RICHTLIJNEN

RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD

van 14 december 2022

betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)

(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 de Europese Centrale Bank ([1]),

Gezien het advies van het Europees Economisch en Sociaal Comité ([2]),

Na raadpleging van het Comité van de Regio's,

Handelend volgens de gewone wetgevingsprocedure ([3]),

Overwegende hetgeen volgt:

(1) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad ([4]) heeft tot doel capaciteiten op het gebied van cyberbeveiliging in de hele Unie op te bouwen, de bedreigingen voor netwerk- en informatiesystemen die worden gebruikt om essentiële diensten in belangrijke sectoren aan te bieden, te beperken en de continuïteit van dergelijke diensten te waarborgen wanneer zij worden geconfronteerd met incidenten, en aldus bij te dragen tot de veiligheid van de Unie en tot de doeltreffende werking van haar economie en samenleving.

(2) Sinds de inwerkingtreding van Richtlijn (EU) 2016/1148 is er aanzienlijke vooruitgang geboekt bij het vergroten van het niveau van digitale weerbaarheid van de Unie. Uit de evaluatie van die richtlijn is gebleken dat zij heeft gediend als katalysator voor de institutionele en regelgevende aanpak van cyberbeveiliging in de Unie, waardoor de weg is vrijgemaakt voor een significante verandering in de manier waarop deze wordt benaderd. Die richtlijn heeft gezorgd voor de voltooiing van nationale kaders voor de beveiliging van netwerk- en informatiesystemen door te voorzien in nationale strategieën voor de beveiliging van netwerk- en informatiesystemen en nationale capaciteiten vast te stellen en door regelgevende maatregelen uit te voeren die betrekking hebben op essentiële infrastructuur en entiteiten die door elke lidstaat zijn geïdentificeerd. Richtlijn (EU) 2016/1148 heeft ook bijgedragen aan de samenwerking op Unieniveau door de oprichting van de samenwerkingsgroep en het netwerk van nationale computer security incident response teams (CSIRT's). Niettegenstaande die resultaten heeft de evaluatie van Richtlijn (EU) 2016/1148 inherente tekortkomingen aan het licht gebracht die verhinderen dat de huidige en opkomende uitdagingen op het gebied van cyberbeveiliging effectief worden aangepakt met die richtlijn.

(3) Netwerk- en informatiesystemen hebben zich ontwikkeld tot een centraal kenmerk van het dagelijks leven door de snelle digitale transformatie en de onderlinge verbondenheid van de samenleving, ook bij grensoverschrijdende uitwisselingen. Die ontwikkeling heeft geleid tot een uitbreiding van het cyberdreigingslandschap, wat nieuwe uitdagingen met zich meebrengt, die in alle lidstaten een aangepaste, gecoördineerde en innovatieve respons vereisen. Het aantal, de omvang, de complexiteit, de frequentie en de impact van incidenten nemen toe en vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Daardoor kunnen incidenten de

([1]) PB C 233 van 16.6.2022, blz. 22.
([2]) PB C 286 van 16.7.2021, blz. 170.
([3]) Standpunt van het Europees Parlement van 10 november 2022 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 28 november 2022.
([4]) 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).

uitoefening van economische activiteiten in de interne markt belemmeren, financieel verlies veroorzaken, het vertrouwen van de gebruikers ondermijnen en grote schade toebrengen aan de economie en de samenleving van de Unie. Voor de goede werking van de interne markt zijn paraatheid en doeltreffendheid op het gebied van cyberbeveiliging daarom nu meer dan ooit van essentieel belang. Bovendien is cyberbeveiliging voor veel kritieke sectoren van essentieel belang om de digitale transformatie met succes te kunnen doorvoeren en de economische, sociale en duurzame voordelen van digitalisering ten volle te benutten.

(4) De rechtsgrondslag voor Richtlijn (EU) 2016/1148 was artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU), dat tot doel heeft de interne markt tot stand te brengen en te laten functioneren door de maatregelen voor de onderlinge aanpassing van de nationale regels te versterken. De cyberbeveiligingseisen die worden gesteld aan entiteiten die diensten of economisch belangrijke activiteiten verrichten, verschillen aanzienlijk van lidstaat tot lidstaat wat betreft het soort eisen, de mate van gedetailleerdheid en de wijze van toezicht. Die verschillen brengen extra kosten met zich mee en leveren problemen op voor entiteiten die goederen of diensten aanbieden over de grenzen heen. De eisen die door de ene lidstaat worden gesteld en die verschillen van of zelfs in strijd zijn met de door een andere lidstaat gestelde eisen kunnen een aanzienlijke invloed hebben op deze grensoverschrijdende activiteiten. Bovendien zal de mogelijkheid van een ontoereikend ontwerp of een ontoereikende uitvoering van de cyberbeveiligingseisen in een lidstaat waarschijnlijk gevolgen hebben op het niveau van de cyberbeveiliging in andere lidstaten, met name gezien de intensiteit van grensoverschrijdende uitwisselingen. Bij de evaluatie van Richtlijn (EU) 2016/1148 is gebleken dat de lidstaten de richtlijn op zeer uiteenlopende wijze uitvoeren, ook wat het toepassingsgebied betreft, waarvan de afbakening grotendeels aan het oordeel van de lidstaten is overgelaten. Richtlijn (EU) 2016/1148 bood de lidstaten ook een zeer ruime discretionaire bevoegdheid bij de uitvoering van de daarin vastgelegde verplichtingen inzake beveiliging en incidentenmelding. Die verplichtingen zijn daarom op nationaal niveau op aanzienlijk verschillende wijzen uitgevoerd. Er bestaan soortgelijke verschillen in de uitvoering van de bepalingen van Richtlijn (EU) 2016/1148 inzake toezicht en handhaving.

(5) Al deze verschillen leiden tot een versnippering van de interne markt en kunnen een nadelig effect hebben op de werking ervan, wat met name gevolgen heeft voor de grensoverschrijdende dienstverlening en het niveau van de digitale weerbaarheid als gevolg van de toepassing van diverse maatregelen. Uiteindelijk kunnen die verschillen sommige lidstaten uiteindelijk meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Unie. Deze richtlijn heeft tot doel dergelijke grote verschillen tussen de lidstaten weg te werken, met name door minimumvoorschriften vast te stellen voor de werking van een gecoördineerd regelgevingskader, door mechanismen vast te stellen voor een doeltreffende samenwerking tussen de verantwoordelijke autoriteiten in elke lidstaat, door de lijst van sectoren en activiteiten waarvoor cyberbeveiligingsverplichtingen gelden bij te werken en door te voorzien in doeltreffende voorzieningen en handhavingsmaatregelen die essentieel zijn voor de doeltreffende handhaving van deze verplichtingen. Daarom moet Richtlijn (EU) 2016/1148 worden ingetrokken en door deze richtlijn worden vervangen.

(6) Met de intrekking van Richtlijn (EU) 2016/1148 moet het toepassingsgebied per sector worden uitgebreid tot een groter deel van de economie om de sectoren en diensten die van vitaal belang zijn voor belangrijke maatschappelijke en economische activiteiten in de interne markt, volledig te bestrijken. Meer bepaald heeft deze richtlijn tot doel de tekortkomingen te verhelpen van het onderscheid tussen aanbieders van essentiële diensten en digitaledienstverleners, dat achterhaald is gebleken, aangezien het niet het belang van de sectoren of diensten voor de maatschappelijke en economische activiteiten in de interne markt weerspiegelt.

(7) Op grond van Richtlijn (EU) 2016/1148 waren de lidstaten verantwoordelijk voor het identificeren van de entiteiten die voldeden aan de criteria om als aanbieders van essentiële diensten te worden aangemerkt. Om de grote verschillen tussen de lidstaten in dat opzicht weg te werken en rechtszekerheid te bieden met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen voor alle relevante entiteiten, moet er een uniform criterium worden vastgesteld dat bepaalt welke entiteiten binnen het toepassingsgebied van deze richtlijn vallen. Dit criterium moet bestaan uit de toepassing van een "size-cap"-regel, waarbij alle entiteiten die worden aangemerkt als middelgrote ondernemingen uit hoofde van artikel 2, lid 1, van de bijlage bij Aanbeveling 2003/361/EG van de Commissie ([5]), of die de plafonds voor middelgrote ondernemingen als bepaald in lid 1 van dat artikel overschrijden, en die actief zijn in de sectoren en de soorten diensten of de onder deze

([5]) Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

richtlijn vallende activiteiten verrichten, binnen het toepassingsgebied van deze richtlijn vallen. De lidstaten moeten er ook voor zorgen dat bepaalde kleine ondernemingen en micro-ondernemingen, als gedefinieerd in artikel 2, leden 2 en 3, van die bijlage, die voldoen aan specifieke criteria welke wijzen op een sleutelrol voor de samenleving, de economie of bepaalde sectoren of soorten diensten, binnen het toepassingsgebied van deze richtlijn vallen.

