met name DNS, BGP en IPv6), de werking van het domeinnaamsysteem (waaronder de werking van alle topniveaudomeinen) en de werking van de „root zone".

(24) De onderliggende taak van Enisa bestaat uit de bevordering van de consistente uitvoering van het desbetreffende juridische kader, en met name de doeltreffende uitvoering van Richtlijn (EU) 2016/1148 en andere relevante rechtsinstrumenten met cyberbeveiligingsaspecten, hetgeen 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 omvattende, beleidsoverschrijdende aanpak voor de opbouw van cyberweerbaarheid.

(25) Enisa moet de lidstaten en de instellingen, organen en instanties van de Unie bijstaan bij hun inspanningen om capaciteiten en paraatheid te ontwikkelen en te vergroten om cyberdreigingen en -incidenten in verband met de beveiliging van netwerk- en informatiesystemen te voorkomen, op te sporen en aan te pakken. Enisa moet met name steun verlenen bij de ontwikkeling en versterking van bij Richtlijn (EU) 2016/1148 voorziene nationale computer security incident response teams („CSIRT's") en CSIRT's van de Unie, met het oog op een hoog gemeenschappelijk niveau aan volwassenheid in de Unie. De activiteiten van Enisa in verband met de operationele capaciteiten van de lidstaten moeten actief ondersteuning bieden aan de maatregelen die de lidstaten zelf nemen om hun verplichtingen op grond van Richtlijn (EU) 2016/1148 na te komen en mogen derhalve daarvoor niet in de plaats komen.

(26) Enisa moet ook helpen bij de ontwikkeling en actualisering van strategieën op Unieniveau en, op verzoek, op het niveau van de lidstaten, voor de beveiliging van netwerk- en informatiesystemen, en met name inzake cyberbeveiliging, en het dient de verspreiding van dergelijke strategieën te bevorderen en de voortgang van hun uitvoering te volgen. Enisa moet ook meehelpen te voorzien in de behoefte aan opleidingen en opleidingsmateriaal, ook ten aanzien van overheidsinstanties, en dient waar passend voor een groot deel de „opleiding voor opleiders" voor zijn rekening te nemen, voortbouwend op het digitalecompetentiekader voor burgers, teneinde de lidstaten en instellingen, organen en instanties van de Unie bij de ontwikkeling van hun eigen opleidingscapaciteit bij te staan.

(27) Enisa moet de lidstaten ondersteunen bij de bewustmaking en voorlichting inzake cyberbeveiliging, door de lidstaten onderling nauwer te helpen samenwerken en beste praktijken te helpen uitwisselen. Zulke steun zou kunnen bestaan uit de ontwikkeling van een netwerk van nationale voorlichtingscontactpunten en de ontwikkeling van een opleidingsplatform voor cyberbeveiliging. Het netwerk van nationale voorlichtingscontactpunten zou binnen het netwerk van nationale verbindingsfunctionarissen kunnen fungeren en zou binnen de lidstaten een startpunt kunnen vormen voor toekomstige coördinatie.

(28) Enisa moet de op grond van de bij Richtlijn (EU) 2016/1148 opgerichte samenwerkingsgroep helpen bij de uitvoering van zijn taken, in het bijzonder door expertise en advies te verstrekken en de uitwisseling van beste praktijken te bevorderen, met name wat betreft de identificatie van aanbieders van essentiële diensten door de lidstaten, alsmede met betrekking tot grensoverschrijdende afhankelijkheid, inzake risico's en incidenten.

(29) Ter bevordering van de samenwerking tussen de overheidssector en de particuliere sector enerzijds, en binnen de particuliere sector anderzijds, in het bijzonder ter ondersteuning van de bescherming van cruciale infrastructuur, moet Enisa het delen van informatie binnen en tussen sectoren, en met name de in bijlage II bij Richtlijn (EU) 2016/1148 vermelde sectoren, ondersteunen door te voorzien in beste praktijken en richtsnoeren over beschikbare instrumenten en over procedures, en richtsnoeren over de manier waarop problemen op regelgevingsgebied in verband met het delen van informatie kunnen worden opgelost, bijvoorbeeld door de oprichting van sectorale centra voor informatie-uitwisseling en -analyse te faciliteren.

(30) Doordat de mogelijke negatieve gevolgen van kwetsbaarheden in ICT-producten, -diensten en -processen constant toenemen, is het achterhalen en verhelpen van die kwetsbaarheden van groot belang om het algehele cyberbeveiligingsrisico te verkleinen. Gebleken is dat de samenwerking tussen enerzijds organisaties, fabrikanten of aanbieders van kwetsbare ICT-producten, -diensten en -processen, en anderzijds de leden van de onderzoeksgemeenschap op cyberbeveiligingsgebied en overheden die kwetsbaarheden aantreffen, een aanzienlijke stijging oplevert van het aantal kwetsbaarheden dat in ICT-producten, -diensten en -processen wordt ontdekt en verholpen. De gecoördineerde openbaarmaking van kwetsbaarheden behelst een gestructureerde samenwerkingsprocedure waarin kwetsbaarheden aan de eigenaar van het informatiesysteem worden gemeld, zodat de organisatie de kans krijgt een diagnose te stellen en de kwetsbaarheden te verhelpen voordat gedetailleerde informatie over de kwetsbaarheden aan derden of het publiek wordt vrijgegeven. In het kader van die procedure worden tussen de vinder en de organisatie ook afspraken gemaakt over het bekendmaken van die kwetsbaarheden. Gecoördineerd openbaarmakingsbeleid inzake kwetsbaarheden kan een belangrijk onderdeel vormen van de inspanningen die de lidstaten ter versterking van cyberbeveiliging leveren.

(31) Enisa moet vrijwillig gedeelde nationale verslagen van de CSIRT's en het interinstitutionele computercrisisteam voor de instellingen, organen en instanties van de Unie dat is opgericht bij de overeenkomst tussen het Europees Parlement, de Europese Raad, de Raad van de Europese Unie, de Europese Commissie, het Hof van Justitie van de Europese Unie, de Europese Centrale Bank, de Europese Rekenkamer, de Europese Dienst voor extern optreden, het Europees Economisch en Sociaal Comité, het Europees Comité van de Regio's en de Europese Investeringsbank betreffende de organisatie en het functioneren van een computercrisisteam voor de instellingen, organen en instanties van de Unie (CERT-EU) ([14]) verzamelen en analyseren om bij te dragen tot de instelling van gemeenschappelijke procedures, taal en terminologie voor de uitwisseling van informatie. Enisa moet daarbij de particuliere sector betrekken, binnen het kader van Richtlijn 2016/1148 die de grondslag legt voor de vrijwillige uitwisseling van technische informatie op operationeel niveau binnen het CSIRT-netwerk.

(32) Enisa moet een bijdrage leveren aan een reactie op Unieniveau in het geval van grootschalige grensoverschrijdende incidenten en -crises in verband met cyberbeveiliging. Enisa moet die taak overeenkomstig zijn mandaat krachtens deze verordening uitvoeren, met een aanpak die de lidstaten overeen dienen te komen in het kader van Aanbeveling (EU) 2017/1584 van de Commissie ([15]) en de conclusies van de Raad van 26 juni 2018 over een gecoördineerde EU-respons op grootschalige cyberincidenten en -crises. Tot die taak 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 dient Enisa, op verzoek van een of meer lidstaten, de operationele samenwerking tussen de lidstaten bij de behandeling van incidenten vanuit een technisch oogpunt te ondersteunen door de uitwisseling van relevante technische oplossingen tussen de lidstaten te vergemakkelijken en input te leveren voor mededelingen aan het publiek. Enisa moet operationele samenwerking ondersteunen door de regelingen voor dergelijke samenwerking door middel van regelmatige cyberbeveiligingsoefeningen te testen.

(33) Bij de ondersteuning van de operationele samenwerking moet Enisa door middel van gestructureerde samenwerking de beschikbare technische en operationele expertise van CERT-EU gebruiken. Dergelijke gestructureerde samenwerking kan voortbouwen op de expertise van Enisa. Indien passend moeten specifieke regelingen tussen de twee entiteiten worden vastgesteld teneinde de praktische uitvoering van dergelijke samenwerking te bepalen en dubbel werk te vermijden.

(34) Bij de uitvoering van zijn taak ter ondersteuning van operationele samenwerking binnen het CSIRT-netwerk moet Enisa in staat zijn ondersteuning te bieden aan de lidstaten indien zij daarom verzoeken, bijvoorbeeld door advies te geven omtrent het vergroten van hun capaciteiten om incidenten te voorkomen, op te sporen en aan te pakken, door de technische afhandeling van incidenten met aanzienlijke of substantiële gevolgen te vergemakkelijken of door te zorgen voor analyses van cyberdreigingen en -incidenten. Enisa dient de technische afhandeling te vergemakkelijken van incidenten met aanzienlijke of substantiële gevolgen, in het bijzonder door het vrijwillig delen van technische oplossingen tussen lidstaten te ondersteunen of gecombineerde technische informatie op te stellen, waaronder door de lidstaten vrijwillig gedeelde technische oplossingen. In Aanbeveling (EU) 2017/1584 wordt aanbevolen dat de lidstaten te goeder trouw samenwerken en zowel onderling als met Enisa onverwijld informatie delen over grootschalige cyberincidenten en -crises. Die informatie moet Enisa verder helpen bij de uitoefening van zijn taak om operationele samenwerking te ondersteunen.

(35) Als onderdeel van de regelmatige samenwerking op technisch niveau ter ondersteuning van het situatiebewustzijn van de Unie, moet Enisa regelmatig en in nauwe samenwerking met de lidstaten grondige een technisch situatieverslag inzake Uniecyberbeveiliging (EU Cybersecurity Technical Situation Report) over incidenten en cyberdreigingen opstellen, op basis van openbaar beschikbare informatie en eigen analyses en verslagen die het ontvangt van de CSIRT's van de lidstaten of de bij Richtlijn (EU) 2016/1148 opgerichte nationale centrale contactpunten inzake de beveiliging van netwerk- en informatiesystemen („centrale contactpunten"), beide op vrijwillige basis, het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) van Europol, CERT-EU, en, voor zover passend, het Inlichtingen- en situatiecentrum van de Europese Unie (EU-INTCEN) van de Europese Dienst voor extern optreden. Dat verslag moet ter beschikking worden gesteld van de Raad, de Commissie, de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid, en het CSIRT-netwerk.

(36) De steun die Enisa op verzoek van de betrokken lidstaten verleent aan technische onderzoeken achteraf van incidenten met aanzienlijke of substantiële gevolgen dient te zijn gericht op de preventie van toekomstige incidenten. De betrokken lidstaten moeten de nodige informatie en bijstand verstrekken opdat Enisa het technisch onderzoek achteraf doeltreffend kan steunen.

([14]) PB C 12 van 13.1.2018, blz. 1.

([15]) Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises (PB L 239 van 19.9.2017, blz. 36).

(37) De lidstaten kunnen de bij het incident betrokken ondernemingen verzoeken medewerking te verlenen door Enisa de nodige informatie en bijstand te geven, zonder afbreuk te doen aan hun recht om commercieel gevoelige informatie en informatie die relevant is voor de openbare veiligheid te beschermen.

(38) Om de cyberbeveiligingsuitdagingen beter te begrijpen en de lidstaten en de instellingen, organen en instanties van de Unie strategisch van langetermijnadvies te voorzien, moet Enisa bestaande en opkomende cyberbeveiligingsrisico's analyseren. Daartoe moet Enisa, in samenwerking met de lidstaten en, wanneer passend, met bureaus voor de statistiek en andere entiteiten, relevante voor iedereen beschikbare of vrijwillig gedeelde 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 Enisa de lidstaten en de instellingen, organen en instanties van de Unie door de analyse van cyberdreigingen, -kwetsbaarheden en -incidenten ondersteunen bij het in kaart brengen van nieuwe cyberbeveiligingsrisico's en het voorkomen van incidenten.

(39) Om de weerbaarheid van de Unie te versterken, moet Enisa expertise ontwikkelen op het gebied van de cyberbeveiliging van infrastructuren, in het bijzonder ter ondersteuning van de in bijlage II bij Richtlijn (EU) 2016/1148 vermelde sectoren en de infrastructuren die worden gebruikt door de in bijlage III bij die richtlijn vermelde digitaledienstverleners, door advies, richtsnoeren en beste praktijken te verstrekken. Met het oog op het waarborgen van gemakkelijkere toegang tot beter gestructureerde informatie over cyberbeveiligingsrisico's en mogelijke oplossingen, moet Enisa zorgen voor de ontwikkeling en instandhouding van het „informatiecentrum" van de Unie, één centraal portaal dat het publiek voorziet van informatie over cyberbeveiliging die afkomstig is van de instellingen, organen en instanties van de Unie en de lidstaten. Het vergemakkelijken van de toegang tot beter gestructureerde informatie over cyberbeveiligingsrisico's en mogelijke oplossingen kan de lidstaten ook helpen hun capaciteiten te versterken en hun praktijken op elkaar af te stemmen, en zo de een algehele weerbaarheid ten aanzien van cyberaanvallen verhogen.

(40) Enisa moet ertoe bijdragen het publiek bewuster te maken van cyberbeveiligingsrisico's, onder meer door een Uniebrede bewustmakingscampagne, door voorlichting te bevorderen, en richtsnoeren te verstrekken inzake goede praktijken voor individuele gebruikers, gericht op burgers, organisaties en bedrijven. Verder moet Enisa bijdragen tot de bevordering van beste praktijken en oplossingen, onder meer inzake cyberhygiëne en cybergeletterdheid, op het niveau van burgers, organisaties en bedrijven, door publiek beschikbare informatie over significante incidenten te verzamelen en analyseren, en door verslagen en richtsnoeren op te stellen en te publiceren voor burgers, organisaties en bedrijven om het algemene paraatheids- en weerbaarheidsniveau te verhogen. Enisa moet er tevens naar streven consumenten van relevante informatie over toepasselijke certificeringsregelingen te voorzien, bijvoorbeeld door richtsnoeren en aanbevelingen te verstrekken. Enisa moet daarnaast regelmatig, overeenkomstig het bij de mededeling van de Commissie van 17 januari 2018 vastgestelde actieplan voor digitaal onderwijs is vastgesteld en in samenwerking met de lidstaten en de instellingen, organen en instanties van de Unie, aan de eindgebruikers gerichte voorlichtingscampagnes opzetten om een veiliger individueel online-gedrag en digitale geletterdheid te bevorderen, het publiek bewuster te maken van potentiële cyberdreigingen, waaronder criminele onlineactiviteiten zoals phishing-aanvallen, botnets, financiële en bankfraude, gegevensfraude-incidenten, en door advies te geven over meervoudige authentificatie, patching, encryptie, anonimisering en gegevensbescherming.

(41) Enisa moet een centrale rol spelen bij de snellere bewustwording van de eindgebruikers over de beveiliging van toestellen en het veilig gebruik van diensten, en moet beveiliging door ontwerp en gegevensbescherming door ontwerp op Unieniveau bevorderen. Om dat doel na te streven moet Enisa zo veel mogelijk gebruikmaken van de beschikbare beste praktijken en ervaring, in het bijzonder van wetenschappelijke instellingen en onderzoekers op het gebied van IT-beveiliging.

(42) Om bedrijven die actief zijn in de cyberbeveiligingssector en de gebruikers van cyberbeveiligingsoplossingen te ondersteunen, moet Enisa een „marktwaarnemingspost" opzetten en onderhouden door regelmatig analyses uit te voeren en informatie te verspreiden over de voornaamste tendensen op de cyberbeveiligingsmarkt, zowel aan de vraag- als aan de aanbodzijde.

(43) Enisa moet de Unie steunen bij haar inspanningen om samen te werken met internationale organisaties, evenals binnen relevante internationale samenwerkingsverbanden op het gebied van cyberbeveiliging. Enisa moet, waar passend, bijdragen aan de samenwerking met organisaties zoals de OESO, de OVSE en de NAVO. Die samenwerking kan bestaan uit gezamenlijke cyberbeveiligingsoefeningen en een gezamenlijke gecoördineerde antwoord op incidenten. Die werkzaamheden moeten worden verricht met volledige inachtneming van de beginselen inclusiviteit, wederkerigheid en besluitvormingsautonomie van de Unie, zonder afbreuk te doen aan het specifieke karakter van het veiligheids- en defensiebeleid van enige lidstaat.

(44) Teneinde te waarborgen dat Enisa zijn doelstellingen volledig verwezenlijkt, moet het overleggen met de betrokken toezichthoudende autoriteiten van de Unie en met andere bevoegde autoriteiten in de Unie, de instellingen, organen en instanties van de Unie, met inbegrip van CERT-EU, EC3, het Europees Defensieagentschap (EDA), het Agentschap van het Europese wereldwijde satellietnavigatiesysteem (Europees GNSS-agentschap), het Orgaan van Europese regelgevende instanties voor elektronische communicatie (Berec), het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA), de Europese Centrale Bank (ECB), de Europese Bankautoriteit (EBA), het Europees Comité voor gegevensbescherming, het Agentschap voor de samenwerking tussen energieregulators (ACER), het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA) en alle andere agentschappen van de Unie die bij cyberbeveiliging betrokken zijn. Enisa moet overleggen met autoriteiten die zich bezighouden met gegevensbescherming teneinde kennis en beste praktijken uit te wisselen en advies te geven over cyberbeveiligingsaspecten die gevolgen kunnen hebben voor hun werkzaamheden. De vertegenwoordigers van de rechtshandhavings- en gegevensbeschermingsautoriteiten van de lidstaten en de Unie moeten recht hebben op vertegenwoordiging in de Enisa-adviesgroep. Wanneer Enisa contact opneemt met rechtshandhavingsautoriteiten betreffende netwerk- en informatiebeveiligingsaspecten die van invloed kunnen zijn op hun werkzaamheden, moet Enisa de bestaande informatiekanalen en gevestigde netwerken respecteren.

(45) Er kunnen partnerschappen worden gesloten met wetenschappelijke instellingen die onderzoek verrichten op de betreffende gebieden, en er moeten geëigende kanalen zijn voor de input van consumentenorganisaties en andere organisaties, dat in ogenschouw moet worden genomen.

(46) Enisa moet in zijn rol van het secretariaat van het CSIRT-netwerk de CSIRT's van de lidstaten en CERT-EU ondersteunen wat betreft de operationele samenwerking in verband met alle in Richtlijn (EU) 2016/1148 bedoelde relevante taken van het CSIRT-netwerk. In het geval van incidenten, aanvallen of storingen van netwerken of infrastructuurvoorzieningen die door de CSIRT's worden beheerd of beveiligd en waarbij ten minste twee CSIRT's betrokken zijn of kunnen zijn, moet Enisa tevens de samenwerking tussen de betrokken CSIRT's bevorderen, daarbij terdege rekening houdend met de standaardwerkwijzen van het CSIRT-netwerk.

(47) Om de paraatheid van de Unie wat betreft de reactie op incidenten te verhogen, moet Enisa regelmatig cyberbeveiligingsoefeningen op Unieniveau organiseren, en de lidstaten alsmede de instellingen, organen en instanties van de Unie op hun verzoek ondersteunen bij het organiseren van dergelijke oefeningen. Om de twee jaar moet grootschalige oefeningen worden georganiseerd, waarbij technische, operationele of strategische aspecten zijn betrokken. Daarnaast kan Enisa regelmatig minder grootschalige oefeningen met hetzelfde doel houden, om de paraatheid van de Unie wat betreft de reactie op incidenten verhogen.

(48) Verder moet Enisa expertise op het gebied van cyberbeveiligingscertificering ontwikkelen en in stand houden met het oog op de ondersteuning van het Uniebeleid op dat gebied. Enisa moet voortbouwen op bestaande beste praktijken en 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 Unieniveau (Europees kader voor cyberbeveiligingscertificering), om de transparantie van de cyberbeveiligingszekerheid van ICT-producten, -diensten en -processen, en daarmee het vertrouwen in en het concurrentievermogen van de digitale interne markt, te vergroten.

(49) 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 Enisa de samenwerking tussen belanghebbenden op Unieniveau bevorderen en hun inspanningen met betrekking tot de vaststelling en het gebruik van Europese en internationale normen voor risicobeheer en meetbare beveiliging van elektronische producten, systemen, netwerken en diensten die, samen met software, de netwerk- en informatiesystemen vormen.

(50) Enisa moet de lidstaten, fabrikanten en aanbieders van ICT-producten, -diensten, of -processen ertoe aansporen hun algemene veiligheidsnormen op te voeren, zodat alle internetgebruikers de nodige stappen kunnen ondernemen om voor hun eigen cyberbeveiliging te zorgen en daartoe worden aangezet. Wanneer ICT-producten, -diensten of -processen niet aan cyberbeveiligingsnormen voldoen, moeten fabrikanten en aanbieders van ICT-producten, -diensten, of -processen alle nodige updates leveren en deze terugnemen, intrekken of recyclen, waarbij importeurs en distributeurs ervoor moeten zorgen dat de ICT-producten, -diensten en -processen die zij in de Unie in de handel brengen, aan de toepasselijke voorschriften voldoen en geen risico vormen voor consumenten in de Unie.

(51) In samenwerking met de bevoegde autoriteiten dient Enisa informatie te kunnen verspreiden over het cyberbeveiligingsniveau van de ICT-producten, diensten en -processen die op de interne markt worden aangeboden, en dient het fabrikanten of aanbieders van ICT-producten, -diensten, of -processen waarschuwen en hen verplichten de beveiliging van hun ICT-producten, diensten en -processen, waaronder de cyberbeveiliging, te verbeteren.

(52) Enisa 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, organen en instanties van de Unie en in voorkomend geval de lidstaten, op hun verzoek, te adviseren over onderzoeksbehoeften op het gebied van cyberbeveiliging. Om te de onderzoeksbehoeften en -prioriteiten te bepalen, moet Enisa ook de relevante gebruikersgroepen raadplegen. Meer specifiek, zou samenwerking met de Europese Onderzoeksraad, het Europees Instituut voor innovatie en technologie, het Instituut voor veiligheidsstudies van de Europese Unie tot stand kunnen worden gebracht.