(8) Overheidsinstanties moeten worden uitgesloten van het toepassingsgebied van deze richtlijn indien de activiteiten van die entiteiten hoofdzakelijk worden uitgevoerd op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Overheidsinstanties waarvan de activiteiten slechts zijdelings verband houden met die gebieden mogen echter niet worden uitgesloten van het toepassingsgebied van deze richtlijn. Voor de toepassing van deze richtlijn worden entiteiten met regelgevende bevoegdheden niet geacht activiteiten op het gebied van rechtshandhaving uit te voeren en zij worden dan ook op die grond niet uitgesloten van het toepassingsgebied van deze richtlijn. Overheidsinstanties die gezamenlijk met een derde land zijn opgericht bij een internationale overeenkomst, worden uitgesloten van het toepassingsgebied van deze richtlijn. Deze richtlijn is niet van toepassing op diplomatieke en consulaire missies van de lidstaten in derde landen of op hun netwerk- en informatiesystemen, voor zover deze systemen zich in de lokalen van de missie bevinden of voor gebruikers in een derde land worden gebruikt.

(9) De lidstaten moeten de noodzakelijke maatregelen kunnen nemen ter bescherming van de wezenlijke belangen van nationale veiligheid, ter vrijwaring van de openbare orde en de openbare veiligheid en om de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken. Daartoe moeten de lidstaten specifieke entiteiten die activiteiten verrichten op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, kunnen vrijstellen van bepaalde in deze richtlijn vastgelegde verplichtingen met betrekking tot die activiteiten. Wanneer een entiteit uitsluitend diensten verleent aan een overheidsinstantie die is uitgesloten van het toepassingsgebied van deze richtlijn, moeten de lidstaten die entiteit kunnen vrijstellen van bepaalde in deze richtlijn vastgelegde verplichtingen met betrekking tot die diensten. Voorts mag geen enkele lidstaat worden verplicht inlichtingen te verstrekken waarvan de openbaarmaking in strijd zou zijn met de wezenlijke belangen van zijn nationale veiligheid, openbare veiligheid of defensie. Er moet in die context rekening worden gehouden met Unieregels of nationale regels voor de bescherming van gerubriceerde informatie, geheimhoudingsovereenkomsten en informele geheimhoudingsovereenkomsten, zoals het verkeerslichtprotocol. Het verkeerslichtprotocol moet worden opgevat als een middel om informatie te verstrekken over eventuele beperkingen met betrekking tot de verdere verspreiding van informatie. Het wordt gebruikt in bijna alle CSIRT's en in sommige centra voor informatie-uitwisseling en -analyse.

(10) Hoewel deze richtlijn van toepassing is op entiteiten die activiteiten verrichten op het gebied van de elektriciteitsproductie van kerncentrales, kunnen sommige van deze activiteiten verband houden met de nationale veiligheid. Indien dat het geval is, moet een lidstaat, overeenkomstig de Verdragen, zijn verantwoordelijkheid kunnen uitoefenen voor het waarborgen van de nationale veiligheid met betrekking tot die activiteiten, met inbegrip van activiteiten in de nucleaire waardeketen.

(11) Sommige entiteiten verrichten activiteiten op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, en verlenen ook vertrouwensdiensten. Verleners van vertrouwensdiensten die binnen het toepassingsgebied van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad [6] vallen, moeten binnen het toepassingsgebied van deze richtlijn vallen om hetzelfde niveau van beveiligingseisen en toezicht te waarborgen als het niveau dat in die verordening was vastgesteld ten aanzien van verleners van vertrouwensdiensten. Overeenkomstig de uitsluiting van bepaalde specifieke diensten van Verordening (EU) nr. 910/2014 mag deze richtlijn niet van toepassing zijn op de verlening van vertrouwensdiensten die uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van nationaal recht of overeenkomsten tussen een bepaalde groep deelnemers.

[6] 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).

(12) Verleners van postdiensten zoals gedefinieerd in Richtlijn 97/67/EG van het Europees Parlement en de Raad ([7]), met inbegrip van verleners van koeriersdiensten, moeten onder deze richtlijn vallen indien zij ten minste een van de stappen in de postbestelketen verzorgen, met name het ophalen, sorteren, vervoeren en bestellen van postzendingen, met inbegrip van de ophaaldiensten, waarbij rekening moet worden gehouden met de mate waarin zij afhankelijk zijn van netwerk- en informatiesystemen. Vervoersdiensten die niet in samenhang met een van die stappen worden ondernomen, mogen niet tot de postdiensten worden gerekend.

(13) Aangezien de cyberdreigingen steeds intenser en geavanceerder worden, moeten de lidstaten trachten te waarborgen dat entiteiten die zijn uitgesloten van het toepassingsgebied van deze richtlijn, een hoog cyberbeveiligingsniveau bereiken en moeten zij de uitvoering ondersteunen van gelijkwaardige maatregelen voor het beheer van cyberbeveiligingsrisico's die het gevoelige karakter van die entiteiten weerspiegelen.

(14) Het Uniegegevensbeschermingsrecht en het Unieprivacyrecht is van toepassing op elke verwerking van persoonsgegevens uit hoofde van deze richtlijn. Meer bepaald doet deze richtlijn geen afbreuk aan Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([8]) en Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([9]). Deze richtlijn moet derhalve onder meer de taken en bevoegdheden onverlet laten van de autoriteiten die bevoegd zijn om toezicht te houden op de naleving van het toepasselijke Uniegegevensbeschermingsrecht en het Unieprivacyrecht.

(15) Entiteiten die voor de naleving van de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen binnen het toepassingsgebied van deze richtlijn vallen, moeten worden ingedeeld in twee categorieën, essentiële entiteiten en belangrijke entiteiten, naargelang de mate waarin zij kritiek zijn door hun sector of het soort door hen verleende diensten, alsook hun omvang. In dat verband moet, in voorkomend geval, terdege rekening worden gehouden met relevante sectorale risicobeoordelingen of richtsnoeren van de bevoegde autoriteiten. De toezichts- en handhavingsregelingen voor die twee categorieën entiteiten moeten worden gedifferentieerd om te zorgen voor een billijk evenwicht tussen op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds.

(16) Om te voorkomen dat entiteiten met partnerondernemingen of verbonden ondernemingen als essentiële of belangrijke entiteiten worden beschouwd wanneer dit onevenredig zou zijn, kunnen de lidstaten bij de toepassing van artikel 6, lid 2, van de bijlage bij Aanbeveling 2003/361/EG rekening houden met de mate van onafhankelijkheid welke die entiteiten ten opzichte van hun partnerondernemingen of verbonden ondernemingen genieten. Meer bepaald kunnen de lidstaten rekening houden met het feit dat een entiteit onafhankelijk is van haar partnerondernemingen of verbonden ondernemingen wat de netwerk- en informatiesystemen betreft waarvan die entiteit gebruikmaakt bij het verlenen van haar diensten en wat de diensten betreft die de entiteit verleent. Op basis daarvan kunnen de lidstaten een dergelijke entiteit in voorkomend geval beschouwen als een entiteit die niet wordt aangemerkt als een middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, noch de plafonds voor een middelgrote onderneming als bepaald in lid 1 van dat artikel overschrijdt, indien die entiteit, rekening houdend met de mate van onafhankelijkheid die zij geniet, niet als middelgrote onderneming zou worden aangemerkt of niet zou worden geacht die plafonds te overschrijden ingeval alleen rekening zou worden gehouden met haar eigen gegevens. Dit doet geen afbreuk aan de in deze richtlijn vastgelegde verplichtingen van partnerondernemingen en verbonden ondernemingen die binnen het toepassingsgebied van deze richtlijn vallen.

(17) De lidstaten moeten kunnen besluiten dat entiteiten die vóór de inwerkingtreding van deze richtlijn overeenkomstig Richtlijn (EU) 2016/1148 als aanbieders van essentiële diensten zijn geïdentificeerd, als essentiële entiteiten moeten worden beschouwd.

([7]) Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst (PB L 15 van 21.1.1998, blz. 14).

([8]) 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).

([9]) 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).

(18) Om te zorgen voor een duidelijk overzicht van de binnen het toepassingsgebied van deze richtlijn vallende entiteiten, moeten de lidstaten een lijst opstellen van essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. Daartoe moeten de lidstaten van entiteiten verlangen dat zij de bevoegde autoriteiten ten minste de volgende informatie verstrekken: de naam, het adres en de actuele contactgegevens, waaronder de e-mailadressen, IP-bereiken en telefoonnummers van de entiteit, evenals, in voorkomend geval, de relevante sectoren en subsectoren als bedoeld in de bijlagen, alsmede, in voorkomend geval, een lijst van de lidstaten waar zij binnen het toepassingsgebied van deze richtlijn vallende diensten verlenen. Daartoe moet de Commissie, met hulp van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), onverwijld richtsnoeren en modellen bepalen met betrekking tot de verplichting om informatie in te dienen. Om het opstellen en bijwerken van de lijst van essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen te vergemakkelijken, moeten de lidstaten nationale mechanismen kunnen instellen voor entiteiten om zich te registreren. Indien er registers bestaan op nationaal niveau, kunnen de lidstaten besluiten over passende mechanismen voor de identificatie van binnen het toepassingsgebied van deze richtlijn vallende entiteiten.

(19) De lidstaten moeten de verantwoordelijkheid dragen om bij de Commissie ten minste het aantal essentiële en belangrijke entiteiten per sector en subsector als bedoeld in de bijlagen in te dienen, evenals relevante informatie over het aantal geïdentificeerde entiteiten, alsook de in deze richtlijn vastgestelde bepaling op basis waarvan zij zijn geïdentificeerd, en het soort diensten dat zij verrichten. De lidstaten worden aangemoedigd om informatie over essentiële en belangrijke entiteiten uit te wisselen met de Commissie evenals, in het geval van een grootschalig cyberbeveiligingsincident, relevante informatie zoals de naam van de betrokken entiteit.

(20) De Commissie moet, in samenwerking met de samenwerkingsgroep en na raadpleging van de relevante belanghebbenden, richtsnoeren bepalen voor de toepassing van de criteria die gelden voor micro-ondernemingen en kleine ondernemingen om te beoordelen of zij binnen het toepassingsgebied van deze richtlijn vallen. De Commissie moet er tevens op toezien dat er passende begeleiding wordt geboden aan micro-ondernemingen en kleine ondernemingen die binnen het toepassingsgebied van deze richtlijn vallen. De Commissie moet in dit verband, met hulp van de lidstaten, informatie ter beschikking stellen aan micro-ondernemingen en kleine ondernemingen.

(21) De Commissie kan richtsnoeren verstrekken om de lidstaten bij te staan bij de uitvoering van de bepalingen van deze richtlijn inzake het toepassingsgebied en bij de beoordeling van de evenredigheid van de maatregelen die uit hoofde van deze richtlijn moeten worden genomen, met name ten aanzien van entiteiten met complexe bedrijfsmodellen of werkomgevingen, waarbij een entiteit tegelijkertijd kan voldoen aan de criteria voor essentiële en belangrijke entiteiten of tegelijkertijd activiteiten kan verrichten waarvan sommige binnen het toepassingsgebied van deze richtlijn vallen en sommige ervan uitgesloten zijn.

(22) In deze richtlijn wordt voor de binnen het toepassingsgebied ervan vallende sectoren het basisniveau vastgesteld voor de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen. Om versnippering van de cyberbeveiligingsbepalingen van rechtshandelingen van de Unie te voorkomen, moet de Commissie, wanneer verdere sectorspecifieke rechtshandelingen van de Unie met betrekking tot maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen noodzakelijk worden geacht om een hoog niveau van cyberbeveiliging in de Unie te waarborgen, beoordelen of dergelijke verdere bepalingen kunnen worden vastgesteld in een uitvoeringshandeling uit hoofde van deze richtlijn. Mocht een dergelijke uitvoeringshandeling niet geschikt zijn voor dat doel, kunnen sectorspecifieke rechtshandelingen van de Unie bijdragen tot het waarborgen van een hoog niveau van cyberbeveiliging in de Unie, waarbij ten volle rekening wordt gehouden met de specifieke kenmerken en complexiteit van de betrokken sectoren. Met het oog daarop vormt deze richtlijn geen beletsel voor de vaststelling van verdere sectorspecifieke rechtshandelingen van de Unie met betrekking tot maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen waarin terdege rekening wordt gehouden met de noodzaak van een alomvattend en samenhangend kader voor cyberbeveiliging. Deze richtlijn laat de bestaande uitvoeringsbevoegdheden die aan de Commissie zijn verleend in een aantal sectoren, waaronder vervoer en energie, onverlet.

(23) Wanneer een sectorspecifieke rechtshandeling van de Unie bepalingen bevat op grond waarvan essentiële of belangrijke entiteiten maatregelen voor het beheer van cyberbeveiligingsrisico's moeten nemen of significante incidenten moeten melden en wanneer die eisen ten minste gelijkwaardig zijn aan de in deze richtlijn vastgestelde

verplichtingen, moeten die bepalingen, onder meer inzake toezicht en handhaving, van toepassing zijn op die entiteiten. Indien een sectorspecifieke rechtshandeling van de Unie niet op alle entiteiten in een specifieke sector betrekking heeft die binnen het toepassingsgebied van deze richtlijn valt, moeten de relevante bepalingen van deze richtlijn van toepassing blijven op de entiteiten waarop die handeling geen betrekking heeft.

(24) Wanneer bepalingen van een sectorspecifieke rechtshandeling van de Unie essentiële of belangrijke entiteiten verplichten te voldoen aan rapportageverplichtingen die ten minste gelijkwaardig zijn aan de in deze richtlijn vastgestelde rapportageverplichtingen, moet de samenhang en doeltreffendheid van de behandeling van meldingen van incidenten worden gewaarborgd. Daartoe moeten de met meldingen van incidenten verband houdende bepalingen van de sectorspecifieke rechtshandeling van de Unie voor de CSIRT's, de bevoegde autoriteiten of de centrale contactpunten voor cyberbeveiliging (centrale contactpunten) uit hoofde van deze richtlijn voorzien in onmiddellijke toegang tot de overeenkomstig de sectorspecifieke rechtshandeling van de Unie ingediende meldingen van incidenten. Deze onmiddellijke toegang kan met name worden gewaarborgd indien meldingen van incidenten onverwijld worden doorgestuurd naar de CSIRT, de bevoegde autoriteit of het centrale contactpunt uit hoofde van deze richtlijn. In voorkomend geval moeten de lidstaten een mechanisme voor automatische en rechtstreekse rapportage opzetten dat ervoor zorgt dat informatie met betrekking tot de behandeling van dergelijke meldingen van incidenten systematisch en onmiddellijk wordt uitgewisseld met de CSIRT's, de bevoegde autoriteiten of de centrale contactpunten. Om de rapportage en de toepassing van het mechanisme voor automatische en rechtstreekse rapportage te vereenvoudigen kunnen de lidstaten, overeenkomstig de sectorspecifieke rechtshandeling van de Unie, gebruikmaken van één centraal contactpunt.

(25) In de sectorspecifieke rechtshandelingen van de Unie die voorzien in maatregelen voor het beheer van cyberbeveiligingsrisico's of rapportageverplichtingen die ten minste gelijkwaardig zijn aan de in deze richtlijn vastgestelde maatregelen en verplichtingen, kan worden vastgelegd dat de in uit hoofde van die handelingen bevoegde autoriteiten hun toezichts- en handhavingsbevoegdheden met betrekking tot die maatregelen of verplichtingen uitoefenen met hulp van de uit hoofde van deze richtlijn bevoegde autoriteiten. Daartoe kunnen de betrokken bevoegde autoriteiten samenwerkingsregelingen treffen. In dergelijke samenwerkingsregelingen kunnen onder meer de procedures voor de coördinatie van toezichtsactiviteiten worden omschreven, met inbegrip van de procedures voor onderzoeken en inspecties ter plaatse overeenkomstig het nationale recht, en die voor een mechanisme voor de uitwisseling van relevante informatie over toezicht en handhaving tussen de bevoegde autoriteiten, met inbegrip van verzoeken van de uit hoofde van deze richtlijn bevoegde autoriteiten om toegang tot cybergerelateerde informatie.

(26) Wanneer sectorspecifieke rechtshandelingen van de Unie entiteiten verplichten of stimuleren om significante cyberdreigingen te melden, moeten de lidstaten ook de uitwisseling van informatie over significante cyberdreigingen met de CSIRT's, de bevoegde autoriteiten of de centrale contactpunten uit hoofde van deze richtlijn bevorderen om die organen beter bewust te maken van het cyberdreigingslandschap en hen in staat te stellen doeltreffend en tijdig te reageren indien significante cyberdreigingen tot incidenten leiden.

(27) Toekomstige sectorspecifieke rechtshandelingen van de Unie moeten terdege rekening houden met de definities en het kader voor toezicht en handhaving van deze richtlijn.