(53) Enisa moet regelmatig normalisatieorganisaties raadplegen, met name Europese normalisatieorganisaties, wanneer het de Europese regelingen voor cyberbeveiligingscertificering opstelt.

(54) Cyberdreigingen zijn een wereldwijd probleem. Er is dan ook behoefte aan nauwere internationale samenwerking om de cyberbeveiligingsnormen, met inbegrip van de omschrijving van gemeenschappelijke gedragsnormen, de vaststelling van gedragscodes, het gebruik van internationale normen en het delen van informatie, te verbeteren om snellere internationale samenwerking bij en een gemeenschappelijke wereldwijde aanpak van problemen op het gebied van netwerk- en informatiebeveiliging te bevorderen. Daartoe moet Enisa een verdergaande betrokkenheid van de Unie bij en samenwerking met derde landen en internationale organisaties ondersteunen door, voor zover van toepassing, de betrokken instellingen, organen en instanties van de Unie van de noodzakelijke expertise en analyses te voorzien.

(55) Enisa moet kunnen reageren op ad-hocverzoeken om advies en bijstand van de lidstaten en de instellingen, organen en instanties van de Unie over aangelegenheden die binnen het mandaat van Enisa vallen.

(56) Het is zinvol en aan te bevelen met betrekking tot het bestuur van Enisa bepaalde beginselen toe te passen uit 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 gedecentraliseerde agentschappen te stroomlijnen en hun prestaties te verbeteren. Ook de aanbevelingen in de gezamenlijke verklaring en de gemeenschappelijke aanpak moeten, waar passend, in de werkprogramma's, evaluaties, verslaglegging en administratieve werkwijzen van Enisa tot uiting komen.

(57) De raad van bestuur, die is samengesteld uit vertegenwoordigers van de lidstaten en de Commissie, moet de algemene richting van de werkzaamheden van Enisa vaststellen en ervoor zorgen 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 Enisa, de goedkeuring van het enig programmeringsdocument van Enisa, de vaststelling van zijn eigen reglement van orde, de benoeming van de uitvoerend directeur en de besluitvorming over de verlenging en beëindiging van de ambtstermijn van de uitvoerend directeur.

(58) Met het oog op van de goede en doeltreffende werking van Enisa moeten de Commissie en de lidstaten erop toezien dat personen die worden benoemd tot de raad van bestuur over passende professionele expertise en ervaring 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.

(59) Voor het goed functioneren van Enisa is het noodzakelijk dat de uitvoerend directeur wordt benoemd op grond van zowel verdiensten en aantoonbare administratieve en leidinggevende vaardigheden, als bekwaamheid en ervaring die relevant is voor cyberbeveiliging. De uitvoerend directeur dient zijn taken op volledig onafhankelijke wijze uit te voeren. De uitvoerend directeur moet een voorstel voor het jaarlijks werkprogramma van Enisa voorbereiden, na voorafgaand overleg met de Commissie, en alle nodige stappen ondernemen om te zorgen voor de goede uitvoering van dat werkprogramma. Hij moet een jaarverslag opstellen over onder andere de uitvoering van het jaarlijkse werkprogramma van Enisa, dat moet worden voorgelegd aan de raad van bestuur, een ontwerpverklaring van de geraamde inkomsten en uitgaven van Enisa opstellen en de begroting uitvoeren. De uitvoerend directeur moet voorts over de mogelijkheid beschikken om ad-hocwerkgroepen op te richten voor specifieke aangelegenheden, met name van wetenschappelijke, technische, juridische of sociaaleconomische aard. Met name voor het opstellen van een specifieke potentiële Europese regeling voor cyberbeveiligingscertificering (potentiële regeling) wordt het nodig geacht een ad-hocwerkgroep in te stellen. De uitvoerend directeur moet erop toezien dat de leden van de ad-hocwerkgroepen overeenkomstig de hoogste normen inzake expertise worden

geselecteerd, waarbij gestreefd wordt naar een evenwicht tussen mannen en vrouwen en, afhankelijk van de specifieke aangelegenheid, een passend evenwicht tussen de overheidsinstanties van de lidstaten, de instellingen, organen en instanties van de Unie, de particuliere sector, waaronder het bedrijfsleven, de gebruikers en wetenschappelijke deskundigen op het gebied van netwerk- en informatiebeveiliging.

(60) 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 de besluiten van de raad van bestuur.

(61) Enisa moet beschikken over een Enisa-adviesgroep als adviserend orgaan teneinde regelmatig overleg met de particuliere sector, consumentenorganisaties en andere relevante belanghebbenden te waarborgen. De op voorstel van de uitvoerend directeur door de raad van bestuur opgerichte Enisa-adviesgroep moet zich richten op voor de belanghebbenden relevante vraagstukken en deze onder de aandacht van Enisa brengen. De Enisa-adviesgroep wordt in het bijzonder geraadpleegd met betrekking tot het ontwerp van het jaarlijks werkprogramma van Enisa. De samenstelling van de Enisa-adviesgroep en de aan deze groep toegewezen taken, moeten waarborgen dat de belanghebbenden voldoende worden vertegenwoordigd in de werkzaamheden van Enisa.

(62) De Groep van belanghebbenden bij cyberbeveiligingscertificering moet worden opgericht om Enisa en de Commissie te helpen het raadplegen van de betrokken belanghebbenden te vergemakkelijken. De Groep van belanghebbenden bij cyberbeveiligingscertificering moet worden samengesteld uit leden die op evenwichtige wijze de sector vertegenwoordigen, zowel wat vraag als aanbod van ICT-producten en -diensten betreft, waaronder met name kleine en middelgrote ondernemingen, digitaledienstverleners, Europese en internationale normalisatieorganisaties, nationale accreditatie-instanties, gegevensbeschermingsautoriteiten en conformiteitsbeoordelingsinstanties overeenkomstig Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad ([16]), de wetenschap alsmede consumentenorganisaties.

(63) Enisa moet beschikken over regels ter voorkoming en beheersing van belangenconflicten. Enisa moet voorts de toepasselijke in Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad ([17]) vastgelegde Unievoorschriften inzake toegang van het publiek tot documenten toepassen, zoals vervat. Persoonsgegevens moeten door Enisa worden verwerkt overeenkomstig Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([18]). Enisa dient de bepalingen na te leven die van toepassing zijn op de instellingen, organen en instanties van de Unie alsmede de nationale wetgeving inzake de behandeling van informatie, in het bijzonder gevoelige niet-gerubriceerde informatie en gerubriceerde informatie van de Europese Unie (EUCI).

(64) Om de volledige autonomie en onafhankelijkheid van Enisa te garanderen en Enisa in staat te stellen bijkomende taken te verrichten, waaronder onvoorziene noodmaatregelen, dient aan Enisa een toereikende eigen begroting te worden toegekend die hoofdzakelijk moet worden gefinancierd uit een bijdrage van de Unie en bijdragen van derde landen die deelnemen aan de werkzaamheden van Enisa. Een passende begroting is cruciaal om te waarborgen dat Enisa over voldoende capaciteit beschikt om al zijn steeds omvangrijkere taken te kunnen vervullen en zijn doelstellingen te verwezenlijken. Het merendeel van het personeel van Enisa moet rechtstreeks worden ingezet voor de operationele uitvoering van het mandaat van Enisa. De lidstaat van vestiging of enige andere lidstaat mag een vrijwillige bijdrage leveren aan de inkomsten van Enisa. De Uniebegrotingsprocedure blijft van toepassing op eventuele subsidies die ten laste van de algemene begroting van de Unie komen. Voorts controleert de Rekenkamer de rekeningen van Enisa teneinde transparantie en verantwoording zeker te stellen.

(65) Cyberbeveiligingscertificering is belangrijk om het vertrouwen in en de beveiliging van ICT-producten, -diensten en -processen te vergroten. 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, diensten en processen een bepaald cyberbeveiligingsniveau bieden. Verbonden en geautomatiseerde auto's, elektronische medische hulpmiddelen, besturingssystemen voor industriële automatisering en slimme netwerken zijn slechts enkele voorbeelden van sectoren waarin certificering reeds op grote schaal wordt gebruikt of naar verwachting in de toekomst zal worden gebruikt. De door Richtlijn (EU) 2016/1148 gereguleerde sectoren, zijn tevens sectoren waarin cyberbeveiligingscertificering van cruciaal belang is.

([16]) Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

([17]) 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).

([18]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295, 21.11.2018, blz. 39).

(66) 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, -diensten en -processen 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 gebrek aan interoperabele oplossingen (technische normen), praktijken en Uniebrede certificeringsmechanismen een tekortkoming van de eengemaakte markt op het gebied van cyberbeveiliging. Dit maakt het voor Europese ondernemingen moeilijk om op nationaal, Unie- en mondiaal niveau te concurreren. Burgers en bedrijven hebben hierdoor slechts toegang tot een beperkte keuze aan levensvatbare en bruikbare cyberbeveiligingstechnologieën. Verder heeft de Commissie in de mededeling van 2017 inzake de tussentijdse evaluatie van de uitvoering van de strategie voor de digitale interne markt — Een connectieve digitale interne markt voor iedereen, 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 interne markt kan worden aangepakt.

(67) Momenteel wordt de cyberbeveiligingscertificering van ICT-producten, -diensten en -processen 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 dat kader wordt een certificaat dat is afgegeven door een nationale cyberbeveiligingscertificeringsautoriteit in principe niet erkend in andere lidstaten. Bijgevolg moeten bedrijven hun ICT-producten, -diensten en -processen wellicht laten certificeren in de verschillende lidstaten waarin zij actief zijn, bijvoorbeeld met het oog op deelname aan nationale aanbestedingsprocedures, waardoor hun kosten oplopen. Er worden weliswaar nieuwe regelingen opgezet, maar er schijnt geen samenhangende en alomvattende benadering te zijn ten aanzien van horizontale cyberbeveiligingsvraagstukken, bijvoorbeeld op het gebied van het internet der dingen. Bestaande regelingen vertonen aanzienlijke tekortkomingen en verschillen wat betreft productdekking, zekerheidsniveaus, materiële criteria en daadwerkelijk gebruik, hetgeen een belemmering vormt voor wederzijdse-erkenningsmechanismen binnen de Unie.

(68) Er zijn enige inspanningen geleverd om te zorgen voor wederzijdse erkenning van certificaten in de Unie. Maar die 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). Dat is weliswaar het belangrijkste model voor samenwerking en wederzijdse erkenning op het gebied van beveiligingscertificering, maar SOG-IS omvat slechts enkele lidstaten. De doeltreffendheid van de overeenkomst inzake wederzijdse erkenning van SOG-IS is daardoor vanuit het oogpunt van de interne markt beperkt.

(69) Het is daarom noodzakelijk een gemeenschappelijke aanpak vast te stellen en een Europees kader voor cyberbeveiligingscertificering op te zetten waarin de voornaamste horizontale voorschriften voor te ontwikkelen Europese cyberbeveiligingscertificeringsregelingen worden vastgesteld, en dat het mogelijk maakt dat Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen voor ICT-producten, -diensten of -processen in alle lidstaten worden erkend en gebruikt. Daarbij is het essentieel om voort te bouwen op zowel bestaande nationale en internationale regelingen als stelsels voor wederzijdse erkenning, in het bijzonder SOG-IS, en een vlotte overgang mogelijk te maken van bestaande regelingen binnen die stelsels naar regelingen binnen het nieuwe Europese kader voor cyberbeveiligingscertificering. Het Europees kader voor cyberbeveiligingscertificering moet een tweeledig doel hebben. Enerzijds moet het bijdragen aan een groter vertrouwen in ICT-producten, -diensten en -processen die op grond van Europese regelingen voor cyberbeveiligingscertificering zijn gecertificeerd. Anderzijds moet het helpen voorkomen dat er meerdere tegenstrijdige of elkaar overlappende nationale cyberbeveiligingscertificeringsregelingen bestaan, en zodoende zorgen voor lagere kosten voor ondernemingen die actief zijn op de digitale eengemaakte markt. De Europese cyberbeveiligingscertificeringsregelingen moeten niet-discriminerend en gebaseerd zijn op Europese of internationale normen, tenzij dergelijke normen met het oog op de verwezenlijking van de desbetreffende legitieme doelstellingen van de Unie niet doeltreffend of niet geschikt zijn.

(70) Het Europees kader voor cyberbeveiligingscertificering moet op uniforme wijze in alle lidstaten worden opgesteld om het „certificeringsshoppen" vanwege verschillende stringentieniveaus in de verschillende lidstaten tegen te gaan.

(71) Europese cybercertificeringsregelingen moeten voortbouwen op wat er al op internationaal en nationaal niveau bestaat en zo nodig op technische specificaties van overlegfora en consortia; er moeten lessen worden getrokken uit de huidige sterke punten en de zwakke punten moeten worden beoordeeld en gecorrigeerd.

(72) Aangezien het bedrijfsleven behoefte heeft aan flexibele cyberbeveiligingsoplossingen om cyberdreigingen voor te blijven, moet alle certificeringsregelingen zo worden ontwerpen dat het risico dat ze snel achterhaald zijn, wordt vermeden.

(73) De Commissie dient de bevoegdheid te krijgen om Europese regelingen voor cyberbeveiligingscertificering met betrekking tot bepaalde groepen van ICT-producten, -diensten en -processen vast te stellen. De uitvoering van en het toezicht op die regelingen moeten worden verricht door de nationale cyberbeveiligingscertificeringsautoriteiten en de in het kader van die regelingen afgegeven certificaten moeten in de hele Unie geldig zijn en worden erkend. Certificeringsregelingen die door het bedrijfsleven of door andere particuliere organisaties worden toegepast, moeten buiten het toepassingsgebied van deze verordening vallen. De organisaties die dergelijke regelingen toepassen, moeten echter kunnen voorstellen dat de Commissie dergelijke regelingen in overweging nemen als basis voor de verbetering daarvan in de vorm van een Europese cyberbeveiligingscertificeringsregeling.

(74) De bepalingen van deze verordening moeten Uniewetgeving waarbij specifieke regels voor de certificering van ICT-producten, -diensten en -processen zijn vastgesteld, onverlet laten. Met name omvat Verordening (EU) 2016/679 bepalingen betreffende de vaststelling van certificeringsmechanismen en van gegevensbeschermingszegels en -merktekens, om de naleving van die verordening bij verwerkingen door verwerkingsverantwoordelijken en verwerkers aan te tonen. Met behulp van dergelijke certificeringsmechanismen en gegevensbeschermingszegels en -merktekens dienen betrokkenen snel te kunnen beoordelen wat het beschermingsniveau van de relevante ICT-producten en -diensten is. Deze verordening doet geen afbreuk aan de certificering van gegevensverwerkingen overeenkomstig Verordening (EU) 2016/649, ook niet als dergelijke verwerkingen zijn geïntegreerd in ICT-producten, -diensten en -processen.

(75) Europese regelingen voor cyberbeveiligingscertificering moeten tot doel hebben te waarborgen dat ICT-producten, -diensten en -processen die door middel van een dergelijke regeling zijn gecertificeerd, aan gespecificeerde voorschriften voldoen met als doel de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of verzonden gegevens of de daaraan gerelateerde diensten die via die producten, diensten en processen, worden aangeboden of toegankelijk zijn, gedurende hun levenscyclus te beschermen. Het is niet mogelijk om in deze verordening de cyberbeveiligingsvoorschriften voor alle ICT-producten, -diensten en -processen in detail op te nemen. ICT-producten, -diensten en -processen en de daarmee verband houdende behoeften inzake cyberbeveiliging zijn zodanig uiteenlopend dat het zeer moeilijk is te voorzien in algemene, in alle omstandigheden geldende cyberbeveiligingsvoorschriften. Met het oog op certificering is daarom een breed en algemeen begrip van cyberbeveiliging noodzakelijk, dat moet worden aangevuld met een reeks specifieke doelstellingen inzake cyberbeveiliging waarmee rekening moet worden gehouden bij het opzetten van Europese regelingen voor cyberbeveiligingscertificering. De regelingen waarmee dergelijke doelstellingen dienen te worden verwezenlijkt in specifieke ICT-producten, -diensten en -processen 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.

(76) De in Europese cyberbeveiligingscertificeringsregelingen te gebruiken technische specificaties moeten de in bijlage II bij Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad ([19]) vastgestelde voorschriften in acht nemen. Enige afwijkingen van die voorschriften kunnen evenwel in naar behoren gemotiveerde gevallen noodzakelijk worden geacht wanneer die technische specificaties moeten worden gebruikt in een Europese cyberbeveiligingscertificeringsregeling waarin zekerheidsniveau „hoog" staat aangegeven. De redenen voor dergelijke afwijkingen moeten openbaar worden gemaakt.

(77) Een conformiteitsbeoordeling is een procedure waarbij wordt geëvalueerd of aan gespecificeerde voorschriften met betrekking tot een ICT-product, -dienst of -proces is voldaan. Die procedure wordt verricht door een onafhankelijke derde partij die niet de fabrikant of de aanbieder van de geëvalueerde ICT-producten, -diensten of -processen is. Een Europese cyberbeveiligingscertificaat dient te worden afgegeven na een succesvolle evaluatie van een ICT-product, -dienst of -proces. Een Europees cyberbeveiligingscertificaat moet worden gezien als een bevestiging dat de evaluatie correct is uitgevoerd. Afhankelijk van het zekerheidsniveau moet in de Europese cyberbeveiligingscertificeringsregeling worden aangegeven of het Europees cyberbeveiligingscertificaat dient te worden afgegeven door een particuliere of een openbare instantie. Conformiteitsbeoordeling en certificering bieden geen garantie dat gecertificeerde ICT-producten, -diensten en -processen cyberbeveiligd zijn. Zij behelzen veeleer procedures en een technische methoden om te bevestigen dat ICT-producten, -diensten en -processen zijn getest en dat zij voldoen aan bepaalde cyberbeveiligingsvoorschriften die elders, bijvoorbeeld in technische normen, zijn vastgesteld.

(78) De keuze van de gebruikers van Europese cyberbeveiligingscertificaten voor de passende certificering en de bijbehorende beveiligingsvoorschriften moet worden gebaseerd op een analyse van de met het gebruik van de ICT-producten, -diensten of -processen verbonden risico's. Het zekerheidsniveau moet daarom in verhouding staan tot het niveau van het risico dat verbonden is aan het beoogde gebruik van een ICT-product, -dienst of -proces.

([19]) Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

(79) In Europese regelingen voor cyberbeveiligingscertificering zou kunnen worden bepaald dat een conformiteitsbeoordeling wordt uitgevoerd onder de uitsluitende verantwoordelijkheid van de fabrikant of aanbieder van ICT-producten, -diensten of -processen („conformiteitszelfbeoordeling"). In dergelijke gevallen moet het volstaan dat de fabrikant of de aanbieder van ICT-producten, -diensten of -processen zelf alle inspecties uitvoert om te zorgen dat de ICT-producten, -diensten of -processen in overeenstemming zijn met de Europese cyberbeveiligingscertificeringsregeling. De conformiteitszelfbeoordeling moet geschikt worden geacht voor ICT-producten, -diensten en -processen met een geringe complexiteit (eenvoudig ontwerp- en productiemechanismen) die een laag risico voor het openbaar belang opleveren. Voorts dient conformiteitszelfbeoordeling ten aanzien van ICT-producten, -diensten of -processen alleen te worden toegestaan wanneer deze zekerheidsniveau „basis" hebben.

(80) Europese regelingen voor cyberbeveiligingscertificering zouden de mogelijkheid kunnen bieden van zowel conformiteitszelfbeoordeling als certificering van ICT-producten, -diensten of -processen. In een dergelijk geval moet de regeling de consumenten of andere gebruikers duidelijke en begrijpelijke middelen aanreiken waarmee zij een onderscheid kunnen maken tussen ICT-producten, -diensten of -processen ten aanzien waarvan de fabrikant of aanbieder verantwoordelijk is voor de beoordeling en ICT-producten, -diensten of -processen die door een derde partij zijn gecertificeerd.

(81) De fabrikant of aanbieder van ICT-producten, -diensten of -processen die een conformiteitszelfbeoordeling uitvoert moet, als onderdeel van de conformiteitsbeoordelingsprocedure, de EU-conformiteitsverklaring kunnen verstrekken en ondertekenen. Een EU-conformiteitsverklaring is een document waarin staat dat een specifiek ICT-product, -dienst of -proces voldoet aan de voorschriften van de Europese cyberbeveiligingscertificeringsregeling. Door de EU-conformiteitsverklaring te verstrekken en ondertekenen verklaart de fabrikant of de aanbieder van ICT-producten, -diensten of -processen zich verantwoordelijk voor de conformiteit van het ICT-product, -dienst of -proces met de wettelijke voorschriften van de Europese cyberbeveiligingscertificeringsregeling. Van de EU-conformiteitsverklaring moet een exemplaar bij de nationale cyberbeveiligingscertificeringsautoriteit en bij Enisa worden ingediend.

(82) Fabrikanten of aanbieders van ICT-producten, -diensten of -processen moeten de EU-conformiteitsverklaring en de technische documentatie van alle andere relevante informatie met betrekking tot de conformiteit van de ICT-producten, -diensten of -processen met een Europese cyberbeveiligingscertificeringsregeling ter beschikking van de bevoegde nationale cyberbeveiligingscertificeringsautoriteit stellen, en wel gedurende een in de betrokken Europese cyberbeveiligingscertificeringsregeling bepaalde periode. In de technische documentatie moeten de krachtens de regeling toepasselijke vereisten worden vermeld en moet, voor zover relevant voor de conformiteitszelfbeoordeling, het ontwerp, de fabricage en de werking van het ICT-product, -dienst of -proces worden bestreken. De technische documentatie moet zodanig worden opgesteld dat kan worden beoordeeld of een ICT-product, -dienst of -proces voldoet aan de krachtens die regeling toepasselijke vereisten.

(83) De governance van het Europees kader voor cyberbeveiligingscertificering houdt rekening met de betrokkenheid van de lidstaten alsmede de passende betrokkenheid van belanghebbenden en legt de rol van de Commissie vast gedurende het plannen, voorstellen, aanvragen, voorbereiden, goedkeuren en evalueren van Europese regelingen voor cyberbeveiligingscertificering.