(28) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad ([10]) moet worden beschouwd als een sectorspecifieke rechtshandeling van de Unie met betrekking tot deze richtlijn voor wat financiële entiteiten betreft. De bepalingen van Verordening (EU) 2022/2554 betreffende risicobeheer op het gebied van informatie- en communicatietechnologie (ICT), het beheer van ICT-gerelateerde incidenten en met name de rapportage van grote ICT-gerelateerde incidenten, alsmede betreffende digitale operationele weerbaarheidstests, informatie-uitwisselingsregelingen en risico van derden op het gebied van ICT, moeten van toepassing zijn in plaats van de bepalingen van deze richtlijn. De lidstaten mogen de bepalingen van deze richtlijn betreffende de verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging, toezicht en handhaving dan ook niet toepassen op financiële entiteiten die onder Verordening (EU) 2022/2554 vallen. Tegelijkertijd is het van belang een sterke relatie en de uitwisseling van informatie met de financiële sector uit hoofde van deze richtlijn in stand te houden. Daartoe biedt Verordening (EU) 2022/2554 de Europese toezichthoudende autoriteiten (ETA's) en de uit hoofde van die verordening bevoegde autoriteit en de mogelijkheid deel te nemen aan de activiteiten van de samenwerkingsgroep en informatie uit te wisselen en samen te werken met de centrale contactpunten en met de CSIRT's en de uit hoofde van die richtlijn bevoegde autoriteiten. De uit hoofde van Verordening (EU) 2022/2554 bevoegde autoriteiten moeten de details van grote ICT-gerelateerde incidenten en significante cyberdreigingen ook doorgeven aan de

([10]) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (zie bladzijde 1 van dit Publicatieblad).

CSIRT's, de bevoegde autoriteiten of de centrale contactpunten uit hoofde van deze richtlijn. Dit is haalbaar door te voorzien in onmiddellijke toegang en erin te voorzien dat meldingen van incidenten rechtstreeks worden doorgestuurd, of door middel van één centraal contactpunt voor de melding van incidenten. Bovendien moeten de lidstaten de financiële sector blijven opnemen in hun cyberbeveiligingsstrategieën en kunnen de CSIRT's de financiële sector bij hun activiteiten betrekken.

(29) Om lacunes in of overlappingen van de cyberbeveiligingsverplichtingen voor entiteiten in de luchtvaartsector te vermijden, moeten de nationale autoriteiten uit hoofde van de Verordeningen (EG) nr. 300/2008 ([11]) en (EU) 2018/1139 ([12]) van het Europees Parlement en de Raad en de uit hoofde van deze richtlijn bevoegde autoriteiten samenwerken bij de uitvoering van maatregelen voor het beheer van cyberbeveiligingsrisico's en het toezicht op de naleving van die maatregelen op nationaal niveau. De naleving door een entiteit van de beveiligingseisen die zijn vastgelegd in de Verordeningen (EG) nr. 300/2008 en (EU) 2018/1139 en in de relevante gedelegeerde en uitvoeringshandelingen die krachtens die verordeningen zijn vastgesteld, kan door de uit hoofde van deze richtlijn bevoegde autoriteiten worden geacht tot naleving van de overeenkomstige eisen van deze richtlijn te dienen.

(30) Gezien de onderlinge verbanden tussen cyberbeveiliging en de fysieke beveiliging van entiteiten moet een coherente aanpak worden gewaarborgd tussen Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad ([13]) en deze richtlijn. Daartoe moeten entiteiten die uit hoofde van Richtlijn (EU) 2022/2557 als kritieke identiteiten worden aangemerkt als essentiële entiteiten uit hoofde van deze richtlijn worden beschouwd. Bovendien moet elke lidstaat ervoor zorgen dat zijn nationale cyberbeveiligingsstrategie voorziet in een beleidskader voor een betere coördinatie binnen die lidstaat tussen zijn uit hoofde van deze richtlijn bevoegde autoriteiten en die uit hoofde van Richtlijn (EU) 2022/2557 in de context van de uitwisseling van informatie over risico's, cyberdreigingen en incidenten alsook over niet-cyberrisico's, -dreigingen en -incidenten, evenals de uitoefening van toezichthoudende taken. De uit hoofde van deze richtlijn bevoegde autoriteiten en die uit hoofde van Richtlijn (EU) 2022/2557 moeten zonder onnodige vertraging samenwerken en informatie uitwisselen, met name met betrekking tot de identificatie van kritieke entiteiten, risico's, cyberdreigingen, en incidenten en niet-cyberrisico's, -dreigingen en -incidenten die kritieke entiteiten treffen, met inbegrip van door kritieke entiteiten genomen maatregelen op het gebied van cyberbeveiliging en fysieke maatregelen, evenals de resultaten van toezichtsactiviteiten met betrekking tot die entiteiten.

Om de toezichtsactiviteiten tussen de uit hoofde van deze richtlijn bevoegde autoriteiten en die uit hoofde van Richtlijn (EU) 2022/2557 te stroomlijnen en om de administratieve lasten voor de betrokken entiteiten tot een minimum te beperken, moeten die bevoegde autoriteiten ernaar streven de modellen voor de melding van incidenten en de toezichtsprocessen te harmoniseren. In voorkomend geval moeten de uit hoofde van Richtlijn (EU) 2022/2557 bevoegde autoriteiten de uit hoofde van deze richtlijn bevoegde autoriteiten kunnen verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen met betrekking tot een entiteit die is aangemerkt als een kritieke entiteit uit hoofde van Richtlijn (EU) 2022/2557. Daartoe moeten de uit hoofde van deze richtlijn bevoegde autoriteiten en die uit hoofde van Richtlijn (EU) 2022/2557, indien mogelijk in realtime, samenwerken en informatie uitwisselen.

(31) Tot de digitale-infrastructuursector behorende entiteiten zijn in wezen gebaseerd op netwerk- en informatiesystemen en daarom moeten de hun uit hoofde van deze richtlijn opgelegde verplichtingen op een omvattende manier betrekking hebben op de fysieke beveiliging van dergelijke systemen in het kader van hun maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen. Aangezien die aangelegenheden onder deze richtlijn vallen, zijn de verplichtingen van de hoofdstukken III, IV en VI van Richtlijn (EU) 2022/2557 niet van toepassing op dergelijke entiteiten.

([11]) Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72).

([12]) Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad (PB L 212 van 22.8.2018, blz. 1).

([13]) Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (zie bladzijde 164 van dit Publicatieblad).

(32) Het ondersteunen en instandhouden van een betrouwbaar, weerbaar en beveiligd domeinnaamsysteem (DNS) zijn sleutelfactoren voor het behoud van de integriteit van het internet en zijn essentieel voor de continue en stabiele werking ervan, waarvan de digitale economie en samenleving afhankelijk zijn. Daarom moet deze richtlijn van toepassing zijn op registers voor topleveldomeinnamen en DNS-dienstverleners die moeten worden opgevat als entiteiten die openbare recursieve domeinnaamomzettingsdiensten verlenen aan interneteindgebruikers of gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden. Deze richtlijn mag niet van toepassing zijn op root-naamservers.

(33) Cloudcomputingdiensten moeten digitale diensten omvatten die beheer op verzoek en brede toegang op afstand ("*broad remote access*") tot een schaalbare en elastische pool van deelbare computercapaciteit mogelijk maken, ook wanneer deze over verschillende locaties is gedistribueerd. Computercapaciteit omvat middelen zoals netwerken, servers of andere infrastructuur, besturingssystemen, software, opslag, toepassingen en diensten. De dienstmodellen van cloudcomputing omvatten onder meer infrastructuur als dienst ("*Infrastructure as a Service*" — IaaS), platform als dienst ("*Platform as a Service*" — PaaS), software als dienst ("*Software as a Service*" — SaaS) en netwerk als dienst ("*Network as a Service*" — NaaS). De invoeringsmodellen van cloudcomputing moeten private, gemeenschaps-, publieke en hybride cloud omvatten. De dienst- en invoeringsmodellen van cloudcomputing hebben dezelfde betekenis als de in de ISO/IEC 17788:2014-norm gedefinieerde benamingen van dienst- en invoeringsmodellen. Het vermogen van de cloudcomputinggebruiker om eenzijdig zelfvoorzienend te zijn, bijvoorbeeld wat servertijd of netwerkopslag betreft, zonder enige menselijke interactie door de cloudcomputingdienstverlener, zou kunnen worden omschreven als beheer op verzoek.

De term "brede toegang op afstand" wordt gebruikt om te beschrijven dat de cloudcapaciteiten via het netwerk worden aangeboden en toegankelijk zijn via mechanismen die het gebruik van heterogene thin- of thick-client-platforms bevorderen, waaronder mobiele telefoons, tablets, laptops en werkstations. De term "schaalbaar" verwijst naar de computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van cloudcomputingdiensten wordt toegewezen teneinde schommelingen in de vraag te kunnen opvangen. De term "elastische pool" wordt gebruikt ter beschrijving van de computercapaciteit die, afhankelijk van de vraag, ter beschikking wordt gesteld en wordt vrijgegeven teneinde deze beschikbare capaciteit snel te kunnen verhogen en verlagen naargelang van het werkvolume. De term "deelbaar" wordt gebruikt ter beschrijving van de computercapaciteit die ter beschikking wordt gesteld van meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische uitrusting wordt verleend. De term "gedistribueerd" wordt gebruikt ter beschrijving van de computercapaciteit die zich op verschillende netwerkcomputers of -apparaten bevindt en waarbij onderlinge communicatie en aansturing plaatsvindt door middel van het doorgeven van berichten.