(84) De Commissie moet na open en breed overleg met de steun van de Europese Groep voor cyberbeveiligingscertificering (de „EGC") en de Groep van belanghebbenden bij cyberbeveiligingscertificering een voortschrijdend werkprogramma van de Unie voor Europese regelingen voor cyberbeveiligingscertificering opstellen en bekendmaken in de vorm van een niet-bindend instrument. Het voortschrijdend werkprogramma van de Unie dient een strategisch document te zijn aan de hand waarvan met name de sector, de nationale autoriteiten en de normalisatieorganisaties zich kunnen voorbereiden op toekomstige Europese regelingen voor cyberbeveiligingscertificering. Het voortschrijdend werkprogramma van de Unie moet een meerjarig overzicht van de verzoeken om potentiële regelingen bevatten die de Commissie ter voorbereiding bij Enisa wil indienen, op specifieke gronden. De Commissie moet met het voortschrijdend werkprogramma van de Unie rekening houden wanneer zij haar voortschrijdend plan voor ICT-normalisatie en normalisatieverzoeken aan Europese normalisatieorganisaties opstelt. In het licht van de snelle invoering en absorptie van nieuwe technologieën, het ontstaan van voorheen onbekende cyberbeveiligingsrisico's en ontwikkelingen in wetgeving en de markt, moet de Commissie of de EGC het recht hebben om Enisa te verzoeken potentiële regelingen op te stellen die niet in het voortschrijdend werkprogramma van de Unie zijn opgenomen. In dergelijke gevallen moeten de Commissie en de EGC ook de noodzaak van een dergelijk verzoek beoordelen, rekening houdend met de algemene doelstellingen van deze verordening en noodzaak tot waarborging van de continuïteit van de planning en het gebruik van de middelen van Enisa.

Enisa moet, naar aanleiding van een dergelijk verzoek, onverwijld potentiële regelingen opstellen voor specifieke ICT-producten, -diensten en -processen. De Commissie moet de positieve en negatieve gevolgen van haar verzoek voor de betrokken specifieke markt evalueren, met name wat betreft kleine en middelgrote ondernemingen, innovatie, belemmeringen om tot die markt toe te treden en kosten voor eindgebruikers. De Commissie moet de bevoegdheid krijgen om vervolgens, op basis van de door Enisa voorgestelde potentiële regeling, de Europese cyberbeveiligingscertificeringsregeling bij uitvoeringshandeling vast te stellen. Rekening houdend met het in deze verordening bepaalde algemene doel en de beveiligingsdoelstellingen, moet in door de Commissie vastgestelde Europese cyberbeveiligingscertificeringsregelingen een minimumreeks elementen worden gespecificeerd wat betreft onderwerp, toepassingsgebied en werking van de afzonderlijke regeling. Tot die elementen moeten onder meer het toepassingsgebied en het voorwerp van de cyberbeveiligingscertificering behoren, met inbegrip van de betrokken categorieën ICT-producten, -diensten en -processen, de gedetailleerde specificatie van de cyberbeveiligingsvoorschriften, bijvoorbeeld door verwijzing naar normen of technische specificaties, de specifieke evaluatiecriteria en -methoden evenals het beoogde zekerheidsniveau („basis", „substantieel" of „hoog") en de evaluatieniveaus, indien van toepassing. Enisa moet een verzoek van de EGC kunnen weigeren. Dergelijke beslissingen moeten door de raad van bestuur worden genomen en moeten naar behoren worden gemotiveerd.

(85) Enisa moet een website in stand houden met informatie over en bekendmaking van Europese cyberbeveiligingscertificeringsregelingen, waaronder de verzoeken voor de opstelling van een potentiële regeling en voor de feedback die wordt ontvangen tijdens het raadplegingsproces dat Enisa in de voorbereidingsfase uitvoert. De website moet ook informatie verstrekken over Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen die krachtens deze verordening worden afgegeven, waaronder informatie over intrekking en verval van dergelijke Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen. Tevens moet de website vermelden welke nationale cyberbeveiligingscertificeringsregelingen zijn vervangen door een Europese cyberbeveiligingscertificeringsregeling.

(86) Het zekerheidsniveau van een Europese certificeringsregeling is een basis voor vertrouwen dat een ICT-product, -dienst of -proces voldoet aan de beveiligingsvoorschriften van een specifieke Europese cyberbeveiligingscertificeringsregeling. Teneinde de samenhang van het Europees cyberbeveiligingscertificeringskader te waarborgen moeten in een Europese cybercertificeringsregeling zekerheidsniveaus kunnen worden aangegeven voor uit hoofde van die regeling afgegeven Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen. In elk Europees cyberbeveiligingscertificaat zou kunnen worden verwezen naar de zekerheidsniveaus „basis", „substantieel" of „hoog", terwijl in de EU-conformiteitsverklaring alleen melding zou kunnen worden gemaakt van zekerheidsniveau „basis". De zekerheidsniveaus zouden de overeenkomstige grondigheid en diepgang van de evaluatie van het ICT-product, de ICT-dienst of het ICT-proces bepalen, en zouden worden gekenmerkt door verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles, waarvan het doel is om incidenten te beperken of voorkomen. Elk zekerheidsniveau dient in overeenstemming te zijn met de diverse sectorale domeinen waar certificering wordt toegepast.

(87) In een Europese cyberbeveiligingscertificeringsregeling zouden verscheidene evaluatieniveaus kunnen worden vermeld, afhankelijk van de vraag hoe strikt en diepgaand de gebruikte evaluatiemethodologie is. Evaluatieniveaus moeten overeenkomen met één van de zekerheidsniveaus en moeten gepaard gaan met een passende combinatie van zekerheidscomponenten. Voor alle zekerheidsniveaus moeten ICT-producten, -diensten of -processen een aantal in de regeling gespecificeerde beveiligde functies bevatten zoals onder meer: een standaardconfiguratie, een ondertekende code, beveiligde actualisering en exploitmitigatie, en volledige bescherming van het stack- of heapgeheugen. Die functies moeten worden ontwikkeld en onderhouden met op beveiliging gerichte benaderingen inzake ontwikkeling en de bijbehorende hulpmiddelen waardoor wordt gewaarborgd dat er doeltreffende software- en hardwaremechanismen op betrouwbare wijze in worden verwerkt.

(88) Voor het zekerheidsniveau „basis" moet de evaluatie worden geleid door ten minste de volgende zekerheidscomponenten: de evaluatie moet ten minste een beoordeling inhouden van de technische documentaties van het ICT-product, de ICT-dienst of het ICT-proces door de conformiteitsbeoordelingsinstantie. Indien de certificering ICT-processen omvat, moet de technische evaluatie ook betrekking hebben op het proces dat wordt gebruikt voor het ontwerpen, ontwikkelen en in stand houden van een ICT-product of -dienst. Indien een Europese cyberbeveiligingscertificeringsregeling voorziet in een conformiteitszelfbeoordeling, moet het voldoende zijn als de fabrikant of aanbieder van ICT-producten, -diensten of -processen zelf heeft beoordeeld of de ICT-producten, -diensten of -processen voldoen aan de certificeringsregeling.

(89) Voor zekerheidsniveau „substantieel" moet de evaluatie, in aanvulling op de vereisten voor het zekerheidsniveau „basis", worden geleid door ten minste de verificatie van de conformiteit van de beveiligingsfuncties van het ICT-product, de ICT-dienst of het ICT-proces met de technische documentatie ervan omvatten.

(90) Voor zekerheidsniveau „hoog" moet de evaluatie, in aanvulling op de vereisten voor zekerheidsniveau „substantieel", worden geleid door ten minste een efficiëntietest waarbij wordt beoordeeld of de beveiligingsfuncties van een ICT-product, -dienst of -proces bestand zijn tegen mensen die complexe cyberaanvallen uitvoeren en over aanzienlijke vaardigheden en middelen beschikken.

(91) Het gebruik van Europese cyberbeveiligingscertificering en EU-conformiteitsverklaringen moet vrijwillig blijven, tenzij anders is bepaald in Unierecht, of in het in overeenstemming met het Unierecht vastgestelde recht van de lidstaten. Bij ontstentenis van geharmoniseerd Unierecht kunnen de lidstaten nationale technische voorschriften vaststellen die voorzien in verplichte certificering uit hoofde van een Europese cyberbeveiligingscertificeringsregeling overeenkomstig Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad ([20]). De lidstaten kunnen tevens gebruikmaken van de Europese cyberbeveiligingscertificering in het kader van overheidsopdrachten en Richtlijn 2014/24/EU van het Europees Parlement en de Raad ([21]).

(92) Op sommige gebieden kan het in de toekomst nodig zijn om specifieke cyberbeveiligingsvoorschriften op te leggen en de certificering daarvan verplicht te maken voor bepaalde ICT-producten, -diensten of -processen teneinde het cyberbeveiligingsniveau in de Unie te verbeteren. De Commissie moet toezien op de vastgestelde Europese cyberbeveiligingscertificeringsregelingen en de beschikbaarheid van beveiligde ICT-producten, -diensten en -processen in de interne markt en regelmatig het niveau van de door de fabrikanten of aanbieders van ICT-producten, -diensten en -processen in de Unie gebruikte certificeringsregelingen beoordelen. De efficiëntie van de Europese cyberbeveiligingscertificeringsregelingen en de vraag of specifieke regelingen verplicht moeten worden gesteld, moet worden beoordeeld in het licht van de Uniewetgeving inzake cyberbeveiliging, met name Richtlijn (EU) 2016/1148, rekening houdend met de beveiliging van de netwerk- en informatiesystemen die door aanbieders van essentiële diensten worden gebruikt.

(93) Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen moeten eindgebruikers helpen geïnformeerde keuzes te maken. Daarom moeten ICT-producten, -diensten en -processen die zijn gecertificeerd of waarvoor een EU-conformiteitsverklaring is afgegeven, vergezeld gaan van gestructureerde informatie die aan het verwachte technische niveau van de beoogde eindgebruiker is aangepast. Alle dergelijke informatie moet online, en waar passend in tastbare vorm, beschikbaar zijn. De eindgebruiker moet toegang hebben tot informatie met betrekking tot het referentienummer van de certificeringsregeling, het zekerheidsniveau, de omschrijving van de cyberbeveiligingsrisico's die gepaard gaan met het ICT-product, de ICT-dienst of het ICT-proces, en de autoriteit of instantie van afgifte, of moet een kopie van het Europees cyberbeveiligingscertificaat kunnen verkrijgen. Daarnaast moet de eindgebruiker worden geïnformeerd over het cyberbeveiligingsondersteuningsbeleid namelijk hoe lang de eindgebruiker mag verwachten cyberbeveiligingsupdates of -patches te krijgen van de fabrikant of aanbieder van ICT-producten, -diensten of -processen. Waar van toepassing dienen richtsnoeren te worden verstrekt over maatregelen of instellingen die de eindgebruiker kan toepassen om de cyberbeveiliging van het ICT-product, de ICT-dienst of het ICT-proces in stand te houden of te verbeteren, alsmede de contactgegevens van een centraal contactpunt om cyberaanvallen te melden of in geval van cyberaanvallen hulp te ontvangen (naast automatische melding). Die informatie moet regelmatig worden geactualiseerd en op een website met informatie over Europese cyberbeveiligingscertificeringsregelingen beschikbaar worden gesteld.

(94) Om de doelstellingen van deze verordening te verwezenlijken en de versnippering van de interne markt te voorkomen, dient de geldigheid van nationale cyberbeveiligingscertificeringsregelingen of -procedures voor ICT-producten, -diensten of -processen die onder een Europese cyberbeveiligingscertificeringsregelingen vallen, te vervallen vanaf een door de Commissie bij de uitvoeringshandeling vastgestelde datum. Bovendien dienen de lidstaten geen nieuwe nationale cyberbeveiligingscertificeringsregelingen in te voeren voor ICT-producten, -diensten of -processen die reeds onder een bestaande Europese regeling voor cyberbeveiligingscertificering vallen. De lidstaten dient echter niet belet te worden nationale cyberbeveiligingscertificeringsregelingen met het oog op de nationale veiligheid vast te stellen of te handhaven. De lidstaten dienen de Commissie en de EGC in te lichten over elk voornemen om nieuwe nationale cyberbeveiligingscertificeringsregelingen op te stellen. De Commissie en de EGC moeten de gevolgen van de nieuwe nationale cyberbeveiligingscertificeringsregelingen voor de goede werking van de interne markt evalueren, mede in het licht van enig strategische belang om in de plaats daarvan om een Europese cyberbeveiligingscertificeringsregeling te verzoeken.

(95) Met Europese cyberbeveiligingscertificeringsregelingen wordt beoogd bij te dragen aan de harmonisatie van cyberbeveiligingspraktijken in de Unie. Zij dienen bij te dragen tot een betere cyberbeveiliging binnen de Unie. Bij het ontwerp van de Europese cyberbeveiligingscertificeringsregelingen moet de ontwikkeling van innovaties op het gebied van cyberbeveiliging in aanmerking worden genomen en mogelijk zijn.

([20]) Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij (PB L 241 van 17.9.2015, blz. 1).

([21]) Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

(96) Bij Europese cyberbeveiligingscertificeringsregelingen dient rekening gehouden te worden met bestaande software- en hardwareontwikkelingsmethoden en in het bijzonder met de gevolgen van veelvuldige updates van software of firmware voor afzonderlijke Europese cyberbeveiligingscertificaten. In Europese cyberbeveiligingscertificeringsregelingen moeten de voorwaarden zijn gespecificeerd waaronder een update kan vereisen dat een ICT-product, -dienst of -proces opnieuw wordt gecertificeerd of dat de geldigheid van dat Europees cyberbeveiligingscertificaat wordt beperkt, rekening houdend met mogelijke negatieve gevolgen van de update voor de naleving van de beveiligingsvoorschriften van dat certificaat.

(97) Zodra een Europese cyberbeveiligingscertificeringsregelingen is vastgesteld, moeten fabrikanten of aanbieders van ICT-producten, -diensten of -processen bij een conformiteitsbeoordelingsinstantie van hun keuze, waar dan ook in de Unie, een aanvraag indienen voor de certificering van hun ICT-producten of -diensten. Conformiteitsbeoordelingsinstanties moeten door een nationale accreditatie-instantie worden geaccrediteerd indien zij aan bepaalde, in deze verordening vastgestelde specifieke vereisten voldoen. De accreditatie moet worden afgegeven voor een maximumperiode van vijf jaar en moet onder dezelfde voorwaarden kunnen worden verlengd, mits de conformiteitsbeoordelingsinstantie nog steeds aan de vereisten voldoet. Nationale 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 de conformiteitsbeoordelingsinstantie inbreuk maakt op deze verordening.

(98) Verwijzingen in nationale wetgeving naar nationale normen die niet langer gelden door de inwerkingtreding van een Europese cyberbeveiligingscertificeringsregelingen, kunnen een bron van verwarring zijn. Daarom moeten de lidstaten de vaststelling van een Europese cyberbeveiligingscertificeringsregelingen in hun nationale wetgeving weerspiegelen.

(99) Om binnen de hele Unie gelijkwaardige normen te bereiken teneinde wederzijdse erkenning te vergemakkelijken en de algemene acceptatie van Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen te bevorderen, moeten de nationale cyberbeveiligingscertificeringsautoriteiten een collegialetoetsingssysteem inrichten. Collegiale toetsing moet procedures omvatten voor het toezicht op de conformiteit van ICT-producten, -diensten en -processen van Europese cyberbeveiligingscertificaten, op de verplichtingen van fabrikanten en aanbieders van ICT-producten, -diensten en -processen die aan zelfbeoordeling doen, op conformiteitsbeoordelingsinstanties, evenals op de relevantie van de expertise van het personeel van de organen die certificaten voor zekerheidsniveau „hoog” afgeven. De Commissie moet, door middel van een uitvoeringshandeling, ten minste een vijfjarenplan voor collegiale toetsingen kunnen opstellen, alsmede ook criteria en methoden vastleggen voor de werking van het systeem van collegiale toetsing.

(100) Sommige Europese cyberbeveiligingscertificeringsregelingen kunnen, onverminderd het algemene systeem van collegiale toetsing dat voor alle nationale cyberbeveiligingscertificeringsautoriteiten binnen het Europees cyberbeveiligingscertificeringskader moet worden ingericht, een collegialetoetsingsmechanisme opzetten voor de instanties die onder dergelijke regelingen Europese cyberbeveiligingscertificaten voor ICT-producten, -diensten en -processen met zekerheidsniveau „hoog” afgeven. De EGC moet de uitvoering van dergelijke collegialetoetsingsmechanismen steunen. Bij de collegiale toetsingen dient in het bijzonder te worden beoordeeld of de betrokken instanties hun taken op geharmoniseerde wijze uitvoeren, en kunnen beroepsmechanismen omvatten. De resultaten van de collegiale toetsing moeten openbaar worden gemaakt. De betrokken instanties kunnen passende maatregelen nemen om hun praktijken en expertise aan te passen.

(101) De lidstaten moeten één of meer nationale cyberbeveiligingscertificeringsautoriteiten aanwijzen om toe te zien op de naleving van de uit deze verordening voortvloeiende verplichtingen. Een nationale cyberbeveiligingscertificeringsautoriteit kan een bestaande of een nieuwe autoriteit zijn. Een lidstaat moet, na overeenstemming met een andere lidstaat, tevens één of meer nationale cyberbeveiligingscertificeringsautoriteiten op het grondgebied van die andere lidstaat kunnen aanwijzen.

(102) Nationale cyberbeveiligingscertificeringsautoriteiten moeten in het bijzonder de verplichtingen van op hun respectieve grondgebieden gevestigde fabrikanten of aanbieders van ICT-producten, -diensten of -processen, ten aanzien van de EU-conformiteitsverklaring, volgen en handhaven, de nationale accreditatie-instanties bijstaan bij het volgen van en toezicht op de activiteiten van conformiteitsbeoordelingsinstanties door hen te voorzien van expertise en relevante informatie, conformiteitsbeoordelingsinstanties toestaan hun taken uit te voeren wanneer dergelijke instanties voldoen aan in Europese cyberbeveiligingscertificeringsregelingen gestelde aanvullende vereisten, en relevante ontwikkelingen volgen op het gebied van cyberbeveiligingscertificering. De nationale cyberbeveiligingscertificeringsautoriteiten moeten klachten behandelen die natuurlijke of rechtspersonen hebben ingediend over door die autoriteiten afgegeven Europese cyberbeveiligingscertificaten of in verband met Europese cyberbeveiligingscertificaten die zijn afgegeven door conformiteitsbeoordelingsinstanties indien in dergelijke certificaten

zekerheidsniveau „hoog" staat aangegeven, 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. Bovendien moeten de nationale cyberbeveiligingscertificeringsautoriteiten samenwerken met andere nationale autoriteiten voor cyberbeveiligingscertificering of andere overheidsinstanties, onder meer door de uitwisseling van informatie over de mogelijke niet-conformiteit van ICT-producten, -diensten en -processen met de voorschriften van deze verordening of van specifieke Europese cyberbeveiligingscertificeringsregelingen. De Commissie moet die informatie-uitwisseling bevorderen door een algemeen elektronisch informatieondersteuningssysteem beschikbaar te stellen, bijvoorbeeld het informatie- en communicatiesysteem voor markttoezicht (ICSMS) en het systeem voor snelle waarschuwingen over gevaarlijke niet-levensmiddelen (Rapex), die overeenkomstig Verordening (EG) nr. 765/2008 al door markttoezichtautoriteiten worden gebruikt.

(103) Om de consistente toepassing van het Europees cyberbeveiligingscertificeringskader te waarborgen moet een EGC worden opgericht die is samengesteld uit vertegenwoordigers van de nationale cyberbeveiligingscertificeringsautoriteiten of andere relevante nationale autoriteiten. De voornaamste taken van de EGC moeten bestaan in het verlenen van advies en bijstand aan de Commissie bij haar taak een samenhangende uitvoering en toepassing van het Europees cyberbeveiligingscertificeringskader te waarborgen, het verlenen van bijstand aan en het nauw samenwerken met Enisa bij het opstellen van potentiële cyberbeveiligingscertificeringsregelingen, het in naar behoren gemotiveerde gevallen verzoeken van Enisa om een potentiële regeling op te stellen, het vaststellen van aan Enisa gerichte standpunten over potentiële regelingen en het vaststellen van aan de Commissie gerichte standpunten over de instandhouding en herziening van bestaande Europese cyberbeveiligingscertificeringsregelingen. De EGC moet de uitwisseling vergemakkelijken van goede praktijken en expertise tussen de verschillende nationale cyberbeveiligingscertificeringsautoriteiten die verantwoordelijk zijn voor de toelating van conformiteitsbeoordelingsinstanties en voor de afgifte van Europese cyberbeveiligingscertificaten.

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

(105) Teneinde de handel verder te vergemakkelijken, en erkennende dat ICT-toeleveringsketens mondiaal zijn, kan de Unie overeenkomstig artikel 218 van het Verdrag betreffende de werking van de Europese Unie (VWEU) overeenkomsten inzake wederzijdse erkenning sluiten met betrekking tot Europese cyberbeveiligingscertificaten. De Commissie, rekening houdend met het advies van Enisa en de Europese Groep voor cyberbeveiligingscertificering, kan aanbevelen daarover onderhandelingen te openen. Iedere Europese cyberbeveiligingscertificeringsregeling moet specifieke voorwaarden bevatten voor dergelijke overeenkomsten met derde landen inzake wederzijdse erkenning.

(106) Aan de Commissie dienen de uitvoeringsbevoegdheden te worden verleend opdat zij voor uniforme omstandigheden voor de uitvoering van deze verordening kan zorgen. Die bevoegdheden moeten worden uitgeoefend overeenkomstig Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad ([22]).