(34) Gezien de opkomst van innovatieve technologieën en nieuwe bedrijfsmodellen wordt verwacht dat er nieuwe dienst- en invoeringsmodellen voor cloudcomputing op de interne markt zullen verschijnen om in te spelen op de veranderende behoeften van klanten. In die context kunnen cloudcomputingdiensten in een sterk gedistribueerde vorm worden verleend, nog dichter bij de plaats waar de gegevens worden gegenereerd of verzameld, waardoor de overstap wordt gemaakt van het traditionele model naar een sterk gedistribueerd model ("*edge computing*").

(35) Diensten die worden aangeboden door aanbieders van datacentrumdiensten kunnen niet altijd in de vorm van een cloudcomputingdienst worden verleend. Datacentra maken dan ook niet altijd deel uit van cloudcomputinginfrastructuur. Om alle risico's voor de beveiliging van netwerk- en informatiesystemen te beheren, moet deze richtlijn dan ook van toepassing zijn op aanbieders van datacentrumdiensten die geen cloudcomputingdiensten zijn. Voor de toepassing van deze richtlijn moet de term "datacentrumdienst" betrekking hebben op de verlening van een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van informatietechnologie (IT) en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuur voor energiedistributie en omgevingscontrole. De term "datacentrumdienst" mag niet gelden voor interne bedrijfsdatacentra die eigendom zijn van en geëxploiteerd worden door de betrokken entiteit, voor eigen doeleinden.

(36) Onderzoeksactiviteiten spelen een sleutelrol bij de ontwikkeling van nieuwe producten en processen. Veel van die activiteiten worden verricht door entiteiten die de resultaten van hun onderzoek delen, verspreiden of exploiteren voor commerciële doeleinden. Die entiteiten kunnen dan ook belangrijke spelers in de waardeketens zijn, zodat de beveiliging van hun netwerk- en informatiesystemen integraal deel uitmaakt van de algemene cyberbeveiliging van de interne markt. Onder onderzoeksorganisaties moeten ook entiteiten worden verstaan die het wezenlijk deel van

hun activiteiten richten op toegepast onderzoek of experimentele ontwikkeling in de zin van het "*Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development*" van de Organisatie voor Economische Samenwerking en Ontwikkeling, om hun resultaten te exploiteren voor commerciële doeleinden, zoals de vervaardiging of ontwikkeling van een product of een proces, de verlening van een dienst, of het in de handel brengen daarvan.

(37) De toenemende onderlinge afhankelijkheid is het resultaat van een steeds meer grensoverschrijdend en onderling afhankelijk dienstverleningsnetwerk waarin gebruik wordt gemaakt van essentiële infrastructuren in de hele Unie in sectoren zoals energie, vervoer, digitale infrastructuur, drinkwater en afvalwater, gezondheid, bepaalde aspecten van het overheidsbestuur, en ruimtevaart, voor zover het gaat om de verlening van bepaalde diensten die afhankelijk zijn van grondgebonden infrastructuren die eigendom zijn van, beheerd worden en geëxploiteerd worden door de lidstaten of door particuliere partijen, en die dus geen betrekking hebben op infrastructuren die eigendom zijn van, beheerd worden of geëxploiteerd worden door of namens de Unie in het kader van haar ruimtevaartprogramma. Die onderlinge afhankelijkheid houdt in dat elke verstoring, zelfs wanneer deze aanvankelijk beperkt blijft tot één entiteit of één sector, meer in het algemeen een cascade-effect kan hebben, met mogelijkerwijs verstrekkende en langdurige negatieve gevolgen voor de verlening van diensten op de hele interne markt. De tijdens de COVID-19-pandemie toegenomen cyberaanvallen hebben de kwetsbaarheid van onze steeds meer onderling afhankelijke samenlevingen voor de risico's van lage waarschijnlijkheid aangetoond.

(38) Gezien de verschillen tussen de nationale governancestructuren en om de reeds bestaande sectorale regelingen of toezichts- en regelgevingsorganen van de Unie te vrijwaren, moeten de lidstaten een of meer bevoegde autoriteiten kunnen aanwijzen of oprichten die verantwoordelijk zijn voor cyberbeveiliging en voor de toezichthoudende taken uit hoofde van deze richtlijn.

(39) Om de grensoverschrijdende samenwerking en communicatie tussen de autoriteiten te vergemakkelijken en een doeltreffende uitvoering van deze richtlijn mogelijk te maken, moet elke lidstaat een centraal contactpunt aanwijzen dat verantwoordelijk is voor de coördinatie van kwesties in verband met de beveiliging van de netwerk- en informatiesystemen en de grensoverschrijdende samenwerking op het niveau van de Unie.

(40) De centrale contactpunten moeten doeltreffende grensoverschrijdende samenwerking met de relevante autoriteiten van andere lidstaten en, in voorkomend geval, met de Commissie en Enisa waarborgen. De centrale contactpunten moeten daarom worden belast met het doorsturen van meldingen van significante incidenten met grensoverschrijdende gevolgen naar de centrale contactpunten van andere betrokken lidstaten op verzoek van het CSIRT of de bevoegde autoriteit. Op nationaal niveau moeten de centrale contactpunten vlotte sectoroverschrijdende samenwerking met andere bevoegde autoriteiten mogelijk maken. De centrale contactpunten kunnen ook de geadresseerden zijn van relevante informatie over incidenten met betrekking tot financiële entiteiten van de uit hoofde van Verordening (EU) 2022/2554 bevoegde autoriteiten, die zij in voorkomend geval moeten kunnen doorsturen naar de CSIRT's of de uit hoofde van deze richtlijn bevoegde autoriteiten.

(41) De lidstaten moeten, wat zowel de technische als de organisatorische mogelijkheden betreft, adequaat worden uitgerust om incidenten en risico's te voorkomen, op te sporen, erop te reageren, ervan te herstellen en te beperken. De lidstaten moeten daarom een of meer CSIRT's instellen of aanwijzen uit hoofde van deze richtlijn en ervoor zorgen dat zij over voldoende middelen en technische capaciteiten beschikken. De CSIRT's moeten voldoen aan de in deze richtlijn vastgestelde eisen om te garanderen dat zij over doeltreffende en compatibele capaciteiten beschikken om incidenten en risico's aan te pakken en om een efficiënte samenwerking op het niveau van de Unie te waarborgen. De lidstaten moeten bestaande computercrisisresponsteams ("*computer emergency response teams*" — CERT's) kunnen aanwijzen als CSIRT's. Om de vertrouwensrelatie tussen de entiteiten en de CSIRT's te versterken, moeten de lidstaten, indien een CSIRT deel uitmaakt van een bevoegde autoriteit, een functionele scheiding kunnen overwegen tussen de operationele taken van de CSIRT's, met name met betrekking tot de aan de entiteiten verleende informatie-uitwisseling en bijstand, en de toezichtsactiviteiten van de bevoegde autoriteiten.

(42) De CSIRT's zijn belast met de behandeling van incidenten. Dit omvat de verwerking van grote hoeveelheden van soms gevoelige gegevens. De lidstaten moeten ervoor zorgen dat de CSIRT's beschikken over een infrastructuur voor het delen en verwerken van informatie, alsook over goed toegerust personeel, zodat de vertrouwelijkheid en betrouwbaarheid van hun activiteiten wordt gewaarborgd. De CSIRT's kunnen in dit verband ook een gedragscode vaststellen.

(43) Aangaande de persoonsgegevens moeten de CSIRT's overeenkomstig Verordening (EU) 2016/679 op verzoek van een essentiële of belangrijke entiteit een proactieve scan kunnen uitvoeren van de netwerk- en informatiesystemen die voor de verlening van de diensten van de entiteit worden gebruikt. In voorkomend geval moeten de lidstaten ernaar streven dat alle sectorale CSIRT's over gelijke technische capaciteiten beschikken. De lidstaten moeten bij de ontwikkeling van hun CSIRT's de hulp van Enisa kunnen inroepen.

(44) De CSIRT's moeten de mogelijkheid hebben om op verzoek van een essentiële of belangrijke entiteit de internetgerichte activa van de entiteit te monitoren, zowel binnen als buiten de lokalen ervan, om de algemene risico's voor de organisatie van de entiteit wat nieuwe aantastingen van de toeleveringsketen of kritieke kwetsbaarheden betreft vast te stellen, te begrijpen en te beheren. De entiteit moet worden aangespoord om aan het CSIRT mee te delen of zij gebruikmaakt van een interface voor bevoorrecht beheer, aangezien dit van invloed kan zijn op de snelheid waarmee beperkende maatregelen worden genomen.

(45) Gezien het belang van internationale samenwerking op het gebied van cyberbeveiliging moeten de CSIRT's kunnen deelnemen aan internationale samenwerkingsnetwerken, naast het bij deze richtlijn opgerichte CSIRT-netwerk. Daarom moeten de CSIRT's en de bevoegde autoriteiten voor de uitvoering van hun taken informatie, met inbegrip van persoonsgegevens, kunnen uitwisselen met de nationale computer security incident response teams of bevoegde autoriteiten van derde landen, mits is voldaan aan de voorwaarden van het Uniegegevensbeschermingsrecht inzake doorgifte van persoonsgegevens aan derde landen, onder meer die van artikel 49 van Verordening (EU) 2016/679.

(46) Met het oog op de verwezenlijking van de doelstellingen van deze richtlijn en om de bevoegde autoriteiten en de CSIRT's in staat te stellen de daarin vastgelegde taken uit te voeren, is het van essentieel belang te zorgen voor voldoende middelen. De lidstaten kunnen op nationaal niveau een financieringsmechanisme invoeren om de uitgaven te dekken in verband met de uitvoering van de taken van overheidsinstanties die op grond van deze richtlijn verantwoordelijk zijn voor cyberbeveiliging in de lidstaat. Een dergelijk mechanisme moet in overeenstemming zijn met het Unierecht en moet evenredig en niet-discriminerend zijn en het aanbieden van beveiligde diensten volgens verschillende benaderingen mogelijk maken.

(47) Het CSIRT-netwerk moet blijven bijdragen aan het versterken van het vertrouwen, en snelle en doeltreffende operationele samenwerking tussen de lidstaten blijven bevorderen. Om de operationele samenwerking op het niveau van de Unie te verbeteren, moet het CSIRT-netwerk overwegen om organen en agentschappen van de Unie die betrokken zijn bij het cyberbeveiligingsbeleid, zoals Europol, uit te nodigen om deel te nemen aan zijn werkzaamheden.

(48) Om een hoog niveau van cyberbeveiliging te bereiken en te handhaven, moeten de op grond van deze richtlijn vereiste nationale cyberbeveiligingsstrategieën bestaan uit samenhangende kaders met strategische doelstellingen en prioriteiten op het gebied van cyberbeveiliging en de governance om deze te verwezenlijken. Die strategieën kunnen bestaan uit een of meer wetgevings- of niet-wetgevingsinstrumenten.

(49) Cyberhygiënebeleid vormt de basis voor de bescherming van de infrastructuur, hardware, software en onlinetoepassingen in het kader van netwerk- en informatiesystemen, en van de gegevens van zakelijke gebruikers of eindgebruikers waar entiteiten afhankelijk van zijn. Cyberhygiënebeleid omvat een gemeenschappelijke basisreeks van praktijken, met inbegrip van software- en hardware-updates, de wijziging van wachtwoorden, het beheer van nieuwe installaties, de beperking van toegangsaccounts op beheersniveau en het back-uppen van gegevens, en het maakt een proactief kader mogelijk met betrekking tot paraatheid en algemene veiligheid en beveiliging in geval van incidenten of cyberdreigingen. Enisa moet het cyberhygiënebeleid van de lidstaten monitoren en analyseren.

(50) Cyberbeveiligingsbewustzijn en cyberhygiëne zijn van essentieel belang om het cyberbeveiligingsniveau in de Unie te verhogen, met name in het licht van het toenemende aantal verbonden apparaten waarvan bij cyberaanvallen steeds vaker gebruik wordt gemaakt. Er moeten inspanningen worden geleverd om het algemene bewustzijn van de risico's in verband met dergelijke apparaten te vergroten, terwijl beoordelingen op Unieniveau kunnen bijdragen tot een gemeenschappelijk begrip van dergelijke risico's binnen de interne markt.

(51) De lidstaten moeten het gebruik aanmoedigen van innovatieve technologieën, met inbegrip van artificiële intelligentie, waarvan het gebruik de preventie en de opsporing van cyberaanvallen kan verbeteren, zodat de middelen ter bestrijding van cyberaanvallen doeltreffender kunnen worden ingezet. Daarom moeten de lidstaten in hun nationale cyberbeveiligingsstrategie activiteiten op het gebied van onderzoek en ontwikkeling bevorderen met het oog op het gebruik van dergelijke technologieën, met name die welke verband houden met geautomatiseerde of semigeautomatiseerde instrumenten op het gebied van cyberbeveiliging, en, indien nodig, het delen van gegevens om gebruikers van dergelijke technologieën op te leiden en deze te verbeteren. Het gebruik van innovatieve technologieën, met inbegrip van artificiële intelligentie, moet in overeenstemming zijn met het Uniegegevensbeschermingsrecht, met inbegrip van de gegevensbeschermingsbeginselen van nauwkeurigheid van de gegevens, minimale gegevensverwerking, billijkheid en transparantie, en gegevensbeveiliging, zoals geavanceerde versleuteling. Er moet ten volle worden tegemoetgekomen aan de in Verordening (EU) 2016/679 vastgestelde eisen inzake gegevensbescherming door ontwerp en door standaardinstellingen.

(52) Opensource-instrumenten en -toepassingen voor cyberbeveiliging kunnen bijdragen tot meer openheid en de efficiëntie van industriële innovatie positief beïnvloeden. Open normen bevorderen de interoperabiliteit tussen beveiligingsinstrumenten, wat ten goede komt aan de beveiliging van belanghebbenden uit het bedrijfsleven. Opensource-instrumenten en -toepassingen voor cyberbeveiliging kunnen een hefboomwerking hebben voor de bredere gemeenschap van ontwikkelaars, waardoor diversificatie van leveranciers mogelijk wordt. Dankzij open source kan het proces voor de verificatie van instrumenten voor cyberbeveiliging transparanter verlopen en kan het proces om kwetsbaarheden te ontdekken door de gemeenschap worden aangestuurd. Daarom moet het voor de lidstaten mogelijk zijn om het gebruik van opensourcesoftware en open normen te bevorderen door het nastreven van beleidsmaatregelen die gericht zijn op het gebruik van open data en open source in het kader van beveiliging door transparantie. Beleidsmaatregelen ter bevordering van de invoering en het duurzame gebruik van opensource-instrumenten voor cyberbeveiliging zijn van bijzonder belang voor kleine en middelgrote ondernemingen die te maken krijgen met aanzienlijke uitvoeringskosten, die tot een minimum kunnen worden beperkt door de behoefte aan specifieke toepassingen of instrumenten te verminderen.

(53) Nutsbedrijven zijn in toenemende mate aangesloten op digitale netwerken in steden om de stedelijke vervoersnetwerken te verbeteren, de watervoorziening en afvalverwijderingsinstallaties te moderniseren en gebouwen efficiënter te verlichten en verwarmen. Die gedigitaliseerde nutsbedrijven zijn kwetsbaar voor cyberaanvallen en lopen het risico dat zij burgers bij een succesvolle cyberaanval op grote schaal schade berokkenen doordat zij onderling verbonden zijn. De lidstaten moeten in het kader van hun nationale cyberbeveiligingsstrategie een beleid vaststellen dat gericht is op de ontwikkeling van dergelijke verbonden of slimme steden en de mogelijke gevolgen daarvan voor de samenleving.

(54) De afgelopen jaren is er in de Unie een exponentiële toename van het aantal ransomwareaanvallen, waarbij gegevens en systemen worden vergrendeld met malware en voor de ontgrendeling losgeld moet worden betaald. De toenemende frequentie en ernst van ransomwareaanvallen kan het gevolg zijn van diverse factoren, zoals verschillende aanvalspatronen, criminele bedrijfsmodellen rond "ransomware als dienst" en cryptovaluta, de vraag om losgeld en de toename van aanvallen op de toeleveringsketen. De lidstaten moeten in het kader van hun nationale cyberbeveiligingsstrategie beleidsmaatregelen ontwikkelen om de toename van ransomwareaanvallen aan te pakken.

(55) Publiek-private partnerschappen (PPP's) op het gebied van cyberbeveiliging kunnen een passend kader bieden om kennis en beste praktijken uit te wisselen en te komen tot een gedeeld niveau van inzicht onder de belanghebbenden. De lidstaten moeten beleidsmaatregelen bevorderen ter ondersteuning van de oprichting van specifieke PPP's op het gebied van cyberbeveiliging. In die beleidsmaatregelen moeten met betrekking tot PPP's onder meer de draagwijdte en de betrokken belanghebbenden, het governancemodel, de beschikbare financieringsmogelijkheden en de interactie tussen de deelnemende belanghebbenden worden verduidelijkt. Dankzij PPP's kunnen entiteiten uit de particuliere sector de bevoegde autoriteiten met hun expertise ondersteunen met het oog op de ontwikkeling van geavanceerde diensten en processen, waaronder informatie-uitwisseling, vroegtijdige waarschuwingen, oefeningen betreffende cyberdreigingen en -incidenten, crisisbeheer en weerbaarheidsplanning.