(107) De onderzoeksprocedure moet worden toegepast voor de vaststelling van uitvoeringshandelingen inzake Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten of -processen, voor de vaststelling van uitvoeringshandelingen inzake regelingen voor door Enisa uit te voeren onderzoeken, voor de vaststelling van uitvoeringshandelingen inzake een plan voor de collegiale toetsing van nationale cyberbeveiligingscertificeringsautoriteiten, alsmede voor de vaststelling van uitvoeringshandelingen inzake de omstandigheden, vormen en procedures voor kennisgeving aan de Commissie van geaccrediteerde conformiteitsbeoordelingsinstanties door de nationale cyberbeveiligingscertificeringsautoriteiten.

(108) De werking van Enisa moet aan een regelmatige en onafhankelijke evaluatie worden onderworpen. Die evaluatie moet betrekking hebben op de verwezenlijking van de doelstellingen van Enisa, zijn werkmethoden en de relevantie van zijn taken, met name zijn taken met betrekking tot de operationele samenwerking op Unieniveau. Bij die evaluatie moeten tevens de gevolgen, de doeltreffendheid en de efficiëntie van het Europees cyberbeveiligingscertificeringskader worden geëvalueerd. In geval van een herziening moet de Commissie nagaan hoe de rol van Enisa als referentiepunt voor advies en expertise kan worden versterkt en moet de Commissie tevens de mogelijkheid evalueren van een rol voor Enisa bij het helpen beoordelen van ICT-producten, -diensten en -processen uit derde landen die niet aan de Unieregels voldoen.

([22]) Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

(109) Aangezien de doelstellingen van deze verordening niet voldoende door de lidstaten kunnen worden verwezenlijkt, maar vanwege de omvang en de gevolgen ervan 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 (VEU) neergelegde subsidiariteitsbeginsel. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om die doelstellingen te verwezenlijken.

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

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 aangelegenheden in verband met Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging); evenals

b) een kader voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen teneinde een toereikend cyberbeveiligingsniveau van ICT-producten, -diensten en -processen in de Unie te waarborgen, alsmede om versnippering van de interne markt wat betreft cyberbeveiligingscertificeringsregelingen in de Unie te vermijden.

Het in de eerste alinea, onder b), bedoelde kader is van toepassing onverminderd specifieke bepalingen inzake vrijwillige of verplichte certificering in andere rechtshandelingen van de Unie.

2. Deze verordening laat de bevoegdheden van de lidstaten betreffende activiteiten op het gebied van openbare beveiliging, defensie, nationale veiligheid 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": de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen;

2. „netwerk- en informatiesysteem": een netwerk- en informatiesysteem als gedefinieerd in artikel 4, punt 1, van Richtlijn (EU) 2016/1148;

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

4. „aanbieder van essentiële diensten": een aanbieder van essentiële diensten als gedefinieerd in artikel 4, punt 4, van Richtlijn (EU) 2016/1148;

5. „digitaledienstverlener": een digitaledienstverlener als gedefinieerd in artikel 4, punt 6, van Richtlijn (EU) 2016/1148;

6. „incident": een incident als gedefinieerd in artikel 4, punt 7, van Richtlijn (EU) 2016/1148;

7. „incidentenbehandeling": incidentenbehandeling als gedefinieerd in artikel 4, punt 8, van Richtlijn (EU) 2016/1148;

8. „cyberdreiging": elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden;

9. „Europese cyberbeveiligingscertificeringsregeling": een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die op Unieniveau zijn vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van specifieke ICT-producten, -diensten en -processen;

10. „nationale cyberbeveiligingscertificeringsregeling": een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die door een nationale overheidsinstantie zijn ontwikkeld en vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van ICT-producten, -diensten en -processen die onder het toepassingsgebied van de specifieke regeling vallen;

11. „Europees cyberbeveiligingscertificaat": een door een bevoegde instantie afgegeven document waarin wordt bevestigd dat is geëvalueerd of een bepaald ICT-product, een bepaalde ICT-dienst of een bepaald ICT-proces voldoet aan de specifieke, in een Europese cyberbeveiligingscertificeringsregeling vastgestelde beveiligingsvoorschriften;

12. „ICT-product": een element of groep elementen van een netwerk- of informatiesysteem;

13. „ICT-dienst": een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen;

14. „ICT-proces": een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden;

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

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

17. „conformiteitsbeoordeling": een conformiteitsbeoordeling als gedefinieerd in artikel 2, punt 12, van Verordening (EG) nr. 765/2008;

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

19. „norm": een norm als gedefinieerd in artikel 2, punt 1, van Verordening (EU) nr. 1025/2012;

20. „technische specificatie": een document waarin de technische vereisten of conformiteitsbeoordelingsprocedures zijn voorgeschreven waaraan een ICT-product, een ICT-dienst of een ICT-proces moet voldoen;

21. „zekerheidsniveau": een basis voor vertrouwen dat een ICT-product, -dienst of -proces aan de beveiligingsvoorschriften van een specifieke Europese cyberbeveiligingscertificeringsregeling voldoet, die aangeeft op welk niveau het betrokken ICT-product, de betrokken ICT-dienst of het betrokken ICT-proces is geëvalueerd maar als zodanig geen maatstaf is voor de beveiliging van het betrokken ICT-product, de betrokken ICT-dienst of het betrokken ICT-proces;

22. „conformiteitszelfbeoordeling": een maatregel die wordt uitgevoerd door een fabrikant of aanbieder van ICT-producten, -diensten of -processen die evalueert of de ICT-producten, -diensten of -processen voldoen aan de in een specifieke Europese cyberbeveiligingscertificeringsregeling opgenomen voorschriften.

TITEL II

ENISA (HET AGENTSCHAP VAN DE EUROPESE UNIE VOOR CYBERBEVEILIGING)

HOOFDSTUK I

Mandaat en doelstellingen

Artikel 3

Mandaat

1. Enisa verricht de krachtens deze verordening aan hem toegewezen taken met als doel een hoog gemeenschappelijk cyberbeveiligingsniveau te bereiken in de hele Unie, onder meer door actief steun te verlenen aan de lidstaten, instellingen, organen en instanties van de Unie met het oog op betere cyberbeveiliging. Enisa fungeert voor de instellingen, organen en instanties van de Unie, evenals voor andere betrokken belanghebbenden van de Unie, als referentiepunt voor advies en expertise op het gebied van cyberbeveiliging.

Door de taken uit te voeren die het krachtens deze verordening krijgt toegewezen, draagt Enisa bij tot het verminderen van de versnippering van de interne markt.

2. Enisa verricht de taken die hem worden toegewezen bij rechtshandelingen van de Unie tot vaststelling van maatregelen voor de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die betrekking hebben op cyberbeveiliging.

3. Enisa voert zijn taken op onafhankelijke wijze uit, waarbij het dubbel werk met de activiteiten van de lidstaten vermijdt en rekening houdt met de reeds bestaande expertise in de lidstaten.

4. Enisa ontwikkelt zijn eigen middelen, met inbegrip van technische en menselijke capaciteiten en vaardigheden, om de uit hoofde van deze verordening toegewezen taken uit te voeren.

Artikel 4

Doelstellingen

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

2. Enisa staat de instellingen, organen en instanties van de Unie alsmede de lidstaten bij in de ontwikkeling en uitvoering van het cyberbeveiligingsbeleid van de Unie, waaronder sectoraal cyberbeveiligingsbeleid.

3. Enisa ondersteunt de capaciteitsopbouw en de paraatheid in de hele Unie door de instellingen, organen en instanties van de Unie, alsmede de lidstaten en publieke en particuliere belanghebbenden bij te staan teneinde de bescherming van hun netwerk- en informatiesystemen te verbeteren, cyberweerbaarheid en cyberresponscapaciteit te ontwikkelen en te verbeteren, en vaardigheden en bekwaamheden op het gebied van cyberbeveiliging te ontwikkelen.

4. Enisa bevordert de samenwerking, met inbegrip van informatie-uitwisseling, en coördinatie op Unieniveau tussen de lidstaten, de instellingen, organen en instanties van de Unie, en betrokken particuliere en publieke belanghebbenden inzake aangelegenheden op het gebied van cyberbeveiliging.

5. Enisa draagt bij tot het versterken van de cyberbeveiligingscapaciteiten op Unieniveau ter ondersteuning van de maatregelen van de lidstaten om cyberdreigingen te voorkomen en daarop te reageren, met name in het geval van grensoverschrijdende incidenten.

6. Enisa bevordert het gebruik van Europese cyberbeveiligingscertificering om versnippering van de interne markt te vermijden. Enisa draagt bij tot het tot stand brengen en handhaven van een Europees cyberbeveiligingscertificeringskader overeenkomstig titel III van deze verordening, met het oog op een transparantere cyberbeveiliging van ICT-producten, -diensten en -processen, waardoor het vertrouwen in de digitale interne markt en haar concurrentievermogen wordt versterkt.

7. Enisa stimuleert bij burgers, organisaties en bedrijven een grote mate van bewustwording betreffende cyberbeveiliging, en bevordert onder meer de cyberhygiëne en cybergeletterdheid.

HOOFDSTUK II

Taken

Artikel 5

Ontwikkeling en uitvoering van Uniebeleid en -recht

Enisa draagt bij tot de ontwikkeling en uitvoering van Uniebeleid en -recht door:

1. bijstand en advies inzake de ontwikkeling en herziening van Uniebeleid en -recht op het gebied van cyberbeveiliging en van sectorspecifieke beleids- en rechtsinitiatieven die verband houden met cyberbeveiliging, met name door het verstrekken van onafhankelijk advies en onafhankelijke analyse en door het verrichten van voorbereidende werkzaamheden;

2. de lidstaten bij te staan bij de consistente uitvoering van het Uniebeleid en -recht inzake cyberbeveiliging, met name in verband met Richtlijn (EU) 2016/1148, onder meer door middel van het verstrekken van standpunten, richtsnoeren, adviezen 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 vlak bevoegde autoriteiten;

3. de lidstaten en instellingen, organen en instanties van de Unie bij te staan in de ontwikkeling en bevordering van cyberbeveiligingsbeleid in verband met het vrijwaren van de algemene beschikbaarheid of integriteit van de openbare kern van het open internet;

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

5. ondersteuning te bieden:

   a) bij de ontwikkeling en uitvoering van Uniebeleid op het gebied van elektronische identiteits- en vertrouwensdiensten, in het bijzonder door advies en technische richtsnoeren te verstrekken alsmede door de uitwisseling van beste praktijken tussen de bevoegde autoriteiten te vergemakkelijken;

   b) bij de bevordering van een verhoogd beveiligingsniveau van elektronische communicatie, onder meer door advies en expertise te verstrekken alsmede door de uitwisseling van beste praktijken tussen de bevoegde autoriteiten te vergemakkelijken;

   c) aan lidstaten bij de uitvoering van specifieke cyberbeveiligingsaspecten van Uniebeleid en -recht inzake gegevensbescherming en privacy, waaronder, op verzoek, het verstrekken van advies aan het Europees Comité voor gegevensbescherming.

6. ondersteuning te bieden bij de regelmatige toetsing van Uniebeleidsactiviteiten door een jaarlijks verslag voor te bereiden over de stand van uitvoering van het juridisch kader inzake:

   a) informatie over de ingevolge artikel 10, lid 3, van Richtlijn (EU) 2016/1148 aan de samenwerkingsgroep door de centrale contactpunten van iedere lidstaat gerapporteerde meldingen van incidenten;

   b) overzichten van de ingevolge artikel 19, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad [23] door de toezichthoudende organen aan Enisa gemaakte meldingen van beveiligingsinbreuken of integriteitsverlies die werden ontvangen van aanbieders van vertrouwensdiensten;

   c) ingevolge artikel 40 van Richtlijn (EU) 2018/1972 door de bevoegde autoriteiten aan Enisa gemaakte meldingen van beveiligingsincidenten door aanbieders van openbare elektronischecommunicatienetwerken of openbare elektronischecommunicatiediensten.

[23] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

Artikel 6

Capaciteitsopbouw

1. Enisa verleent bijstand aan:

a) de lidstaten bij hun inspanningen ter verbetering van de preventie, opsporing en analyse van en de capaciteit om te reageren op cyberdreigingen en -incidenten, door hen te voorzien van kennis en expertise;

b) de lidstaten en instellingen, organen en instanties van de Unie bij de opstelling en uitvoering van openbaarmakingsbeleid inzake kwetsbaarheden op vrijwillige basis;

c) de instellingen, organen en instanties van de Unie bij hun inspanningen ter verbetering van de preventie, opsporing en analyse van cyberdreigingen en -incidenten en ter verbetering van hun capaciteit om op dergelijke dreigingen en incidenten te reageren, met name door passende ondersteuning voor het CERT-EU;

d) de lidstaten, bij de ontwikkeling van nationale CSIRT's, indien het daarom wordt verzocht op grond van artikel 9, lid 5, van Richtlijn (EU) 2016/1148;

e) de lidstaten bij de ontwikkeling van nationale strategieën voor de beveiliging van netwerk- en informatiesystemen, indien het daarom wordt verzocht op grond van artikel 7, lid 2, van Richtlijn (EU) 2016/1148, en het bevordert de verspreiding van die strategieën en neemt kennis van de voortgang van hun uitvoering in de hele Unie teneinde beste praktijken te bevorderen;

f) de instellingen van de Unie bij de ontwikkeling en evaluatie van Uniestrategieën inzake cyberbeveiliging, door de verspreiding van die strategieën te bevorderen en de voortgang van de uitvoering ervan te volgen;

g) de nationale CSIRT's en EU-CSIRT's bij het verhogen van het niveau van hun capaciteiten, 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 minimumcapaciteiten beschikt en overeenkomstig de beste praktijken te werk gaat;

h) de lidstaten door regelmatig en ten minste tweejaarlijks cyberbeveiligingsoefeningen op Unieniveau te organiseren overeenkomstig artikel 7, lid 5, en door beleidsaanbevelingen te verstrekken op basis van de evaluatie van de oefeningen en de daaruit getrokken lessen;

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

j) de samenwerkingsgroep bij de uitwisseling van beste praktijken, met name voor het in kaart brengen van aanbieders van essentiële diensten door de lidstaten, krachtens artikel 11, lid 3, punt 1, van Richtlijn (EU) 2016/1148, onder meer wat grensoverschrijdende afhankelijkheid inzake risico's en incidenten betreft.

2. Enisa ondersteunt 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 inzake beschikbare instrumenten en procedures, en over de manier waarop regelgevingsvraagstukken in verband met informatie-uitwisseling kunnen worden opgelost.

Artikel 7

Operationele samenwerking op Unieniveau

1. Enisa ondersteunt de operationele samenwerking tussen de lidstaten, de instellingen, organen en instanties van de Unie en tussen belanghebbenden.

2. Enisa werkt op operationeel niveau samen met en brengt synergieën tot stand met de instellingen, organen en instanties van de Unie, met inbegrip van CERT-EU, alsook met de diensten die zich bezighouden met cybercriminaliteit, en met de toezichthoudende autoriteiten die zich bezighouden met de bescherming van de persoonlijke levenssfeer en persoonsgegevens, met als doel onderwerpen van gemeenschappelijk belang aan te pakken, onder meer door:

a) het uitwisselen van kennis en beste praktijken;

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

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

3. Enisa verzorgt het secretariaat van het CSIRT-netwerk op grond van artikel 12, lid 2, van Richtlijn (EU) 2016/1148 en steunt in die hoedanigheid op actieve wijze de uitwisseling van informatie en de samenwerking tussen de leden ervan.

4. Enisa steunt de lidstaten wat hun operationele samenwerking binnen het CSIRT-netwerk betreft, door

a) advies te verstrekken over de wijze waarop zij hun preventie-, opsporings- en responscapaciteiten ten aanzien van incidenten kunnen versterken en door, op verzoek van één of meer lidstaten, advies te verstrekken over een specifieke cyberdreiging;

b) op verzoek van één of meer lidstaten te helpen bij de beoordeling van incidenten met aanzienlijke of substantiële gevolgen door expertise aan te reiken en de technische afhandeling van dergelijke incidenten te vergemakkelijken, onder meer door de vrijwillige uitwisseling van relevante informatie en technische oplossingen tussen de lidstaten te steunen;

c) kwetsbaarheden en incidenten te analyseren op basis van algemeen beschikbare informatie of informatie die hiertoe vrijwillig door de lidstaten wordt verstrekt, en

d) op verzoek van één of meer lidstaten steun te verlenen in verband met technische onderzoeken achteraf van incidenten met aanzienlijke of substantiële gevolgen, in de zin van Richtlijn (EU) 2016/1148.

Bij de uitvoering van die taken werken Enisa en CERT-EU op gestructureerde wijze samen om te kunnen profiteren van synergieën en om dubbel werk te voorkomen.

5. Enisa organiseert regelmatig cyberbeveiligingsoefeningen op Unieniveau en ondersteunt de lidstaten en de instellingen, organen en instanties van de Unie op hun verzoek bij de organisatie van cyberbeveiligingsoefeningen. Dergelijke cyberbeveiligingsoefeningen op Unieniveau kunnen technische, operationele of strategische onderdelen bevatten. Om de twee jaar organiseert Enisa een grootschalige alomvattende oefening.

Enisa levert in voorkomend geval ook een bijdrage aan, en hulp bij de organisatie van, sectorale cyberbeveiligingsoefeningen, samen met relevante organisaties die ook deelnemen aan cyberbeveiligingsoefeningen op Unieniveau.

6. Enisa stelt in nauwe samenwerking met de lidstaten regelmatig een grondig technisch situatieverslag inzake de EU-cyberbeveiliging op met betrekking tot incidenten en cyberdreigingen, op basis 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 Richtlijn (EU) 2016/1148 opgerichte centrale contactpunten, beide op vrijwillige basis, EC3 en CERT-EU.

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

a) algemeen beschikbare of op vrijwillige basis gedeelde verslagen van nationale bronnen te bundelen en te analyseren teneinde bij te dragen tot het tot stand brengen van een gemeenschappelijk situatiebewustzijn;

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

c) op verzoek de technische afhandeling van dergelijke incidenten of crises te vergemakkelijken, met name door onder meer steun te verlenen aan het vrijwillig delen van technische oplossingen tussen de lidstaten;

d) steun te verlenen aan de instellingen, organen en instanties van de Unie en, op hun verzoek, aan de lidstaten bij de communicatie met het publiek in verband met dergelijke incidenten of crises;

e) de samenwerkingsplannen wat betreft de reactie op dergelijke incidenten of crises op Unieniveau te toetsen, en op hun verzoek de lidstaten te steunen bij het toetsen van dergelijke plannen op nationaal niveau.

Artikel 8

Markt, cyberbeveiligingscertificering en normalisatie

1. Enisa ondersteunt en bevordert de ontwikkeling en uitvoering van het Uniebeleid inzake cyberbeveiligingscertificering van ICT-producten, -diensten en -processen, zoals vastgesteld in titel III van deze verordening, door:

a) de ontwikkelingen op het vlak van normalisatie in aanverwante gebieden voortdurend te blijven volgen en op grond van artikel 54, lid 1, onder c), passende technische specificaties aan te bevelen voor gebruik bij de ontwikkeling van Europese cyberbeveiligingscertificeringsregelingen indien geen normen beschikbaar zijn;

b) overeenkomstig artikel 49 potentiële Europese cyberbeveiligingscertificeringsregelingen („potentiële regelingen") voor ICT-producten, -diensten en -processen voor te bereiden;

c) vastgestelde Europese cyberbeveiligingscertificeringsregelingen overeenkomstig artikel 49, lid 8, te evalueren;

d) op grond van artikel 59, lid 4, deel te nemen aan collegiale toetsingen;

e) op grond van artikel 62, lid 5, de Commissie bij te staan bij het verzorgen van het secretariaat van de EGC.

2. Enisa verzorgt het secretariaat van de Groep van belanghebbenden bij cyberbeveiligingscertificering op grond van artikel 22, lid 4.

3. Enisa stelt richtsnoeren op en maakt die bekend, en ontwikkelt goede praktijken, wat betreft de cyberbeveiligingsvoorschriften voor ICT-producten, -diensten en -processen, in samenwerking met de nationale cyberbeveiligingscertificeringsautoriteiten en de sector in een formeel, gestructureerd en transparant proces.

4. Enisa draagt bij aan capaciteitsopbouw in verband met evaluatie- en certificeringsprocessen door richtsnoeren te verzamelen en bekend te maken, en door op verzoek steun te verlenen aan de lidstaten.

5. Enisa vergemakkelijkt de opstelling en toepassing van Europese en internationale normen voor risicobeheersing en voor de beveiliging van ICT-producten, -diensten en -processen;

6. Enisa verleent op grond van artikel 19, lid 2, van Richtlijn (EU) 2016/1148 advies en stelt richtsnoeren op — in samenwerking met de lidstaten en de sector — met betrekking tot de technische gebieden die verband houden met de beveiligingsvoorschriften voor aanbieders van essentiële diensten en digitaledienstverleners, en met betrekking tot reeds bestaande normen, met inbegrip van nationale normen van de lidstaten.

7. Enisa verricht en verspreidt regelmatig analyses van de voornaamste tendensen op de markt voor cyberbeveiliging, zowel aan de vraag- als aan de aanbodzijde, teneinde de markt voor cyberbeveiliging in de Unie te stimuleren.

Artikel 9

Kennis en informatie

Enisa:

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

b) verricht strategische langetermijnanalyses van cyberdreigingen en -incidenten teneinde nieuwe tendensen in kaart te brengen en incidenten te helpen voorkomen;

c) verstrekt, in samenwerking met deskundigen van autoriteiten van de lidstaten en betrokken belanghebbenden, 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 vermelde sectoren ondersteunen en die welke worden gebruikt door de in bijlage III bij die richtlijn vermelde digitaledienstverleners;

d) het bundelt en organiseert door middel van een hiervoor bestemd portaal informatie over cyberbeveiliging die door de instellingen, organen en instanties van de Unie wordt verstrekt en informatie over cyberbeveiliging die op vrijwillige basis door de lidstaten en publieke en particuliere belanghebbenden wordt verstrekt, en stelt die informatie via dat portaal beschikbaar aan het publiek;

e) het verzamelt en analyseert publiek beschikbare informatie over significante incidenten, en stelt verslagen op met het oog op het verstrekken van richtsnoeren aan burgers, organisaties en bedrijven in de hele Unie.

Artikel 10

Bewustmaking en voorlichting

Enisa:

a) draagt bij tot de maatschappelijke bewustmaking van cyberbeveiligingsrisico's en verstrekt richtsnoeren inzake goede praktijken voor individuele gebruikers, gericht op burgers, organisaties en bedrijven, waaronder cyberhygiëne en cybergeletterdheid;

b) het organiseert, in samenwerking met de lidstaten, de instellingen, organen en instanties van de Unie en de sector, regelmatig voorlichtingscampagnes teneinde de cyberbeveiliging in de Unie te versterken en zichtbaarder te maken en een breed publiek debat te stimuleren;

c) staat de lidstaten bij in hun inspanningen mom het cyberbeveiligingsbewustzijn te verhogen en bevordert cyberbeveiligingsvoorlichting;

d) ondersteunt nauwere coördinatie en uitwisseling van beste praktijken tussen de lidstaten met betrekking tot cyberbeveiligingsbewustzijn en -voorlichting.

Artikel 11

Onderzoek en innovatie

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

a) advies verlenen aan de instellingen, organen en instanties van 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 cyberdreigingen, onder meer met betrekking tot nieuwe en opkomende informatie- en communicatietechnologieën, en om risicopreventietechnologieën doeltreffend te kunnen gebruiken;

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

c) bijdragen aan de strategische onderzoeks- en innovatieagenda op Unieniveau op het gebied van cyberbeveiliging.

Artikel 12

Internationale samenwerking

Enisa draagt bij aan de inspanningen van de Unie om met derde landen en internationale organisaties evenals binnen de toepasselijke internationale samenwerkingskaders samen te werken teneinde de internationale samenwerking op het gebied van cyberbeveiliging te bevorderen, door:

a) waar passend, als waarnemer betrokken te zijn bij de organisatie van internationale oefeningen, en de resultaten van dergelijke oefeningen te analyseren en er verslag over uit te brengen aan de raad van bestuur;

b) op verzoek van de Commissie de uitwisseling van beste praktijken te vergemakkelijken;

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

d) de Commissie advies en steun te verlenen inzake overeenkomsten met derde landen betreffende de wederzijdse erkenning van cyberbeveiligingscertificaten, zulks in samenwerking met de bij artikel 62 ingestelde EGC.

HOOFDSTUK III

Organisatie van Enisa

Artikel 13

Structuur van Enisa

De administratieve en beheersstructuur van Enisa is samengesteld uit:

a) een raad van bestuur;

b) een dagelijks bestuur;

c) een uitvoerend directeur;

d) een Enisa-adviesgroep;

e) een netwerk van nationale verbindingsfunctionarissen.

Afdeling 1

Raad van bestuur

Artikel 14

Samenstelling van de raad van bestuur

1. De raad van bestuur bestaat uit per lidstaat één lid dat door die lidstaat is benoemd en twee door de Commissie benoemde leden. Alle leden hebben stemrecht.

2. Elk lid van de raad van bestuur heeft een plaatsvervanger. Die plaatsvervanger vertegenwoordigt het lid in geval van diens 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 rekening houdend met hun relevante leidinggevende, 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 vertegenwoordiging 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 15

Taken van de raad van bestuur

1. De raad van bestuur:

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

b) stelt het in artikel 24 bedoelde ontwerp van het enig programmeringsdocument van Enisa vast, voordat het bij de Commissie voor advies wordt ingediend;

c) stelt, rekening houdend met het advies van de Commissie, het enig programmeringsdocument van Enisa vast;

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

e) stelt de jaarlijkse begroting van Enisa vast en oefent andere functies uit met betrekking tot de begroting van Enisa overeenkomstig hoofdstuk IV;

f) beoordeelt het geconsolideerde jaarverslag over de activiteiten van Enisa, dat de rekeningen bevat en beschrijft hoe Enisa zijn prestatie-indicatoren heeft nageleefd, en keurt dit jaarverslag goed, doet zowel het jaarverslag als zijn beoordeling daarvan uiterlijk op 1 juli van het volgende jaar toekomen aan het Europees Parlement, de Raad, de Commissie en de Rekenkamer, en maakt dit jaarverslag openbaar;

g) stelt overeenkomstig artikel 32 de financiële regels vast die van toepassing zijn op Enisa;

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

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

j) zorgt voor adequate opvolging 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;

k) stelt zijn reglement van orde vast, met inbegrip van voorlopige besluiten over de delegatie van specifieke taken op grond van artikel 19, lid 7;

l) oefent, overeenkomstig lid 2 van dit artikel, ten aanzien van het personeel van Enisa de bevoegdheden uit die het Statuut van de ambtenaren van de Europese Unie (het „Statuut van de ambtenaren") en de Regeling welke van toepassing is op de andere personeelsleden van de Europese Unie (de „Regeling welke van toepassing is op de andere personeelsleden"), zoals vastgesteld in Verordening (EEG, Euratom, EGKS) nr. 259/68 van de Raad ([24]), toekennen aan het tot aanstelling bevoegde gezag en het tot het aangaan van arbeidsovereenkomsten bevoegde gezag (hierna „de bevoegdheden van het tot aanstelling bevoegde gezag" genoemd);

m) stelt overeenkomstig in artikel 110 bepaalde de procedure van het Statuut van de ambtenaren voorschriften op voor de toepassing van het Statuut van de ambtenaren en van de Regeling welke van toepassing is op de andere personeelsleden;

n) benoemt de uitvoerend directeur en, indien van toepassing, verlengt zijn of haar ambtstermijn of ontheft hem uit zijn of haar functie overeenkomstig artikel 36;

o) benoemt een rekenplichtige, die de rekenplichtige van de Commissie kan zijn en die volledig onafhankelijk is bij de uitvoering van zijn of haar taken;

p) neemt alle beslissingen in verband met het opzetten van de interne structuren van Enisa en, waar nodig, de wijziging van die interne structuren, rekening houdend met de activiteitenbehoeften van Enisa en met het oog op een gezond begrotingsbeheer;

q) geeft machtiging tot het opstellen van werkafspraken ten aanzien van artikel 7.

r) geeft machtiging tot het opstellen of het sluiten van werkafspraken overeenkomstig artikel 42.

2. Overeenkomstig artikel 110 van het Statuut van de ambtenaren neemt de raad van bestuur op grond van artikel 2, lid 1, van het Statuut van de ambtenaren alsmede op grond van artikel 6 van de Regeling welke van toepassing is op de andere personeelsleden, een besluit waarbij hij de nodige bevoegdheden van het tot aanstelling bevoegde gezag delegeert aan de uitvoerend directeur en de voorwaarden bepaalt voor de opschorting van die gedelegeerde bevoegdheden. De uitvoerend directeur kan die bevoegdheden op zijn beurt delegeren.

([24]) PB L 56 van 4.3.1968, blz. 1.

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 van het tot aanstelling bevoegde gezag die de uitvoerend directeur op zijn beurt heeft gedelegeerd, tijdelijk opschorten en die bevoegdheden in diens plaats zelf uitoefenen of delegeren aan een van zijn leden of aan een ander personeelslid dan de uitvoerend directeur.

Artikel 16

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. Hun ambtstermijn bedraagt 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 niet in staat is om zijn taken te verrichten.

Artikel 17

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 zijn 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 aan de vergaderingen van de raad van bestuur, maar heeft geen stemrecht.

4. De leden van de Enisa-adviesgroep kunnen deelnemen aan de vergaderingen van de raad van bestuur op uitnodiging van de voorzitter, maar hebben geen stemrecht.

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

6. Enisa verzorgt het secretariaat voor de raad van bestuur.

Artikel 18

Stemregels in de raad van bestuur

1. De raad van bestuur neemt besluiten met een meerderheid van zijn 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 of haar plaatsvervanger gerechtigd het stemrecht van het lid uit te oefenen.

4. De voorzitter van de raad van bestuur neemt deel aan de stemming.

5. De uitvoerend directeur neemt niet deel aan de stemming.

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 19

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 opvolging van de bevindingen en aanbevelingen die voortkomen uit onderzoeken van OLAF en de diverse interne of externe auditverslagen en evaluaties;

c) verleent, onverminderd de in artikel 20 bepaalde verantwoordelijkheden van de uitvoerend directeur, op grond van dat artikel bijstand en advies aan de uitvoerend directeur bij de uitvoering van de besluiten van de raad van bestuur inzake administratieve en budgettaire aangelegenheden.

3. Het dagelijks bestuur bestaat uit vijf leden. Zij worden benoemd uit de leden van de raad van bestuur. Een van de leden is de voorzitter van de raad van bestuur, die tevens het dagelijks bestuur kan voorzitten, en een ander lid is een van de vertegenwoordigers van de Commissie. Bij de benoemingen van de leden van het dagelijks bestuur wordt een evenwicht tussen mannen en vrouwen nagestreefd. De uitvoerend directeur neemt deel aan de vergaderingen van het dagelijks bestuur, maar heeft geen stemrecht.

4. De ambtstermijn van de leden van het dagelijks bestuur bedraagt vier jaar. Die termijn kan worden verlengd.

5. Het dagelijks bestuur vergadert ten minste eens in de drie maanden. De voorzitter van het dagelijks bestuur belegt aanvullende vergaderingen op verzoek van de leden ervan.

6. De raad van bestuur stelt het reglement van orde van het dagelijks bestuur vast.

7. Indien nodig wegens hoogdringendheid kan het dagelijks bestuur namens de raad van bestuur bepaalde voorlopige besluiten nemen, met name op het gebied van administratief beheer, met inbegrip van de opschorting van de delegatie van de bevoegdheden van het tot aanstelling bevoegde gezag en begrotingsaangelegenheden. Een dergelijk voorlopig besluit wordt onverwijld ter kennis gebracht van de raad van bestuur. De raad van bestuur besluit vervolgens, uiterlijk drie maanden nadat het besluit was genomen, of het voorlopig besluit wordt goedgekeurd of afgewezen. Het dagelijks bestuur neemt geen besluiten namens de raad van bestuur waarvoor een tweederdemeerderheid van de leden van de raad van bestuur is vereist.

Afdeling 3

Uitvoerend directeur

Artikel 20

Taken van de uitvoerend directeur

1. Enisa 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) de dagelijks leiding van Enisa;

b) de uitvoering van de besluiten van de raad van bestuur;

c) de opstelling van het enig programmeringsdocument en de indiening ter goedkeuring ervan bij de raad van bestuur voordat het bij de Commissie wordt ingediend;

d) de uitvoering van het enig programmeringsdocument en de verslaglegging erover aan de raad van bestuur;

e) de opstelling van het geconsolideerde jaarverslag over de activiteiten van Enisa, waaronder de uitvoering van het jaarlijkse werkprogramma van Enisa, en de indiening ter beoordeling en goedkeuring ervan bij de raad van bestuur;

f) de opstelling van een actieplan voor de opvolging van de conclusies van de evaluaties achteraf, en de verslaglegging elke twee jaar aan de Commissie over de geboekte vooruitgang;

g) de opstelling van een actieplan voor de opvolging van de conclusies van interne of externe auditverslagen, alsook van onderzoeken van het OLAF, en de verslaglegging over de geboekte vooruitgang, tweemaal per jaar aan de Commissie en op regelmatige tijdstippen aan de raad van bestuur;

h) de opstelling van het ontwerp van de in artikel 32 bedoelde financiële regels die van toepassing is op Enisa;

i) de opstelling van de ontwerpraming van ontvangsten en uitgaven van Enisa en de uitvoering van de begroting van Enisa;

j) de bescherming van de financiële belangen van de Unie door maatregelen ter voorkoming van fraude, corruptie en andere illegale activiteiten toe te passen, controles te verrichten en, wanneer er onregelmatigheden worden ontdekt, ten onrechte betaalde bedragen terug te vorderen en in voorkomend geval doeltreffende, evenredige en afschrikkende administratieve en financiële sancties op te leggen;

k) de opstelling van een fraudebestrijdingsstrategie voor Enisa en de voorlegging ervan aan de raad van bestuur ter goedkeuring;

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

m) de regelmatige uitwisseling van standpunten en informatie met de instellingen, organen en instanties van de Unie over hun cyberbeveiligingsactiviteiten om te zorgen voor samenhang in de ontwikkeling en uitvoering van het Uniebeleid;

n) de verrichting van andere taken waarmee de uitvoerend directeur krachtens deze verordening is belast.

4. Indien noodzakelijk en in overeenstemming met de doelstellingen en taken van Enisa, kan de uitvoerend directeur ad-hocwerkgroepen instellen, samengesteld uit deskundigen, waaronder deskundigen van de bevoegde autoriteiten van de lidstaten. De raad van bestuur wordt daarvan van tevoren door de uitvoerend directeur 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 Enisa vastgesteld.

5. De uitvoerend directeur kan, indien nodig voor de efficiënte en doeltreffende uitvoering van de taken van Enisa 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 advies van de betrokken lidstaten, waaronder de lidstaat waar de zetel van Enisa 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 aangelegenheid ter bespreking aan de Raad voorgelegd. Het aantal personeelsleden in alle lokale kantoren wordt tot een minimum beperkt en maakt in totaal maximaal 40 % uit van het voltallige personeel van Enisa in de lidstaat waar de zetel van Enisa zich bevindt. Het aantal personeelsleden in elk lokaal kantoor maakt maximaal 10 % uit van het totaal aantal personeelsleden van Enisa in de lidstaat waar de zetel van Enisa zich bevindt.

In het besluit tot het opzetten van een lokaal kantoor wordt het toepassingsgebied van de in dat lokale kantoor te verrichten activiteiten omschreven, op zodanige wijze dat onnodige kosten en verdubbeling van administratieve functies van Enisa worden vermeden.

Afdeling 4

Enisa-adviesgroep, groep van belanghebbenden bij cyberbeveiligingscertificering en netwerk van nationale verbindingsfunctionarissen

Artikel 21

Enisa-adviesgroep

1. De raad van bestuur richt, op voorstel van de uitvoerend directeur, op transparante wijze de Enisa-adviesgroep op, samengesteld uit erkende deskundigen die de relevante belanghebbenden vertegenwoordigen, zoals de ICT-sector, aanbieders van openbare elektronischecommunicatienetwerken of -diensten, kleine en middelgrote ondernemingen, aanbieders van essentiële diensten, consumentenorganisaties, universitaire deskundigen op het gebied van cyberbeveiliging en vertegenwoordigers van overeenkomstig Richtlijn (EU) 2018/1972 aangemelde bevoegde autoriteiten, Europese normalisatieorganisaties, evenals rechtshandhavingsinstanties en toezichthoudende autoriteiten voor gegevensbescherming. De raad van bestuur streeft naar een passend evenwicht tussen mannen en vrouwen, een geografisch evenwicht en een evenwicht tussen de verschillende groepen belanghebbenden.

2. Procedures voor de Enisa-adviesgroep, met name betreffende de samenstelling, het in lid 1 bedoelde voorstel van de uitvoerend directeur, het aantal, en de benoeming van zijn leden en de werking van de Enisa-adviesgroep, worden in het huishoudelijk reglement van Enisa vastgelegd en gepubliceerd.

3. De Enisa-adviesgroep 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 Enisa-adviesgroep bedraagt tweeënhalf jaar. Leden van de raad van bestuur zijn geen lid van de Enisa-adviesgroep. Deskundigen van de Commissie en van de lidstaten mogen de vergaderingen van de Enisa-adviesgroep bijwonen en aan de werkzaamheden ervan deelnemen. Vertegenwoordigers van andere door de uitvoerend directeur relevant geachte organen, die geen lid zijn van de Enisa-adviesgroep, mogen worden uitgenodigd op de vergaderingen van de Enisa-adviesgroep en deelnemen aan de werkzaamheden ervan.

5. De Enisa-adviesgroep adviseert Enisa met betrekking tot de uitvoering van zijn activiteiten, met uitzondering van de toepassing van de bepalingen van titel III van deze verordening. Zij adviseert met name de uitvoerend directeur met betrekking tot de opstelling van een voorstel voor het jaarlijkse werkprogramma van Enisa en met betrekking tot de communicatie met de relevante belanghebbenden over met het jaarlijkse werkprogramma verband houdende aangelegenheden.

6. De Enisa-adviesgroep informeert de raad van bestuur regelmatig over haar activiteiten.

Artikel 22

Groep van belanghebbenden bij cyberbeveiligingscertificering

1. De Groep van belanghebbenden bij cyberbeveiligingscertificering wordt opgericht.

2. De Groep van belanghebbenden bij cyberbeveiligingscertificering bestaat uit leden die gekozen worden uit erkende deskundigen die de betrokken belanghebbenden vertegenwoordigen. De Commissie selecteert de leden van de Groep van belanghebbenden bij cyberbeveiligingscertificering op basis van een voorstel van Enisa na een transparante en open oproep en zorgt voor een evenwicht tussen de verschillenden groepen belanghebbenden alsmede voor een evenwicht tussen mannen en vrouwen en een geografisch evenwicht.

3. De Groep van belanghebbenden bij cyberbeveiligingscertificering:

a) adviseert de Commissie over strategische aangelegenheden met betrekking tot het Europees cyberbeveiligingscertificeringskader;

b) verleent Enisa op verzoek advies over algemene en strategische aangelegenheden wat betreft de taken van Enisa in verband met de markt, cyberbeveiligingscertificering en normalisatie;

c) staat de Commissie bij in de voorbereiding van het in artikel 47 bedoelde voortschrijdend werkprogramma van de Unie;

d) verleent advies over het voortschrijdend werkprogramma van de Unie, overeenkomstig artikel 47, lid 4, en

e) verstrekt in dringende gevallen advies aan de Commissie en de EGC over de behoefte aan aanvullende certificeringsregelingen die niet in het voortschrijdend werkprogramma van de Unie zijn opgenomen, zoals uiteengezet in de artikelen 47 en 48.

4. De Groep van belanghebbenden bij cyberbeveiligingscertificering wordt gezamenlijk voorgezeten door de vertegenwoordigers van de Commissie en Enisa, waarbij het secretariaat wordt verzorgd door Enisa.

Artikel 23

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 alle lidstaten (netwerk van nationale verbindingsfunctionarissen). Elke lidstaat wijst één vertegenwoordiger voor het netwerk van nationale verbindingsfunctionarissen aan. De vergaderingen van het netwerk van nationale verbindingsfunctionarissen kunnen in verschillende samenstellingen van deskundigen worden gehouden.

2. Het netwerk van nationale verbindingsfunctionarissen vergemakkelijkt met name de uitwisseling van informatie tussen Enisa en de lidstaten en verleent steun aan Enisa bij de verspreiding van zijn activiteiten, bevindingen en aanbevelingen onder de betrokken belanghebbenden in de hele Unie.

3. De nationale verbindingsfunctionarissen fungeren als contactpunt op nationaal niveau om de samenwerking tussen Enisa en nationale deskundigen in het kader van de uitvoering van het jaarlijkse werkprogramma van Enisa te vergemakkelijken.

4. Hoewel de nationale verbindingsfunctionarissen nauw samenwerken met de vertegenwoordigers van hun respectieve lidstaten in de raad van bestuur, verricht het netwerk van nationale verbindingsfunctionarissen zelf geen dubbel werk ten aanzien van de werkzaamheden van de raad van bestuur, noch ten aanzien van die van andere Uniefora.

5. De taken en procedures van het netwerk van nationale verbindingsfunctionarissen worden in het huishoudelijk reglement van Enisa vastgesteld en bekendgemaakt.

Afdeling 5

Werking

Artikel 24

Enig programmeringsdocument

1. Enisa voert zijn werkzaamheden uit overeenkomstig een enig programmeringsdocument, bestaande uit een jaarlijkse en meerjarige programmering, dat al zijn geplande activiteiten bevat.

2. Elk jaar stelt de uitvoerend directeur overeenkomstig artikel 32 van Gedelegeerde Verordening (EU) nr. 1271/2013 van de Commissie ([25]) een ontwerp van het enig programmeringsdocument op dat de jaarlijkse en meerjarige programmering met de bijbehorende planning van financiële en personele 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 waar nodig aangepast.

([25]) 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).

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

6. De raad van bestuur past het vastgestelde jaarlijkse werkprogramma aan wanneer een nieuwe taak aan Enisa 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 67 bedoelde evaluatie.

Artikel 25

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 nauwkeurig en volledig, en worden jaarlijks schriftelijk afgelegd en telkens wanneer dat nodig is bijgewerkt.

2. De leden van de raad van bestuur, de uitvoerend directeur en de externe deskundigen die deelnemen aan adhocwerkgroepen 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 aangelegenheden.

3. Enisa 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 26

Transparantie

1. Enisa voert zijn activiteiten uit met een hoog niveau van transparantie en overeenkomstig artikel 28.

2. Enisa zorgt ervoor dat geïnteresseerden en alle belanghebbenden worden voorzien van passende, objectieve, betrouwbare en gemakkelijk toegankelijke informatie, in het bijzonder met betrekking tot de resultaten van zijn werkzaamheden. Tevens maakt het de overeenkomstig artikel 25 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 Enisa als waarnemer bij te wonen.

4. Enisa legt in zijn huishoudelijk reglement de praktische regelingen voor de toepassing van de in de leden 1 en 2 vervatte transparantiebepalingen vast.

Artikel 27

Vertrouwelijkheid

1. Onverminderd artikel 28 onthult Enisa aan derden geen verwerkte of ontvangen informatie waarvoor een met redenen omkleed verzoek om vertrouwelijke behandeling is ingediend.

2. De leden van de raad van bestuur, de uitvoerend directeur, de leden van de Enisa-adviesgroep, de externe deskundigen die deelnemen aan ad-hocwerkgroepen en de personeelsleden van Enisa, met inbegrip van de door de lidstaten tijdelijk gedetacheerde ambtenaren, leven ook na de beëindiging van hun functie de geheimhoudingsplicht uit hoofde van artikel 339 VWEU na.