(56) De lidstaten moeten in hun nationale cyberbeveiligingsstrategieën rekening houden met de specifieke behoeften van kleine en middelgrote ondernemingen op het gebied van cyberbeveiliging. Kleine en middelgrote ondernemingen vertegenwoordigen in de hele Unie een groot percentage van de industriële en zakelijke markt en hebben vaak moeite om zich aan te passen aan nieuwe bedrijfspraktijken in een meer verbonden wereld en aan de digitale wereld, met thuiswerkende werknemers en steeds meer online verrichte bedrijfsactiviteiten. Sommige kleine en middelgrote ondernemingen worden geconfronteerd met specifieke uitdagingen op het gebied van cyberbeveiliging, namelijk een beperkt cyberbewustzijn, een gebrek aan IT-beveiliging op afstand, hoge kosten van cyberbeveiligingsoplossingen en een verhoogd dreigingsniveau, onder meer door ransomware, waarvoor zij begeleiding en bijstand moeten krijgen. Kleine en middelgrote ondernemingen worden steeds vaker het doelwit van aanvallen op de toeleveringsketen omdat zij minder strenge maatregelen voor het beheer van cyberbeveiligingsrisico's en aanvalsbeheer nemen, en omdat zij beperkte beveiligingsmiddelen hebben. Dergelijke aanvallen op de toeleveringsketen hebben niet alleen gevolgen voor kleine en middelgrote ondernemingen en hun activiteiten, maar

kunnen ook een cascade-effect veroorzaken en zo leiden tot grotere aanvallen op entiteiten waaraan kleine en middelgrote ondernemingen hebben geleverd. De lidstaten moeten via hun nationale cyberbeveiligingsstrategieën kleine en middelgrote ondernemingen helpen de uitdagingen in hun toeleveringsketen aan te pakken. De lidstaten moeten beschikken over een contactpunt voor kleine en middelgrote ondernemingen op nationaal of regionaal niveau, dat begeleiding en bijstand verleent aan kleine en middelgrote ondernemingen of hen doorverwijst naar de passende instanties voor begeleiding en bijstand met betrekking tot cyberbeveiliging. De lidstaten worden ook aangespoord om diensten zoals websiteconfiguratie en registratiesystemen aan te bieden aan micro-ondernemingen en kleine ondernemingen die niet over deze mogelijkheden beschikken.

(57) De lidstaten moeten in het kader van hun nationale cyberbeveiligingsstrategieën beleidsmaatregelen vaststellen ter bevordering van actieve cyberbescherming in het kader van een bredere verdedigingsstrategie. In plaats van achteraf te reageren, bestaat actieve cyberbescherming uit het actief voorkomen, opsporen, monitoren, analyseren en beperken van inbreuken op de beveiliging van netwerken, in combinatie met het gebruik van capaciteiten die binnen en buiten het netwerk van de slachtoffers worden ingezet. Daarbij kan het gaan om lidstaten die gratis diensten of instrumenten aanbieden aan bepaalde entiteiten, waaronder zelfbedieningscontroles, opsporingsinstrumenten en verwijderingsdiensten. Het vermogen om snel en automatisch informatie over en analyses van dreigingen, cyberactiviteitswaarschuwingen en responsacties te delen en te begrijpen, is van cruciaal belang om gezamenlijke inspanningen mogelijk te maken om aanvallen op netwerk- en informatiesystemen met succes te voorkomen, op te sporen, aan te pakken en tegen te houden. Actieve cyberbescherming is gebaseerd op een verdedigingsstrategie die offensieve maatregelen uitsluit.

(58) Aangezien de exploitatie van kwetsbaarheden in netwerk- en informatiesystemen aanzienlijke verstoringen en schade kan veroorzaken, is het snel identificeren en verhelpen van dergelijke kwetsbaarheden een belangrijke factor in het verminderen van het risico. Entiteiten die netwerk- en informatiesystemen ontwikkelen of beheren, moeten daarom passende procedures vaststellen om kwetsbaarheden aan te pakken wanneer deze worden ontdekt. Aangezien kwetsbaarheden vaak door derden worden ontdekt of bekendgemaakt, moet de fabrikant of aanbieder van ICT-producten of ICT-diensten ook voorzien in de noodzakelijke procedures om kwetsbaarheidsinformatie van derden te ontvangen. In dat verband bieden de internationale normen ISO/IEC 30111 en ISO/IEC 29147 richtsnoeren voor de respons op en de bekendmaking van kwetsbaarheden. Het versterken van de coördinatie tussen de rapporterende natuurlijke personen en rechtspersonen en de fabrikanten of aanbieders van ICT-producten of ICT-diensten is met name van belang ten behoeve van het vrijwillige kader voor de bekendmaking van kwetsbaarheden. De gecoördineerde bekendmaking van kwetsbaarheden duidt een gestructureerd proces aan waarbij kwetsbaarheden aan de fabrikant of aanbieder van de potentieel kwetsbare ICT-producten of ICT-diensten worden gemeld op een manier die deze in staat stelt de kwetsbaarheid te diagnosticeren en te verhelpen voordat gedetailleerde informatie over de kwetsbaarheid aan derden of aan het publiek wordt bekendgemaakt. De gecoördineerde bekendmaking van kwetsbaarheden moet ook betrekking hebben op de coördinatie tussen de rapporterende natuurlijke persoon of rechtspersoon en de fabrikant of aanbieder van de potentieel kwetsbare ICT-producten of ICT-diensten wat betreft het tijdstip van het herstel en de bekendmaking van de kwetsbaarheden.

(59) De Commissie, Enisa en de lidstaten moeten de afstemming op de internationale normen en bestaande beste praktijken van het bedrijfsleven op het gebied van risicobeheer inzake cyberbeveiliging blijven bevorderen, bijvoorbeeld op het gebied van de beoordeling van de beveiliging van de toeleveringsketen, de informatie-uitwisseling en de bekendmaking van kwetsbaarheden.

(60) De lidstaten moeten in samenwerking met Enisa maatregelen nemen om een gecoördineerde bekendmaking van kwetsbaarheden te vergemakkelijken door een relevant nationaal beleid vast te stellen. In het kader van hun nationaal beleid moeten de lidstaten ernaar streven zoveel mogelijk de problemen weg te nemen waar onderzoekers van kwetsbaarheden mee worden geconfronteerd, waaronder hun mogelijke blootstelling aan strafrechtelijke aansprakelijkheid, overeenkomstig het nationale recht. Aangezien natuurlijke en rechtspersonen die onderzoek doen naar kwetsbaarheden in sommige lidstaten strafrechtelijk en civielrechtelijk aansprakelijk kunnen worden gesteld, worden de lidstaten aangespoord richtsnoeren vast te stellen met betrekking tot niet-vervolging van onderzoekers op het gebied van informatiebeveiliging en vrijstelling van civielrechtelijke aansprakelijkheid voor hun activiteiten.

(61) De lidstaten moeten een van hun CSIRT's aanwijzen als coördinator die, indien nodig, optreedt als betrouwbare tussenpersoon tussen de rapporterende natuurlijke of rechtspersonen en de fabrikanten of aanbieders van ICT-producten of ICT-diensten, die waarschijnlijk door de kwetsbaarheid zullen worden getroffen. De taken van het als coördinator aangewezen CSIRT moeten met name bestaan uit het identificeren van en contact opnemen met de betrokken entiteiten, het bijstaan van de natuurlijke of rechtspersonen die een kwetsbaarheid melden, het onderhandelen over tijdschema's voor de bekendmaking en het beheren van kwetsbaarheden die van invloed zijn

op meerdere entiteiten (gecoördineerde bekendmaking van kwetsbaarheden door meerdere partijen). Wanneer de gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan een lidstaat, moeten de als coördinator aangewezen CSIRT's in voorkomend geval binnen het CSIRT-netwerk samenwerken.

(62) Toegang tot correcte en tijdige informatie over kwetsbaarheden die van invloed zijn op ICT-producten en ICT-diensten draagt bij aan een verbeterd risicobeheer inzake cyberbeveiliging. Bronnen van publiek beschikbare informatie over kwetsbaarheden zijn een belangrijk instrument voor de entiteiten en voor de gebruikers van hun diensten, maar ook voor de bevoegde autoriteiten en de CSIRT's. Daarom moet Enisa een Europese kwetsbaarheidsdatabase instellen waarin entiteiten, ongeacht of zij binnen het toepassingsgebied van deze richtlijn vallen, en hun leveranciers van netwerk- en informatiesystemen, evenals de bevoegde autoriteiten en de CSIRT's, op vrijwillige basis algemeen bekende kwetsbaarheden kunnen publiceren en registreren om gebruikers in staat te stellen passende beperkende maatregelen te nemen. Het doel van die database is de unieke uitdagingen aan te pakken die voortvloeien uit de risico's voor entiteiten in de Unie. Voorts moet Enisa voorzien in een passende procedure voor het bekendmakingsproces teneinde entiteiten de tijd te geven om beperkende maatregelen te nemen met betrekking tot hun kwetsbaarheden en gebruik te maken van geavanceerde maatregelen voor het beheer van cyberbeveiligingsrisico's, alsook van machinaal leesbare gegevenssets en bijbehorende interfaces. Om een cultuur van bekendmaking van kwetsbaarheden te bevorderen, mag bekendmaking geen nadelige gevolgen hebben voor de rapporterende natuurlijke persoon of rechtspersoon.