3. Enisa 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 Enisa noodzakelijk is, besluit de raad van bestuur Enisa toestemming te geven om gerubriceerde informatie te verwerken. In dat geval stelt Enisa, in overleg met de diensten van de Commissie, een beveiligingsreglement vast waarbij de veiligheidsbeginselen van Besluiten (EU, Euratom) 2015/443 ([26]) en 2015/444 ([27]) worden toegepast. Dat beveiligingsreglement omvat onder meer bepalingen betreffende de uitwisseling, de verwerking en de opslag van gerubriceerde gegevens.

Artikel 28

Toegang tot documenten

1. Verordening (EG) nr. 1049/2001 is van toepassing op de documenten die gehouden worden door Enisa.

2. De raad van bestuur stelt uiterlijk op 28 december 2019 regelingen voor de uitvoering van Verordening (EG) nr. 1049/2001 vast.

3. Tegen besluiten van Enisa ingevolge artikel 8 van Verordening (EG) nr. 1049/2001 kan een klacht bij de Europese Ombudsman worden ingediend op grond van artikel 228 VWEU of beroep bij het Hof van Justitie van de Europese Unie worden ingesteld op grond van artikel 263 VWEU.

HOOFDSTUK IV

Vaststelling en structuur van de begroting van Enisa

Artikel 29

Vaststelling van de begroting van Enisa

1. De uitvoerend directeur stelt jaarlijks een ontwerpraming op van de ontvangsten en uitgaven van Enisa 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 Enisa 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 raming, die deel uitmaakt van het ontwerp van het enig programmeringsdocument, naar de Commissie en de derde landen waarmee de Unie overeenkomstig artikel 42, lid 2, een overeenkomst heeft gesloten.

4. Op basis van de raming voert de Commissie in het ontwerp van algemene begroting van de Unie, dat zij overeenkomstig artikel 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 van de Unie.

5. Het Europees Parlement en de Raad keuren de kredieten voor de bijdrage van de Unie aan Enisa goed.

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

([26]) 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).

([27]) 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).

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

Artikel 30

Structuur van de begroting van Enisa

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

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

b) bestemmingsontvangsten voor de financiering van specifieke uitgaven in overeenstemming met de in artikel 32 bedoelde financiële regels;

c) financiering van de Unie in de vorm van delegatieovereenkomsten of ad-hocsubsidies in overeenstemming met de in artikel 32 bedoelde financiële regels en met de bepalingen van de relevante instrumenten die het beleid van de Unie ondersteunen;

d) bijdragen van derde landen die overeenkomstig artikel 42 aan de werkzaamheden van Enisa deelnemen;

e) eventuele vrijwillige bijdragen in geld of in natura van de lidstaten.

Lidstaten die vrijwillig bijdragen op grond van de eerste alinea, onder e), kunnen geen aanspraak maken op specifieke rechten of diensten op grond daarvan.

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

Artikel 31

Uitvoering van de begroting van Enisa

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

2. De interne controleur van de Commissie heeft ten aanzien van Enisa 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 Enisa de voorlopige rekeningen van het begrotingsjaar (jaar N) 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 Enisa ingevolge artikel 246 van Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad ([28]) maakt de rekenplichtige van Enisa onder eigen verantwoordelijkheid de definitieve rekeningen van Enisa op en legt deze voor advies voor aan de raad van bestuur.

5. De raad van bestuur brengt advies uit over de definitieve rekeningen van Enisa.

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 van Enisa de definitieve rekeningen van Enisa en het advies van de raad van bestuur toe aan het Europees Parlement, de Raad, de rekenplichtige van de Commissie en de Rekenkamer.

([28]) Verordening (EU, Euratom) 2018/1046 van het Europees Parlement en de Raad van 18 juli 2018 tot vaststelling van de financiële regels van toepassing op de algemene begroting van de Unie, tot wijziging van Verordeningen (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 en Besluit nr. 541/2014/EU en tot intrekking van Verordening (EU, Euratom) nr. 966/2012 (PB L 193 van 30.7.2018, blz. 1).

8. Op dezelfde dag als die waarop hij de definitieve rekeningen van Enisa toezendt, zendt de rekenplichtige van Enisa aan de Rekenkamer een begeleidende brief betreffende die definitieve rekeningen toe, met kopie aan de rekenplichtige van de Commissie.

9. Uiterlijk op 15 november van jaar N + 1 maakt de uitvoerend directeur de definitieve rekeningen van Enisa bekend in het *Publicatieblad van de Europese Unie*.

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

11. De uitvoerend directeur verstrekt het Europees Parlement op verzoek alle inlichtingen die nodig zijn voor het goede verloop van de kwijtingsprocedure voor het desbetreffende begrotingsjaar overeenkomstig artikel 261, lid 3, van Verordening (EU, Euratom) 2018/1046.

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

Artikel 32

Financiële regels

De financiële regels die van toepassing zijn op Enisa worden vastgesteld door de raad van bestuur, na raadpleging van de Commissie. Die regels wijken niet af van Gedelegeerde Verordening (EU) nr. 1271/2013 tenzij dat in verband met de werking van Enisa specifiek vereist is en de Commissie vooraf toestemming heeft verleend.

Artikel 33

Fraudebestrijding

1. Om de bestrijding van fraude, corruptie en andere onwettige activiteiten als bedoeld in Verordening (EU, Euratom) nr. 883/2013 van het Europees Parlement en de Raad ([29]) te bevorderen, treedt Enisa uiterlijk op 28 december 2019 toe tot het Interinstitutioneel Akkoord van 25 mei 1999 tussen het Europees Parlement, de Raad van de Europese Unie en de Commissie van de Europese Gemeenschappen betreffende de interne onderzoeken verricht door het Europees Bureau voor fraudebestrijding (OLAF) ([30]). Enisa stelt het de passende, voor alle werknemers van Enisa 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 Enisa Uniemiddelen hebben ontvangen, audits te verrichten zowel op basis van documenten als door middel van inspecties ter plaatse.

3. OLAF kan, overeenkomstig de bepalingen en procedures van Verordening (EU, Euratom) nr. 883/2013 en Verordening (Euratom, EG) nr. 2185/96 van de Raad ([31]), onderzoeken verrichten, waaronder controles en verificaties ter plaatse, om vast te stellen of er in verband met een door Enisa gefinancierde subsidie of overeenkomst sprake is van fraude, corruptie of andere illegale activiteiten waardoor de financiële belangen van de Unie worden geschaad.

4. Samenwerkingsovereenkomsten met derde landen of internationale organisaties, overeenkomsten, subsidieovereenkomsten en subsidiebesluiten van het Enisa 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.

([29]) 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).

([30]) PB L 136 van 31.5.1999, blz. 15.

([31]) 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).

HOOFDSTUK V

Personeel

Artikel 34

Algemene bepalingen

Het Statuut van de ambtenaren en de Regeling welke 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 Enisa.

Artikel 35

Voorrechten en immuniteit

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

Artikel 36

Uitvoerend directeur

1. De uitvoerend directeur wordt in dienst genomen als een tijdelijk functionaris van Enisa overeenkomstig artikel 2, onder a), van de Regeling welke 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 de arbeidsovereenkomst met de uitvoerend directeur wordt Enisa 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 vijf jaar. Aan het eind van die termijn voert de Commissie een beoordeling uit van de prestaties van de uitvoerend directeur en de toekomstige taken en uitdagingen van Enisa.

6. De raad van bestuur neemt besluiten over de benoeming van de uitvoerend directeur, de verlenging van diens ambtstermijn en de ontheffing van de uitvoerend directeur uit zijn of haar functie overeenkomstig artikel 18, lid 2.

7. Op voorstel van de Commissie, waarin rekening wordt gehouden met de in lid 5 bedoelde beoordeling, kan de raad van bestuur de ambtstermijn van de uitvoerend directeur eenmaal verlengen met vijf jaar.

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

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

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

Artikel 37

Gedetacheerde nationale deskundigen en andere personeelsleden

1. Enisa kan gebruikmaken van gedetacheerde nationale deskundigen of ander personeel dat niet in dienst is van Enisa. Het Statuut van de ambtenaren van de Europese Unie en de Regeling welke 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 Enisa.

HOOFDSTUK VI

Algemene bepalingen betreffende Enisa

Artikel 38

Juridische status van Enisa

1. Enisa 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. Enisa kan in het bijzonder roerende en onroerende zaken verkrijgen of vervreemden en kan in rechte optreden.

3. Enisa wordt vertegenwoordigd door de uitvoerend directeur.

Artikel 39

Aansprakelijkheid van Enisa

1. De contractuele aansprakelijkheid van Enisa 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 Enisa gesloten overeenkomst.

3. In geval van niet-contractuele aansprakelijkheid vergoedt Enisa alle schade die Enisa zelf of zijn personeelsleden in de uitoefening van hun functie hebben veroorzaakt, overeenkomstig de algemene beginselen die de wetgevingen van de lidstaten gemeen hebben.

4. Het Hof van Justitie van de Europese Unie is bevoegd inzake geschillen over de vergoeding van schade als bedoeld in lid 3.

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

Artikel 40

Talenregeling

1. Verordening nr. 1 van de Raad ([32]) is van toepassing op Enisa. De lidstaten en de overige door de lidstaten aangewezen instanties mogen hun verzoeken aan Enisa 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 Enisa vereiste vertaaldiensten worden geleverd door het Vertaalbureau voor de organen van de Europese Unie.

Artikel 41

Bescherming van persoonsgegevens

1. Op de verwerking van persoonsgegevens door Enisa is Verordening (EU) 2018/1725 van toepassing.

2. De raad van bestuur stelt uitvoeringsvoorschriften als bedoeld in artikel 45, lid 3, van Verordening (EU) 2018/1725 vast. De raad van bestuur kan aanvullende maatregelen vaststellen met het oog op de toepassing van Verordening (EU) 2018/1725 door Enisa.

([32]) Verordening (EEG) nr. 1/58 van de Raad van 15 april 1958 tot regeling van het taalgebruik in de Europese Economische Gemeenschap (PB 17 van 6.10.1958, blz. 385).

Artikel 42

Samenwerking met derde landen en internationale organisaties

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

2. Enisa staat open voor deelname van derde landen die met de Unie overeenkomsten in die zin hebben gesloten. Krachtens de desbetreffende bepalingen van dergelijke overeenkomsten worden werkregelingen uitgewerkt voor met name de aard, de omvang en de wijze van deelname van elk van die derde landen aan de werkzaamheden van Enisa, met inbegrip van bepalingen betreffende de deelname aan de initiatieven van Enisa en betreffende financiële en personele bijdragen. Wat personeelszaken betreft, voldoen die werkregelingen in elk geval aan het Statuut van de ambtenaren en de Regeling welke van toepassing is op de andere personeelsleden.

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

Artikel 43

Beveiligingsvoorschriften voor de bescherming van gevoelige niet-gerubriceerde informatie en gerubriceerde informatie

Enisa stelt na overleg met de Commissie beveiligingsvoorschriften vast en past daarbij de beveiligingsbeginselen toe die zijn vervat in de veiligheidsvoorschriften van de Commissie voor de bescherming van gevoelige niet-gerubriceerde gegevens en EUCI, als vermeld in Besluiten (EU, Euratom) 2015/443 en 2015/444. De veiligheidsvoorschriften van Enisa bevatten bepalingen voor de uitwisseling, verwerking en opslag van dergelijke informatie.

Artikel 44

Zetelovereenkomst en voorwaarden voor de werking

1. De nodige regelingen betreffende de huisvesting van Enisa in de gastlidstaat en de faciliteiten die die lidstaat ter beschikking moet stellen, alsmede de specifieke voorschriften die in de gastlidstaat gelden voor de uitvoerend directeur, de leden van de raad van bestuur, de personeelsleden van Enisa en hun gezinsleden, worden vastgelegd in een zetelovereenkomst tussen Enisa en de gastlidstaat, die gesloten wordt nadat de raad van bestuur daarmee heeft ingestemd.

2. De gastlidstaat van Enisa verschaft zo goed mogelijke voorwaarden om een goede werking van Enisa te waarborgen, rekening houdend met 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 45

Administratief toezicht

De Europese Ombudsman ziet overeenkomstig artikel 228 VWEU toe op de activiteiten van Enisa.

TITEL III

CYBERBEVEILIGINGSCERTIFICERINGSKADER

Artikel 46

Europees cyberbeveiligingscertificeringskader

1. Het Europees cyberbeveiligingscertificeringskader wordt ingesteld teneinde de omstandigheden voor de werking van de interne markt te verbeteren, en wel middels een verhoging van het cyberbeveiligingsniveau in de Unie en het mogelijk maken van een geharmoniseerde aanpak op Unieniveau van Europese cyberbeveiligingscertificeringsregelingen, met als doel de totstandbrenging van een digitale eengemaakte markt voor ICT-producten, -diensten en -processen.

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

Artikel 47

Het voortschrijdend werkprogramma van de Unie voor Europese cyberbeveiligingscertificering

1. De Commissie publiceert een voortschrijdend werkprogramma van de Unie voor Europese cyberbeveiligingscertificering („het voortschrijdend werkprogramma van de Unie") met strategische prioriteiten voor toekomstige Europese cyberbeveiligingscertificeringsregelingen.

2. Het voortschrijdend werkprogramma van de Unie omvat met name een lijst van ICT-producten, -diensten en -processen of categorieën daarvan die kunnen worden opgenomen in het toepassingsgebied van een Europese cyberbeveiligingscertificeringsregeling.

3. De opname van specifieke ICT-producten, -diensten en -processen of categorieën daarvan in het voortschrijdend werkprogramma van de Unie geschiedt op een of meer van de volgende gronden:

a) de beschikbaarheid en ontwikkeling van nationale cyberbeveiligingscertificeringsregelingen voor een specifieke categorie ICT-producten, -diensten of -processen, en met name ten aanzien van het risico op versnippering;

b) relevant recht en beleid ter zake van de Unie of de lidstaten;

c) marktvraag;

d) ontwikkelingen in het cyberdreigingslandschap;

e) verzoek om opstelling van een specifieke potentiële regeling door de EGC.

4. De Commissie houdt terdege rekening met de adviezen over het ontwerp van voortschrijdend werkprogramma van de Unie die zijn uitgebracht door de EGC en de Groep van belanghebbenden bij cyberbeveiligingscertificering.

5. Het eerste voortschrijdend werkprogramma van de Unie wordt uiterlijk op 28 juni 2020 bekendgemaakt. Het voortschrijdend werkprogramma van de Unie wordt ten minste eens in de drie jaar, en wanneer dat nodig is vaker, bijgewerkt.

Artikel 48

Verzoek om een Europese cyberbeveiligingscertificeringsregeling

1. De Commissie kan Enisa verzoeken een potentiële regeling) op te stellen of een bestaande Europese cyberbeveiligingscertificeringsregeling te herzien op basis van het voortschrijdend werkprogramma van de Unie.

2. In naar behoren gemotiveerde gevallen kan de Commissie of de EGC Enisa verzoeken een potentiële regeling op te stellen of een bestaande Europese cyberbeveiligingscertificeringsregeling te herzien die niet is opgenomen in het voortschrijdend werkprogramma van de Unie. Het voortschrijdend werkprogramma van de Unie wordt dienovereenkomstig gewijzigd.

Artikel 49

Opstelling, vaststelling en herziening van een Europese cyberbeveiligingscertificeringsregeling

1. Naar aanleiding van een verzoek van de Commissie overeenkomstig artikel 48 bereidt Enisa een potentiële regeling voor die voldoet aan de in de artikelen 51, 52 en 54 bepaalde voorschriften.

2. Naar aanleiding van een verzoek van de EGC overeenkomstig artikel 48, lid 2, kan Enisa een potentiële regeling opstellen die voldoet aan de in de artikelen 51, 52 en 54 bepaalde eisen. Indien Enisa een dergelijk verzoek afwijst, motiveert het zijn afwijzing. Een besluit tot afwijzing van een dergelijk verzoek wordt genomen door de raad van bestuur.

3. Bij de opstelling van een potentiële regeling, raadpleegt Enisa door middel van een formele, open, transparante en inclusieve raadplegingsprocedure alle betrokken partijen.

4. Voor elke potentiële regeling stelt Enisa overeenkomstig artikel 20, lid 4, een ad-hocwerkgroep in, met het doel Enisa van specifiek advies en expertise te voorzien.

5. Enisa werkt nauw samen met de EGC. De EGC verleent Enisa bijstand en deskundig advies met betrekking tot de opstelling van de potentiële regeling en brengt over de potentiële regeling advies uit.

6. Enisa houdt zo veel mogelijk rekening met het advies van de EGC voordat de overeenkomstig de leden 3, 4 en 5 opgestelde potentiële regeling aan de Commissie wordt toegezonden. Het advies van de EGC is niet bindend en het ontbreken daarvan belet Enisa niet de potentiële regeling aan de Commissie toe te zenden.

7. Op basis van de door Enisa opgestelde potentiële regeling kan de Commissie uitvoeringshandelingen vaststellen om te voorzien in een Europese cyberbeveiligingscertificeringsregeling voor ICT-producten, -diensten en -processen die voldoen aan de in de artikelen 51, 52 en 54 bepaalde voorschriften. Die uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 66, lid 2, bedoelde onderzoeksprocedure.

8. Enisa evalueert ten minste om de vijf jaar elke vastgestelde Europese cyberbeveiligingscertificeringsregeling en houdt daarbij rekening met de feedback die het ontvangt van belanghebbenden. Indien nodig kan de Commissie of de EGC Enisa verzoeken de procedure te beginnen voor het ontwikkelen van een herziene potentiële regeling overeenkomstig de artikel 48 en dit artikel.

Artikel 50

Website over Europese cyberbeveiligingscertificeringsregelingen

1. Enisa beheert een specifieke website met informatie over, en bekendmaking van, Europese cyberbeveiligingscertificeringsregelingen, Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen, met inbegrip van informatie inzake Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen die niet langer geldig, ingetrokken of verstreken zijn, en inzake het register voor links naar overeenkomstig artikel 55 verstrekte informatie over cyberbeveiliging.

2. Waar van toepassing staan op de in lid 1 bedoelde website ook de nationale cyberbeveiligingscertificeringsregelingen die zijn vervangen door een Europese cyberbeveiligingscertificeringsregeling.

Artikel 51

Beveiligingsdoelstellingen van Europese cyberbeveiligingscertificeringsregelingen

De opzet van een Europese cyberbeveiligingscertificeringsregelingen is van dien aard dat, voor zover van toepassing, ten minste de volgende beveiligingsdoelstellingen worden verwezenlijkt:

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

b) opgeslagen, doorgegeven of anderszins verwerkte gegevens worden gedurende het gehele proces en de gehele levensduur van het ICT-product, de ICT-dienst of het ICT-proces beschermd tegen onbedoelde of onbevoegde vernietiging, verlies of wijziging, of gebrekkige beschikbaarheid;

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

d) afhankelijkheid en kwetsbaarheden worden opgespoord en, indien gekend, gedocumenteerd;

e) er wordt geregistreerd op welk tijdstip en door wie gegevens, diensten of functies zijn ingezien, gebruikt of anderszins verwerkt;

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

g) er wordt geverifieerd dat ICT-producten, -diensten en -processen geen bekende kwetsbaarheden bevatten;

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

i) ICT-producten, -diensten en -processen zijn door standaardinstellingen en door ontwerp veilig;

j) ICT-producten, -diensten en -processen worden geleverd met actuele software en hardware die geen algemeen bekende kwetsbaarheden bevatten, en met mechanismen voor beveiligde updates.

Artikel 52

Zekerheidsniveaus van Europese cyberbeveiligingscertificeringsregelingen

1. In een Europese cyberbeveiligingscertificeringsregeling kunnen voor ICT-producten, -diensten en -processen een of meer van de volgende zekerheidsniveaus worden gespecificeerd: „basis", „substantieel" of „hoog". Het zekerheidsniveau staat in verhouding tot het niveau van risico dat verbonden is aan het beoogde gebruik van een ICT-product, -dienst of -proces, wat betreft de waarschijnlijkheid en de gevolgen van een incident.

2. In Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen wordt verwezen naar een zekerheidsniveau dat staat aangegeven in de Europese cyberbeveiligingscertificeringsregeling uit hoofde waarvan het Europese cyberbeveiligingscertificaat of de EU-conformiteitsverklaring is afgegeven.

3. In de betrokken Europese cyberbeveiligingscertificeringsregeling worden de overeenkomstige beveiligingsvoorschriften voor elk zekerheidsniveau bepaald, waaronder de overeenkomstige beveiligingsfuncties en de overeenkomstige grondigheid en diepgang van de evaluatie waaraan dat ICT-product, die ICT-dienst of dat ICT-proces wordt onderworpen.

4. Het certificaat of de EU-conformiteitsverklaring geeft de daaraan gerelateerde technische specificaties, normen en procedures, waaronder technische controles, weer, welke tot doel hebben het risico van cyberbeveiligingsincidenten te verminderen of die incidenten te voorkomen.

5. Een Europees cyberbeveiligingscertificaat of EU-conformiteitsverklaring voor het zekerheidsniveau „basis" biedt de zekerheid dat de ICT-producten, -diensten en -processen voldoen aan de, waarvoor dat certificaat of die EU-conformiteitsverklaring is afgegeven, de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op het niveau dat bedoeld is om de bekende basisrisico's van cyberincidenten en cyberaanvallen tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste een toetsing van technische documenten. Indien een dergelijke toetsing niet geschikt is, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.

6. Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau „substantieel", biedt de zekerheid dat de ICT-producten, -diensten en -processen voldoen waarvoor dat certificaat is afgegeven aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende cyberbeveiligingsrisico's, en het risico op cyberincidenten en cyberaanvallen door actoren met beperkte vaardigheden en middelen, tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste het volgende: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, en testen of bij de ICT-producten, -diensten of -processen de benodigde beveiligingsfuncties correct worden toegepast. Indien dergelijke evaluatiewerkzaamheden niet geschikt zijn, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.

7. Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau „hoog", biedt de zekerheid dat de ICT-producten, -diensten en -processen waarvoor dat certificaat is afgegeven voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken.

De te ondernemen evaluatiewerkzaamheden behelzen ten minste het volgende: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, testen of bij de ICT-producten, -diensten of -processen 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. Indien dergelijke evaluatiewerkzaamheden niet geschikt zijn, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.

8. In een Europese cyberbeveiligingscertificeringsregeling kunnen meerdere evaluatieniveaus worden aangegeven, afhankelijk van de grondigheid en de diepgang van de gebruikte evaluatiemethodologie. Elk evaluatieniveau komt overeen met één van de zekerheidsniveaus en wordt door middel van een passende combinatie van zekerheidscomponenten omschreven.

Artikel 53

Conformiteitszelfbeoordeling

1. In een Europese cyberbeveiligingscertificeringsregeling mag worden bepaald dat een conformiteitszelfbeoordeling uitsluitend onder de verantwoordelijkheid van de fabrikant of aanbieder van ICT-producten, -diensten of -proces wordt uitgevoerd. Conformiteitsbeoordelingen worden uitsluitend toegestaan voor ICT-producten, -diensten en -processen met een laag risico of voor Europese cyberbeveiligingscertificeringsregelingen met zekerheidsniveau „basis".

2. De fabrikant of aanbieder van ICT-producten, -diensten of -processen kan een EU-conformiteitsverklaring 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, -diensten of -processen verantwoordelijkheid voor de conformiteit van het ICT-product, de ICT-dienst of het ICT-proces met de in die regeling bepaalde voorschriften.

3. De fabrikant of aanbieder van ICT-producten, -diensten of -processen stelt de EU-conformiteitsverklaring, de technische documenten en alle andere relevante informatie over de conformiteit van de ICT-producten of ICT-diensten met een regeling ter beschikking van de in artikel 58, lid 1, bedoelde nationale cyberbeveiligingscertificeringsautoriteit gedurende de termijn die is vastgesteld in de betrokken Europese cyberbeveiligingscertificeringsregeling. Aan de nationale cyberbeveiligingscertificeringsautoriteit en aan Enisa wordt een kopie van de EU-conformiteitsverklaring voorgelegd.

4. De afgifte van een EU-conformiteitsverklaring geschiedt op basis van vrijwilligheid, tenzij in de wetgeving van de Unie of de lidstaten anders is bepaald.

5. EU-conformiteitsverklaringen worden in alle lidstaten erkend.

Artikel 54

Elementen van Europese cyberbeveiligingscertificeringsregelingen

1. Een Europese cyberbeveiligingscertificeringsregeling omvat ten minste de volgende elementen:

a) het onderwerp en het toepassingsgebied van de certificeringsregeling, met inbegrip van het type of de categorieën ICT-producten, -diensten en -processen die eronder vallen;

b) een duidelijke beschrijving van het doel van de regeling en van de wijze waarop de geselecteerde normen, evaluatiemethoden en zekerheidsniveaus beantwoorden aan de behoeften van de beoogde gebruikers van de regeling.

c) een vermelding van de internationale, Europese of nationale norm die bij de evaluatie wordt gevolgd of, indien dergelijke normen niet beschikbaar of geschikt zijn, een vermelding van de technische specificaties die voldoen aan de in bijlage II bij Verordening (EU) nr. 1025/2012 bepaalde voorschriften, of, indien dergelijke specificaties niet beschikbaar zijn, de technische specificaties of andere cyberbeveiligingsvoorschriften die in de Europese cyberbeveiligingscertificeringsregelingen zijn omschreven;

d) indien van toepassing, één of meer zekerheidsniveaus;

e) een vermelding of conformiteitszelfbeoordeling is toegestaan uit hoofde van de regeling;

f) indien van toepassing, specifieke of aanvullende voorschriften voor conformiteitsbeoordelingsinstanties, om te garanderen dat zij beschikken over de technische bekwaamheid om de cyberbeveiligingsvoorschriften te evalueren;

g) de specifieke evaluatiecriteria en -methoden, met inbegrip van soorten evaluaties, die worden gebruikt om aan te tonen dat de in artikel 51 genoemde beveiligingsdoelstellingen worden verwezenlijkt;

h) indien van toepassing, de door een aanvrager aan de conformiteitsbeoordelingsinstanties te verstrekken of anderszins beschikbaar te stellen informatie die nodig is voor certificering;

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

j) de regels voor het toezicht op de conformiteit van ICT-producten, -diensten en -processen van de Europese cyberbeveiligingscertificaten of van de EU-conformiteitsverklaringen, met inbegrip van mechanismen om aan te tonen dat de vermelde cyberbeveiligingsvoorschriften nog altijd worden nageleefd;

k) indien van toepassing, de voorwaarden voor de afgifte, handhaving, voortzetting en vernieuwing van een Europese cyberbeveiligingscertificaat, evenals de voorwaarden voor uitbreiding of beperking van het toepassingsgebied van de certificering;

l) regels over de gevolgen voor ICT-producten, -diensten en -processen die zijn gecertificeerd of waarvoor een EU-conformiteitsverklaring is afgegeven, maar die niet voldoen aan de voorschriften van de regeling;

m) regels over de wijze waarop voorheen onopgemerkte kwetsbaarheden in de cyberbeveiliging van ICT-producten, -diensten en -processen moeten worden gemeld en aangepakt;

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

o) een overzicht van nationale of internationale cyberbeveiligingscertificeringsregelingen die betrekking hebben op hetzelfde type of dezelfde categorieën ICT-producten, -diensten en -processen, beveiligingsvoorschriften, evaluatiecriteria en -methoden en zekerheidsniveaus;

p) de inhoud en vorm van de af te geven Europees cyberbeveiligingscertificaten en EU-conformiteitsverklaringen;

q) de beschikbaarheidstermijn van de EU-conformiteitsverklaring, de technische documentatie en alle andere relevante informatie die door de fabrikant of aanbieder van ICT-producten, -diensten of -processen ter beschikking moet worden gesteld;

r) de maximale geldigheidsduur van Europees cyberbeveiligingscertificaten die uit hoofde van de regeling zijn afgegeven;

s) het openbaarmakingsbeleid inzake uit hoofde van de regeling afgegeven, gewijzigde en ingetrokken Europees cyberbeveiligingscertificaten die zijn afgegeven;

t) voorwaarden voor de wederzijdse erkenning van certificeringsregelingen met derde landen;

u) indien van toepassing, regels met betrekking tot een door de regeling vastgesteld collegialetoetsingsmechanisme voor autoriteiten of instanties die krachtens artikel 56, lid 6, Europese cyberbeveiligingscertificaten afgeven met zekerheidsniveau „hoog". Een dergelijk mechanisme doet geen afbreuk aan de in artikel 59 bedoelde collegiale toetsing;

v) vormen en procedures waaraan de fabrikanten of aanbieders van ICT-producten, -diensten of -processen zich moeten houden bij de verstrekking en actualisering van de aanvullende informatie over cyberbeveiliging overeenkomstig artikel 55.

2. De specifieke eisen van de Europese cyberbeveiligingscertificeringsregeling moeten in overeenstemming zijn met de toepasselijke wettelijke voorschriften, met name voorschriften die voortvloeien uit geharmoniseerd Unierecht.

3. Indien een specifieke rechtshandeling van de Unie daarin voorziet, kan een certificaat of een EU-conformiteitsverklaring op grond van een Europese cyberbeveiligingscertificeringsregeling worden gebruikt om het vermoeden van conformiteit met de voorschriften van die rechtshandeling aan te tonen.

4. Bij ontstentenis van geharmoniseerd Unierecht, kan in nationaal recht ook worden bepaald dat een Europese cyberbeveiligingscertificeringsregeling kan worden gebruikt om het vermoeden van conformiteit met de wettelijke voorschriften vast te stellen.

Artikel 55

Aanvullende cyberbeveiligingsinformatie voor gecertificeerde ICT-producten, -diensten en -processen

1. De fabrikant of aanbieder van gecertificeerde ICT-producten, -diensten en -processen of van ICT-producten, -diensten en -processen waarvoor een EU-conformiteitsverklaring is afgegeven maakt de hierna genoemde aanvullende cyberbeveiligingsinformatie openbaar:

a) richtsnoeren en aanbevelingen om eindgebruikers te helpen met de beveiligde configuratie, installatie, inzet, exploitatie en onderhoud van de ICT-producten of -diensten;

b) de periode gedurende welke beveiligingsondersteuning zal worden aangeboden aan eindgebruikers, met name wat betreft de beschikbaarheid van actualiseringen in verband met cyberbeveiliging;

c) contactgegevens van de fabrikant of aanbieder en aanvaarde methoden voor het ontvangen, van eindgebruikers en beveiligingsonderzoekers, van kwetsbaarheidsinformatie;

d) een verwijzing naar online registers van openbaar gemaakte kwetsbaarheden met betrekking tot het ICT-product, de ICT-dienst of het ICT-proces en met betrekking tot relevante cyberbeveiligingsadviesorganen.

2. De in lid 1 bedoelde informatie wordt in elektronische vorm beschikbaar gesteld, blijft beschikbaar en wordt indien nodig bijgewerkt, ten minste tot het verstrijken van het overeenkomstige Europese cyberbeveiligingscertificaat of de overeenkomstige EU-conformiteitsverklaring.

Artikel 56

Cyberbeveiligingscertificering

1. ICT-producten, -diensten en -processen die zijn gecertificeerd uit hoofde van een overeenkomstig artikel 49 vastgestelde Europese cyberbeveiligingscertificeringsregeling, worden geacht te voldoen aan de voorschriften van een dergelijke regeling.

2. De cyberbeveiligingscertificering geschiedt op basis van vrijwilligheid, tenzij in het recht van de Unie of de lidstaten anders is bepaald.

3. De Commissie beoordeelt regelmatig de efficiëntie en het gebruik van de vastgestelde Europese cyberbeveiligingscertificeringsregelingen en beoordeelt of er door middel van het relevante Unierecht een specifieke Europese cyberbeveiligingscertificeringsregeling verplicht moet worden gesteld om te zorgen voor een passend niveau van cyberbeveiliging van ICT-producten, -diensten en -processen in de Unie en om de werking van de interne markt te verbeteren. De eerste zulke beoordeling vindt uiterlijk op 31 december 2023 plaats en daaropvolgende beoordelingen vinden ten minste om de twee jaar daarna plaats.

Op basis van de resultaten van die beoordelingen stelt de Commissie een lijst op van de onder een bestaande certificeringsregeling vallende ICT-producten, -diensten en -processen die gedekt moeten worden door een verplichte certificeringsregeling.

De Commissie concentreert zich prioritair op de in bijlage II bij Richtlijn (EU) 2016/1148 vermelde sectoren, die uiterlijk twee jaar na de vaststelling van de eerste Europese cyberbeveiligingscertificeringsregeling moeten worden beoordeeld.

Bij de voorbereiding van de beoordeling moet de Commissie:

a) rekening houden met de gevolgen die de maatregelen hebben voor de fabrikanten of aanbieders van zulke ICT-producten, -diensten of -processen en voor de gebruikers in termen van de kosten van die maatregelen, evenals de maatschappelijke of economische voordelen die voortvloeien uit de verwachte betere beveiliging voor de beoogde ICT-producten, -diensten of -processen;

b) rekening houden met het bestaan en de uitvoering van relevant recht in de lidstaten en derde landen;

c) een open, transparant en inclusief overleg voeren met alle betrokken belanghebbenden en lidstaten;

d) rekening houden met eventuele uitvoeringstermijnen, overgangsmaatregelen en overgangstermijnen, in het bijzonder betreffende de mogelijke gevolgen van de maatregelen voor de fabrikanten of aanbieders van ICT- producten, -diensten en -processen, met inbegrip van kleine en middelgrote ondernemingen;

e) de snelste en efficiëntste wijze voorstellen waarop de overgang van vrijwillige naar verplichte certificeringsregelingen moet worden uitgevoerd.

4. De in artikel 60 bedoelde conformiteitsbeoordelingsinstanties geven ingevolge dit artikel Europese cyberbeveiligingscertificaten voor zekerheidsniveau „basis" of „substantieel" af op basis van de criteria die zijn opgenomen in de op grond van artikel 49 door de Commissie vastgestelde Europese cyberbeveiligingscertificeringsregeling.

5. In afwijking van lid 4 en in naar behoren gemotiveerde gevallen kan een Europese cyberbeveiligingscertificeringsregeling erin voorzien dat uit die regeling voortvloeiende Europees cyberbeveiligingscertificaten alleen door een overheidsinstantie kunnen worden afgegeven. Een dergelijke instantie is een van de volgende organen:

a) een in artikel 58, lid 1, bedoelde nationale cyberbeveiligingscertificeringsautoriteit, of

b) een overheidsorgaan dat als een conformiteitsbeoordelingsinstantie overeenkomstig artikel 60, lid 1, is geaccrediteerd.

6. Indien een op grond van artikel 49 vastgestelde Europese cyberbeveiligingscertificeringsregeling een zekerheidsniveau „hoog" voorschrijft, dient het Europees cyberbeveiligingscertificaat uit hoofde van die regeling uitsluitend te worden afgegeven door een nationale cyberbeveiligingscertificeringsautoriteit, of, in de volgende gevallen, door een conformiteitsbeoordelingsinstantie:

a) nadat de nationale cyberbeveiligingscertificeringsautoriteit elk door de conformiteitsbeoordelingsinstantie afgegeven individueel Europees cyberbeveiligingscertificaat heeft goedgekeurd, of

b) op basis van een algemene delegatie door de nationale cyberbeveiligingscertificeringsautoriteit van de taak tot afgifte van dergelijke Europese cyberbeveiligingscertificaten aan een conformiteitsbeoordelingsinstantie.

7. De natuurlijke of rechtspersoon die zijn ICT-producten, -diensten of -processen, aan de certificering onderwerpt, stelt aan de in artikel 58 bedoelde nationale cyberbeveiligingscertificeringsautoriteit, indien deze autoriteit het Europees cyberbeveiligingscertificaat afgeeft, of aan de in artikel 60 bedoelde conformiteitsbeoordelingsinstantie alle informatie ter beschikking die nodig is voor de uitvoering van de certificering.

8. De houder van een Europees cyberbeveiligingscertificaat stelt de instantie of het orgaan, bedoeld in lid 7, in kennis van kwetsbaarheden of onregelmatigheden in verband met de beveiliging van gecertificeerde ICT-producten, -diensten of -processen die achteraf zijn vastgesteld en die gevolgen kunnen hebben voor de naleving van de met de certificering verband houdende voorschriften. Die instantie of dat orgaan stuurt die informatie onverwijld door naar de betrokken nationale cyberbeveiligingscertificeringsautoriteit.

9. Een Europees cyberbeveiligingscertificaat wordt afgegeven voor de periode die is vastgesteld in de betrokken Europese cyberbeveiligingscertificeringsregeling en kan worden verlengd, mits nog steeds aan de desbetreffende voorschriften wordt voldaan.

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

Artikel 57

Nationale cyberbeveiligingscertificeringsregelingen en -certificaten

1. Onverminderd lid 3 van dit artikel hebben nationale cyberbeveiligingscertificeringsregelingen en de daaraan verbonden procedures voor de ICT-producten, -diensten en -processen die onder een Europese cyberbeveiligingscertificeringsregeling vallen, niet langer gevolgen vanaf de datum die wordt bepaald in de op grond van artikel 49, lid 7, vastgestelde uitvoeringshandeling. Nationale cyberbeveiligingscertificeringsregelingen en de daaraan verbonden procedures voor ICT-producten, -diensten en -processen die niet onder een Europese cyberbeveiligingscertificeringsregeling vallen, blijven bestaan.

2. De lidstaten voeren geen nieuwe nationale cyberbeveiligingscertificeringsregelingen in voor ICT-producten, -diensten en -processen die onder een van kracht zijnde Europese cyberbeveiligingscertificeringsregeling vallen.

3. Bestaande certificaten die op grond van nationale cyberbeveiligingscertificeringsregelingen waren afgegeven en onder een Europese cyberbeveiligingscertificeringsregeling vallen, blijven geldig tot hun vervaldatum.

4. Om versnippering van de interne markt te vermijden leggen de lidstaten elk voornemen voor de opstelling van nieuwe nationale cyberbeveiligingscertificeringsregelingen voor aan de Commissie en de EGC.

Artikel 58

Nationale cyberbeveiligingscertificeringsautoriteiten

1. Iedere lidstaat wijst één of meer nationale cyberbeveiligingscertificeringsautoriteiten op zijn grondgebied aan, of wijst, in onderlinge overeenstemming met een andere lidstaat, één of meer in die andere lidstaat gevestigde nationale cyberbeveiligingscertificeringsautoriteiten aan die verantwoordelijk zijn voor de toezichthoudende taken in de aanwijzende lidstaat.

2. Elke lidstaat stelt de Commissie in kennis van de identiteit van de aangewezen nationale cyberbeveiligingscertificeringsautoriteiten, wanneer een lidstaat meer dan één autoriteit aanwijst, geeft hij de Commissie ook informatie over de taken die aan elke van die autoriteiten zijn toegewezen.

3. Onverminderd artikel 56, lid 5, onder a), en artikel 56, lid 6, is elke nationale cyberbeveiligingscertificeringsautoriteit op het vlak van haar organisatie, financieringsbeslissingen, rechtsstructuur en besluitvorming onafhankelijk van de entiteiten waarop zij toezicht houdt.

4. De lidstaten zorgen ervoor dat de werkzaamheden van de nationale cyberbeveiligingscertificeringsautoriteit met betrekking tot de afgifte van de in artikel 56, lid 5, onder a), en artikel 56, lid 6, bedoelde Europese cyberbeveiligingscertificaten strikt gescheiden zijn van de in dit artikel bedoelde toezichthoudende werkzaamheden en dat die werkzaamheden onafhankelijk van elkaar worden verricht.

5. De lidstaten zorgen ervoor dat de nationale cyberbeveiligingscertificeringsautoriteiten over voldoende middelen beschikken om hun bevoegdheden uit te oefenen en hun taken op een doeltreffende en doelmatige wijze uit te voeren.

6. Met het oog op de doeltreffende uitvoering van deze verordening is het passend dat nationale cyberbeveiligingscertificeringsautoriteiten op een actieve, doeltreffende, efficiënte en betrouwbare manier deelnemen aan de EGC.

7. Nationale cyberbeveiligingscertificeringsautoriteiten

a) zien toe op en handhaven op grond van artikel 54, lid 1, onder j), in Europese cyberbeveiligingscertificeringsregelingen opgenomen regels voor toezicht op de conformiteit van ICT-producten, -diensten en -processen met de voorschriften van de Europese cyberbeveiligingscertificaten die zijn afgegeven op hun respectieve grondgebieden, in samenwerking met andere betrokken markttoezichtautoriteiten;

b) monitoren de naleving door en handhaven de verplichtingen van de fabrikanten of aanbieders van ICT-producten, -diensten en -processen die gevestigd zijn op hun respectieve grondgebieden en conformiteitszelfbeoordelingen verrichten, en zien met name toe op de naleving en handhaving van de in artikel 53, leden 2 en 3, en in de overeenkomstige Europese cyberbeveiligingscertificeringsregeling bepaalde verplichtingen;

c) verlenen, onverminderd artikel 60, lid 3, bijstand en ondersteuning aan de nationale accreditatie-instanties bij de monitoring van en het toezicht op de werkzaamheden van de conformiteitsbeoordelingsinstanties voor de toepassing van deze verordening;

d) monitoren en houden toezicht op de werkzaamheden van de in artikel 56, lid 5, bedoelde openbare instanties;

e) laten, indien van toepassing, overeenkomstig artikel 60, lid 3, conformiteitsbeoordelingsinstanties toe en gaan over tot het beperken, opschorten of intrekken van bestaande toelatingen indien de conformiteitsbeoordelingsinstanties inbreuk maken op de in deze verordening neergelegde voorschriften;

f) behandelen klachten van natuurlijke of rechtspersonen over door de nationale cyberbeveiligingscertificeringsautoriteiten of overeenkomstig artikel 56, lid 6, door conformiteitsbeoordelingsinstanties afgegeven Europese cyberbeveiligingscertificaten, of over uit hoofde van artikel 53 afgegeven EU-conformiteitsverklaringen, en zij onderzoeken, voor zover passend, de inhoud van dergelijke klachten en stellen de klager binnen een redelijke termijn in kennis van de voortgang en het resultaat van het onderzoek;

g) stellen een samenvattend jaarverslag op over de uit hoofde van de punten b), c) en d) van dit lid of overeenkomstig lid 8 ondernomen werkzaamheden voor Enisa en de EGC;

h) werken samen met andere nationale cyberbeveiligingscertificeringautoriteiten of andere overheidsinstanties, onder meer door informatie uit te wisselen over de mogelijke niet-conformiteit van ICT-producten, -diensten en -processen met de voorschriften van deze verordening of met de voorschriften van specifieke Europese cyberbeveiligingscertificeringsregelingen, en

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

8. Elke nationale cyberbeveiligingscertificeringautoriteit beschikt ten minste over de volgende bevoegdheden:

a) het verzoeken van conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen om alle informatie te verstrekken die zij nodig heeft voor de uitvoering van haar taken;

b) het verrichten van onderzoeken, in de vorm van audits, naar conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen om hun naleving van deze titel te verifiëren;

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

d) het verkrijgen van toegang tot de gebouwen en terreinen van een conformiteitsbeoordelingsinstantie of houders van Europese cyberbeveiligingscertificaten voor het verrichten van onderzoeken overeenkomstig het procesrecht van de Unie of lidstaat;

e) het overeenkomstig nationaal recht intrekken van door de nationale cyberbeveiligingscertificeringsautoriteit of overeenkomstig artikel 56, lid 6, door conformiteitsbeoordelingsinstanties afgegeven Europese cyberbeveiligingscertificaten die niet voldoen aan deze verordening of een Europese cyberbeveiligingscertificeringsregeling;

f) de oplegging overeenkomstig nationaal recht van in artikel 65 bedoelde sancties en het eisen dat onmiddellijk een einde wordt gemaakt aan de niet-nakoming van de verplichtingen van deze verordening.

9. Nationale cyberbeveiligingscertificeringsautoriteiten 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 vraagstukken met betrekking tot de cyberbeveiliging van ICT-producten, -diensten en -processen.

Artikel 59

Collegiale toetsing

1. Met het oog op de verwezenlijking van gelijkwaardige normen in de hele Unie ten aanzien van Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen, worden nationale cyberbeveiligingscertificeringsautoriteiten onderworpen aan collegiale toetsing.

2. De collegiale toetsing wordt verricht op basis van deugdelijke en transparante toetsingscriteria en -procedures, met name op het gebied van structuur-, personeels- en procesvereisten, vertrouwelijkheid en klachten.

3. Collegiale toetsing beoordeelt:

a) indien van toepassing, de vraag of de werkzaamheden van de nationale cyberbeveiligingscertificeringsautoriteiten met betrekking tot de in artikel 56, lid 5, onder a), en artikel 56, lid 6, bedoelde afgifte van Europese cyberbeveiligingscertificaten strikt gescheiden zijn van de in artikel 58 bepaalde toezichthoudende werkzaamheden en of die werkzaamheden onafhankelijk van elkaar worden verricht;

b) de procedures voor het toezicht op en de handhaving van de regels voor het toezicht op de conformiteit van ICT-producten, -diensten en processen met Europese cyberbeveiligingscertificaten op grond van artikel 58, lid 7, onder a);

c) de procedures voor de monitoring en handhaving van de verplichtingen van fabrikanten en aanbieders van ICT-producten, -diensten of -processen op grond van artikel 58, lid 7, onder b);

d) de procedures voor het monitoren en toestaan van en het toezien op de werkzaamheden van de conformiteitsbeoordelingsinstanties;

e) indien van toepassing, de vraag of het personeel van autoriteiten of instanties die op grond van artikel 56, lid 6, certificaten afgeven voor zekerheidsniveau „hoog", over de passende expertise beschikt.

4. Collegiale toetsingen worden verricht door ten minste twee nationale cyberbeveiligingscertificeringsautoriteiten van andere lidstaten en de Commissie en worden ten minste om de vijf jaar uitgevoerd. Enisa mag aan de collegiale toetsing deelnemen.

5. De Commissie kan uitvoeringshandelingen vaststellen met een plan voor collegiale toetsingen dat een periode van ten minste vijf jaar beslaat, waarin criteria worden vastgesteld voor de samenstelling van het collegialetoetsingsteam, de bij de collegiale toetsing gebruikte methode, en het tijdschema, de frequentie en andere taken die daarmee verband houden. Bij de vaststelling van die uitvoeringshandelingen houdt de Commissie terdege rekening met de zienswijzen van de EGC. Die uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 66, lid 2, bedoelde onderzoeksprocedure.

6. De uitkomsten van de collegiale toetsing worden onderzocht door de EGC, die een overzicht opstelt dat openbaar kan worden gemaakt en die, indien nodig, richtsnoeren of aanbevelingen uitvaardigt over door de betrokken entiteiten te ondernemen acties of te nemen maatregelen.

Artikel 60

Conformiteitsbeoordelingsinstanties

1. De conformiteitsbeoordelingsinstanties worden door de op grond van Verordening (EG) nr. 765/2008 aangestelde nationale accreditatie-instantie geaccrediteerd. Dergelijke accreditatie wordt enkel verstrekt indien de conformiteitsbeoordelingsinstantie aan de in de bijlage bij deze verordening vastgestelde voorschriften voldoet.

2. Indien op grond van artikel 56, lid 5, onder a), en artikel 56, lid 6, door een nationale cyberbeveiligingscertificeringsautoriteit een Europees cyberbeveiligingscertificaat wordt afgegeven, wordt de certificeringsinstantie van de nationale cyberbeveiligingscertificeringsautoriteit op grond van lid 1 van dit artikel geaccrediteerd als een conformiteitsbeoordelingsinstantie.

3. Indien in Europese cyberbeveiligingscertificeringregelingen op grond van artikel 54, lid 1, onder f), specifieke of aanvullende eisen zijn bepaald, worden alleen conformiteitsbeoordelingsinstanties die aan die eisen voldoen door de nationale cyberbeveiligingscertificeringautoriteit toegestaan om taken uit hoofde van dergelijke regelingen uit te voeren.

4. De in lid 1 bedoelde accreditatie wordt aan conformiteitsbeoordelingsinstanties afgegeven voor een maximumperiode van vijf jaar en kan onder dezelfde voorwaarden worden verlengd, mits de conformiteitsbeoordelingsinstantie nog steeds aan de in dit artikel gestelde eisen voldoet. Nationale accreditatie-instanties nemen binnen een redelijke termijn alle passende maatregelen om de op grond van lid 1 afgegeven accreditatie van een conformiteitsbeoordelingsinstantie te beperken, op te schorten of in te trekken wanneer niet of niet meer aan de voorwaarden voor de accreditatie wordt voldaan of wanneer de conformiteitsbeoordelingsinstantie inbreuk maakt op deze verordening.

Artikel 61

Aanmelding

1. Voor elke Europese cyberbeveiligingscertificeringsregeling stellen de nationale cyberbeveiligingscertificeringautoriteiten de Commissie in kennis van de conformiteitsbeoordelingsinstanties die geaccrediteerd en, in voorkomend geval, overeenkomstig artikel 60, lid 3, gemachtigd zijn om Europese cyberbeveiligingscertificaten af te geven voor in artikel 52 bedoelde gespecificeerde zekerheidsniveaus. De nationale cyberbeveiligingscertificeringautoriteiten stellen de Commissie onverwijld in kennis van alle latere wijzigingen daarvan.

2. Eén jaar na de inwerkingtreding van een Europese cyberbeveiligingscertificeringsregeling maakt de Commissie in het *Publicatieblad van de Europese Unie* een lijst met de uit hoofde van die regeling aangemelde conformiteitsbeoordelingsinstanties bekend.

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 lijst van aangemelde conformiteitsbeoordelingsinstanties bekend.

4. Een nationale cyberbeveiligingscertificeringsautoriteit kan bij de Commissie een verzoek indienen om een door die autoriteit aangemelde conformiteitsbeoordelingsinstantie te verwijderen van de in lid 2 bedoelde lijst van aangemelde conformiteitsbeoordelingsinstanties. Binnen één maand vanaf de datum van ontvangst van het verzoek van de nationale cyberbeveiligingscertificeringsautoriteit maakt de Commissie de overeenkomstige wijzigingen van die lijst bekend in het *Publicatieblad van de Europese Unie*.

5. De Commissie kan uitvoeringshandelingen vaststellen om de omstandigheden, vormen en procedures van de in lid 1 van dit artikel bedoelde aanmeldingen vast te leggen. Die uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 66, lid 2, bedoelde onderzoeksprocedure.

Artikel 62

Europese Groep voor cyberbeveiligingscertificering

1. De Europese Groep voor cyberbeveiligingscertificering („de EGC") wordt opgericht.

2. De EGC bestaat uit vertegenwoordigers van nationale cyberbeveiligingscertificeringsautoriteiten of vertegenwoordigers van andere relevante nationale autoriteiten. Een lid van de EGC vertegenwoordigt niet meer dan twee lidstaten.

3. Belanghebbenden en relevante derde partijen kunnen worden uitgenodigd om de vergaderingen van de EGC bij te wonen en aan de werkzaamheden ervan deelnemen.

4. De EGC heeft de volgende taken:

a) advies en bijstand verlenen aan de Commissie in haar werkzaamheden om te zorgen voor een consistente uitvoering en toepassing van deze titel, met name met betrekking tot het voortschrijdend werkprogramma van de Unie, beleidsvraagstukken inzake cyberbeveiligingscertificering, de coördinatie van beleidsbenaderingen en de opstelling van Europese cyberbeveiligingscertificeringsregelingen;

b) bijstand en advies verlenen aan en samenwerken met Enisa bij de voorbereiding van een potentiële regeling op grond van artikel 49;

c) een advies uitbrengen over potentiële regelingen op grond van artikel 49;

d) Enisa verzoeken potentiële regelingen op te stellen op grond artikel 48, lid 2;

e) adviezen aan de Commissie uitbrengen met betrekking tot de instandhouding en herziening van bestaande Europese cyberbeveiligingscertificeringsregelingen;

f) de relevante ontwikkelingen op het gebied van cyberbeveiligingscertificering bestuderen en informatie en goede praktijken op het gebied van cyberbeveiligingscertificeringsregelingen uitwisselen;

g) de samenwerking tussen de nationale cyberbeveiligingscertificeringsautoriteiten voor uit hoofde van deze titel vergemakkelijken door middel van capaciteitsopbouw en informatie-uitwisseling, met name door de vaststelling van methoden voor de efficiënte uitwisseling van informatie over alle aangelegenheden die verband houden met cyberbeveiligingscertificering;

h) ondersteuning verlenen aan de uitvoering van collegialetoetsingsmechanismen overeenkomstig de regels die op grond van artikel 54, lid 1, onder u), in een Europese cyberbeveiligingscertificeringsregeling zijn vastgesteld;

i) de onderlinge afstemming van Europese cyberbeveiligingscertificeringsregelingen en internationaal erkende normen vergemakkelijken, onder andere door bestaande Europese cyberbeveiligingscertificeringsregelingen te herzien en waar nodig aanbevelingen te doen aan Enisa om betrekkingen met relevante internationale normalisatieorganisaties aan te knopen om tekortkomingen of hiaten in beschikbare internationaal erkende normen aan te pakken.

5. De Commissie zit, bijgestaan door Enisa, de EGC voor en verzorgt het secretariaat van de EGC overeenkomstig artikel 8, lid 1, onder e).

Artikel 63

Recht om een klacht in te dienen

1. Natuurlijke en rechtspersonen hebben het recht een klacht in te dienen bij de afgever van een Europees cyberbeveiligingscertificaat of, wanneer de klacht verband houdt met een Europees cyberbeveiligingscertificaat dat is afgegeven door een conformiteitsbeoordelingsinstantie handelend overeenkomstig artikel 56, lid 6), bij de bevoegde nationale cyberbeveiligingscertificeringsautoriteit.

2. De autoriteit of instantie waarbij de klacht is ingediend stelt de klager in kennis van de voortgang van de procedure en van het genomen besluit, alsmede van de mogelijkheid van een doeltreffende voorziening in rechte als bedoeld in artikel 64.

Artikel 64

Recht op een doeltreffende voorziening in rechte

1. Onverminderd bestuurlijke of buitengerechtelijke rechtsmiddelen hebben natuurlijke en rechtspersonen recht op een doeltreffende voorziening in rechte met betrekking tot:

a) door de autoriteit of instantie bedoeld in artikel 63, lid 1, genomen besluiten, onder meer, in voorkomend geval, met betrekking tot onjuiste afgifte, nalaten van afgifte of erkenning van een Europees cyberbeveiligingscertificaat dat door die natuurlijke en rechtspersonen wordt gehouden;

b) het verzuim om gevolg te geven aan een klacht die is ingediend bij de in artikel 63, lid 1, bedoelde autoriteit of instantie.

2. Procedures op grond van dit artikel worden ingesteld bij een gerechtelijke instantie van de lidstaat waar de autoriteit of instantie jegens welke de voorziening in rechte wordt verzocht, is gevestigd.

Artikel 65

Sancties

De lidstaten stellen voorschriften vast betreffende sancties voor inbreuken op deze titel en voor inbreuken op Europese cyberbeveiligingscertificeringsregelingen en treffen alle nodige maatregelen om ervoor te zorgen dat die sancties worden toegepast. De vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend. De lidstaten stellen de Commissie onverwijld van die voorschriften en die maatregelen in kennis alsmede van alle eventuele latere wijzigingen ervan.

TITEL IV

SLOTBEPALINGEN

Artikel 66

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 67

Evaluatie en toetsing

1. Uiterlijk op 28 juni 2024, en vervolgens om de vijf jaar evalueert de Commissie het effect, de doeltreffendheid en de efficiëntie van Enisa, zijn werkmethoden, de eventuele noodzaak om het mandaat van Enisa te wijzigen en de financiële gevolgen van een dergelijke wijziging. Bij de evaluatie wordt rekening gehouden met feedback die aan Enisa is gegeven naar aanleiding van zijn activiteiten. Als de Commissie van oordeel is dat het voortbestaan van Enisa niet langer gerechtvaardigd is in het licht van de hem toegewezen doelstellingen, mandaat en taken, kan zij voorstellen om de bepalingen van deze verordening die betrekking hebben op Enisa, te wijzigen.

2. Bij de evaluatie wordt ook gekeken naar de gevolgen, de doeltreffendheid en de efficiëntie van de bepalingen van titel III van deze verordening met betrekking tot de doelstellingen om een adequaat cyberbeveiligingsniveau van ICT-producten, -diensten en -processen in de Unie te waarborgen en de werking van de interne markt te verbeteren.

3. Bij de evaluatie wordt beoordeeld of er voor cyberbeveiliging essentiële voorschriften voor toegang tot de interne markt nodig zijn om te voorkomen dat ICT-producten, -diensten en -processen die niet aan de basisvoorschriften inzake cyberbeveiliging voldoen, de markt van de Unie binnenkomen.

4. Uiterlijk op 28 juni 2024 en vervolgens om de vijf jaar stuurt de Commissie een verslag over de evaluatie tezamen met haar conclusies toe aan het Europees Parlement, de Raad en de raad van bestuur. De bevindingen van dat evaluatieverslag worden openbaar gemaakt.

Artikel 68

Intrekking en opvolging

1. Verordening (EU) nr. 526/2013 wordt met ingang van 27 juni 2019 ingetrokken.

2. Verwijzingen naar Verordening (EG) nr. 526/2013 en naar Enisa gelden als verwijzingen naar deze verordening en naar Enisa, zoals bij deze verordening opgericht.

3. Enisa zoals bij de onderhavige verordening opgericht, volgt Enisa zoals bij Verordening (EG) nr. 526/2013 opgericht, op wat alle eigendommen, overeenkomsten, juridische verplichtingen, arbeidsovereenkomsten, financiële verbintenissen en aansprakelijkheden betreft. Alle overeenkomstig Verordening (EU) nr. 526/2013 vastgestelde besluiten van de raad van bestuur en het dagelijks bestuur blijven geldig, mits zij stroken met deze verordening.

4. Enisa wordt opgericht voor onbepaalde tijd met ingang van 27 juni 2019.

5. De overeenkomstig artikel 24, lid 4, van Verordening (EU) nr. 526/2013 aangewezen uitvoerend directeur blijft in functie en oefent de taken uit van de uitvoerend directeur als bedoeld in artikel 20 van deze verordening voor het resterende gedeelte van de ambtstermijn van de uitvoerend directeur. De andere voorwaarden van zijn of haar contract blijven ongewijzigd.

6. De overeenkomstig artikel 6 van Verordening (EU) nr. 526/2013 aangewezen leden van de raad van bestuur en hun plaatsvervangers blijven in functie en oefenen de taken uit van de raad van bestuur als bedoeld in artikel 15 van deze verordening voor het resterende gedeelte van hun ambtstermijn.

Artikel 69

Inwerkingtreding

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

2. De artikelen 58, 60, 61, 63, 64 en 65 zijn van toepassing met ingang van 28 juni 2021.

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

Gedaan te Straatsburg, 17 april 2019.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
A. TAJANI	G. CIAMBA

BIJLAGE

VEREISTEN WAARAAN CONFORMITEITSBEOORDELINGSINSTANTIES MOETEN VOLDOEN

Conformiteitsbeoordelingsinstanties die wensen te worden geaccrediteerd, moeten aan de volgende vereisten 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, -diensten of -processen.

3. Een instantie die behoort tot een branche- of beroepsorganisatie die ondernemingen vertegenwoordigt die betrokken zijn bij het ontwerpen, vervaardigen, leveren, monteren, gebruiken of onderhouden van de door haar beoordeelde ICT-producten, -diensten of -processen, kan als conformiteitsbeoordelingsinstantie worden beschouwd op voorwaarde dat haar onafhankelijkheid en de afwezigheid van belangenconflicten zijn aangetoond.

4. De conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden en personen die de conformiteitsbeoordelingstaken verrichten, mogen niet de ontwerper, fabrikant, leverancier, installateur, koper, eigenaar, gebruiker of onderhouder zijn van het ICT-product, -dienst of -proces dat of die wordt beoordeeld, noch de gemachtigde van één van die partijen. Dat verbod vormt geen beletsel voor het gebruik van de beoordeelde ICT-producten die nodig zijn voor de activiteiten van de conformiteitsbeoordelingsinstantie of voor het gebruik van dergelijke ICT-producten voor persoonlijke doeleinden.

5. De conformiteitsbeoordelingsinstantie, hun hoogste leidinggevenden en personen die de conformiteitsbeoordeling verrichten, zijn noch rechtstreeks noch als vertegenwoordiger van de betrokken partijen betrokken bij het ontwerpen, vervaardigen of bouwen, op de markt brengen, installeren, gebruiken of onderhouden van de ICT-producten, -diensten of -processen die worden beoordeeld. De conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden en personen die de conformiteitsbeoordelingstaken verrichten geen activiteiten die hun onafhankelijk oordeel of hun integriteit met betrekking tot hun conformiteitsbeoordelingswerkzaamheden, in het gedrang kunnen brengen. Dat verbod geldt met name voor adviesdiensten.

6. Indien een conformiteitsbeoordelingsinstantie in eigendom is van of wordt geëxploiteerd door een overheidsinstantie, worden de onafhankelijkheid en de afwezigheid van belangenconflicten tussen de nationale cyberbeveiligingscertificeringsautoriteit en de conformiteitsbeoordelingsinstantie gewaarborgd en gedocumenteerd.

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

8. Conformiteitsbeoordelingsinstanties en hun personeel voeren conformiteitsbeoordelingswerkzaamheden 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 conformiteitsbeoordelingswerkzaamheden zouden kunnen beïnvloeden, in het bijzonder van of door personen of groepen van personen die belang hebben bij de resultaten van deze activiteiten.

9. Een conformiteitsbeoordelingsinstantie is in staat alle conformiteitsbeoordelingstaken te vervullen die haar krachtens deze verordening zijn toegewezen, ongeacht of die taken door de conformiteitsbeoordelingsinstantie zelf dan wel namens haar en onder haar verantwoordelijkheid worden verricht. Elke uitbesteding aan of raadpleging van extern personeel wordt naar behoren gedocumenteerd, brengt geen tussenpersonen met zich mee en geschiedt bij schriftelijke overeenkomst waarin onder meer de vertrouwelijkheid en belangenconflicten worden geregeld. De betrokken conformiteitsbeoordelingsinstantie neemt de volledige verantwoordelijkheid voor de verrichte taken.

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

    a) personeel met technische kennis en voldoende geschikte ervaring om de conformiteitsbeoordelingstaken te verrichten;

    b) beschrijvingen van de procedures voor de uitvoering van de conformiteitsbeoordeling, om de transparantie en de mogelijkheid tot reproductie van die procedures te waarborgen. Zij beschikt over een gepast beleid en geschikte procedures die een onderscheid maken tussen taken die zij als op grond van artikel 61 aangemelde instantie verricht en haar andere activiteiten;

c) procedures voor de uitoefening van haar werkzaamheden, 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 het of de betrokken ICT-product, -dienst of -proces en het massa- of seriële karakter van het productieproces.

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

12. De voor de uitvoering van de conformiteitsbeoordelingswerkzaamheden verantwoordelijke personen:

a) hebben een gedegen technische en beroepsopleiding gevolgd die alle relevante conformiteitsbeoordelingswerkzaamheden omvat;

b) beschikken over toereikende kennis van de eisen inzake de conformiteitsbeoordelingen die ze verrichten en over voldoende bevoegdheid om die beoordelingen uit te voeren;

c) beschikken over voldoende kennis van en inzicht in de toepasselijke eisen en testnormen;

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

13. De onpartijdigheid van de conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden, de voor de verrichting van de conformiteitsbeoordelingswerkzaamheden verantwoordelijke personen en eventuele onderaannemers wordt gegarandeerd.

14. De beloning van de hoogste leidinggevenden en van de voor de verrichting van de conformiteitsbeoordelingswerkzaamheden verantwoordelijke personen hangt niet af van het aantal uitgevoerde conformiteitsbeoordelingen of van de resultaten daarvan.

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

16. De conformiteitsbeoordelingsinstantie en haar personeel, comités, dochterondernemingen, onderaannemers en aanverwante instanties of het personeel van externe organisaties van een conformiteitsbeoordelingsinstantie zijn verplicht tot geheimhouding en zijn gebonden aan het beroepsgeheim ten aanzien van alle informatie waarvan zij kennisnemen bij de uitoefening van hun conformiteitsbeoordelingstaken uit hoofde van deze verordening of op grond van bepalingen van nationaal recht die aan deze verordening uitvoering geven, behalve wanneer bekendmaking wordt vereist door wetgeving van de Unie of de lidstaat waaronder zij vallen en behalve ten opzichte van de bevoegde autoriteiten van de lidstaat waarin de werkzaamheden plaatsvinden. Intellectuele eigendomsrechten worden beschermd. De conformiteitsbeoordelingsinstantie beschikt over gedocumenteerde procedures met betrekking tot de vereisten van dit punt.

17. Met uitzondering van punt 16 sluiten de voorschriften van deze bijlage op geen enkele wijze de uitwisseling uit van technische inlichtingen en regelgevingsrichtsnoeren tussen een conformiteitsbeoordelingsinstantie en een persoon die om certificering verzoekt of dat overweegt.

18. Conformiteitsbeoordelingsinstanties handelen overeenkomstig een reeks consistente, billijke en redelijke voorwaarden, met inachtneming van de belangen van kleine en middelgrote ondernemingen met betrekking tot vergoedingen.

19. Conformiteitsbeoordelingsinstanties voldoen aan de eisen van de toepasselijke norm die op grond van Verordening (EG) nr. 765/2008 is geharmoniseerd voor de accreditatie van conformiteitsbeoordelingsinstanties die ICT-producten, -diensten of -processen certificeren.

20. Conformiteitsbeoordelingsinstanties zorgen ervoor dat testlaboratoria die worden gebruikt voor conformiteitsbeoordelingen voldoen aan de eisen van de toepasselijke norm die op grond van Verordening (EG) nr. 765/2008 is geharmoniseerd voor de accreditatie van laboratoria die tests uitvoeren.