(63) Hoewel er soortgelijke kwetsbaarheidsregisters of -databases bestaan, worden deze gehost en onderhouden door entiteiten die niet in de Unie zijn gevestigd. Een door Enisa bijgehouden Europese kwetsbaarheidsdatabase zou zorgen voor meer transparantie met betrekking tot het bekendmakingsproces voordat de kwetsbaarheid openbaar wordt gemaakt, en voor meer weerbaarheid in geval van een verstoring of een onderbreking van de verlening van soortgelijke diensten. Om dubbel werk te voorkomen en zoveel mogelijk complementariteit na te streven, moet Enisa de mogelijkheid onderzoeken om gestructureerde samenwerkingsovereenkomsten te sluiten met soortgelijke registers of databases die onder de jurisdictie van derde landen vallen. Meer bepaald moet Enisa de mogelijkheid onderzoeken van nauwe samenwerking met de beheerders van het systeem voor gemeenschappelijke kwetsbaarheden en blootstellingen (CVE).

(64) De samenwerkingsgroep moet de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten ondersteunen en bevorderen, en het onderlinge vertrouwen tussen de lidstaten vergroten. De samenwerkingsgroep moet om de twee jaar een werkprogramma vaststellen. Het werkprogramma moet de acties omvatten die de samenwerkingsgroep moet ondernemen om haar doelstellingen en taken uit te voeren. Om mogelijke verstoringen van de werkzaamheden van de samenwerkingsgroep te voorkomen, moet het tijdschema voor de vaststelling van het eerste werkprogramma dat uit hoofde van deze richtlijn wordt vastgesteld, worden afgestemd op het tijdschema van het laatste werkprogramma dat uit hoofde van Richtlijn (EU) 2016/1148 is vastgesteld.

(65) Bij de ontwikkeling van richtsnoeren moet de samenwerkingsgroep consequent nationale oplossingen en ervaringen in kaart brengen, het effect van de resultaten van de samenwerkingsgroep op de nationale aanpak beoordelen, de uitdagingen op het gebied van de uitvoering bespreken en specifieke aanbevelingen formuleren — met name over het vergemakkelijken van de onderlinge afstemming tussen de lidstaten bij de omzetting van deze richtlijn — die moeten worden aangepakt door een betere uitvoering van de bestaande regels. De samenwerkingsgroep kan ook de nationale oplossingen in kaart brengen om compatibele oplossingen op het gebied van cyberbeveiliging die in elke specifieke sector in de Unie worden toegepast, te bevorderen. Dit is met name relevant voor sectoren met een internationaal en grensoverschrijdend karakter.

(66) De samenwerkingsgroep moet een flexibel forum blijven en in staat zijn te reageren op veranderende en nieuwe beleidsprioriteiten en -uitdagingen, rekening houdend met de beschikbaarheid van middelen. Zij kan regelmatig gezamenlijke bijeenkomsten organiseren met relevante particuliere belanghebbenden uit de hele Unie om de activiteiten van de samenwerkingsgroep te bespreken en gegevens en input over nieuwe beleidsuitdagingen te verzamelen. Daarnaast moet de samenwerkingsgroep regelmatig de stand van zaken met betrekking tot cyberdreigingen of -incidenten, zoals ransomware, beoordelen. Om de samenwerking op Unieniveau te versterken, moet de samenwerkingsgroep overwegen de relevante instellingen, organen en instanties van de Unie die betrokken zijn bij het cyberbeveiligingsbeleid, zoals het Europees Parlement, Europol, het Europees Comité voor gegevensbe-

scherming, het bij Verordening (EU) 2018/1139 opgerichte Agentschap van de Europese Unie voor de veiligheid van de luchtvaart en het bij Verordening (EU) 2021/696 van het Europees Parlement en de Raad ([14]) opgerichte Agentschap van de Europese Unie voor het ruimtevaartprogramma, uit te nodigen om deel te nemen aan de werkzaamheden van de groep.

(67) De bevoegde autoriteiten en de CSIRT's moeten kunnen deelnemen aan uitwisselingsprogramma's voor ambtenaren uit andere lidstaten, binnen een specifiek kader en, in voorkomend geval, op voorwaarde dat de ambtenaren die aan dergelijke uitwisselingsprogramma's deelnemen over de vereiste veiligheidsmachtiging beschikken, teneinde de samenwerking te verbeteren en het vertrouwen tussen de lidstaten te versterken. De bevoegde autoriteiten moeten de noodzakelijke maatregelen nemen om ambtenaren uit andere lidstaten in staat te stellen een doeltreffende rol te spelen in de activiteiten van de bevoegde autoriteit van ontvangst of het CSIRT van ontvangst.

(68) De lidstaten moeten bijdragen aan de totstandbrenging van het in Aanbeveling (EU) 2017/1584 van de Commissie ([15]) beschreven EU-kader voor respons op cybercrises via de bestaande samenwerkingsnetwerken, met name het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe), het CSIRT-netwerk en de samenwerkingsgroep. EU-CyCLONe en het CSIRT-netwerk moeten samenwerken op basis van procedurele regelingen waarin die samenwerking nader wordt gespecificeerd en moeten dubbel werk voorkomen. In het reglement van orde van EU-CyCLONe moeten de regelingen voor de werking van dat netwerk nader worden gespecificeerd, met inbegrip van de rollen van het netwerk, de samenwerkingswijzen, de interactie met andere relevante actoren en de modellen voor het delen van informatie, alsmede de communicatiemiddelen. Voor crisisbeheer op Unieniveau moeten de relevante partijen zich baseren op de geïntegreerde Unieregeling politieke crisisrespons overeenkomstig Uitvoeringsbesluit (EU) 2018/1993 van de Raad ([16]) (IPCR-regeling). De Commissie moet daartoe gebruikmaken van het ARGUS-proces voor sectoroverschrijdende crisiscoördinatie op hoog niveau. Als de crisis een belangrijke externe dimensie heeft of raakt aan het gemeenschappelijk veiligheids- en defensiebeleid, moet het crisisresponsmechanisme van de Europese Dienst voor extern optreden worden geactiveerd.

(69) Overeenkomstig de bijlage bij Aanbeveling (EU) 2017/1584 moet onder een grootschalig cyberbeveiligingsincident een incident worden verstaan dat leidt tot een verstoring die te groot is om door een getroffen lidstaat alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten. Afhankelijk van hun oorzaak en gevolgen kunnen grootschalige cyberbeveiligingsincidenten escaleren en veranderen in volwaardige crises die de goede werking van de interne markt niet mogelijk maken of ernstige risico's voor de openbare veiligheid en beveiliging met zich meebrengen voor entiteiten of burgers in verschillende lidstaten of in de Unie als geheel. Gezien het brede toepassingsgebied en in de meeste gevallen het grensoverschrijdende karakter van dergelijke incidenten, moeten de lidstaten en de betrokken instellingen, organen en instanties van de Unie op technisch, operationeel en politiek niveau samenwerken om de respons in de hele Unie naar behoren te coördineren.

(70) Grootschalige cyberbeveiligingsincidenten en crises op het niveau van de Unie vereisen een gecoördineerd optreden om een snelle en doeltreffende respons te waarborgen, gezien de sterke onderlinge verwevenheid tussen sectoren en lidstaten. De beschikbaarheid van cyberbestendige netwerk- en informatiesystemen en de beschikbaarheid, vertrouwelijkheid en integriteit van gegevens zijn van vitaal belang voor de beveiliging van de Unie en voor de bescherming van haar burgers, bedrijven en instellingen tegen incidenten en cyberdreigingen, alsook voor het versterken van het vertrouwen van personen en organisaties in het vermogen van de Unie om een mondiale, open, vrije, stabiele en beveiligde cyberspace te bevorderen en te beschermen die gebaseerd is op de mensenrechten, de fundamentele vrijheden, de democratie en de rechtsstaat.

([14]) Verordening (EU) 2021/696 van het Europees Parlement en de Raad van 28 april 2021 tot vaststelling van het ruimtevaartprogramma van de Unie, tot oprichting van het Agentschap van de Europese Unie voor het ruimtevaartprogramma en tot intrekking van de Verordeningen (EU) nr. 912/2010, (EU) nr. 1285/2013 en (EU) nr. 377/2014 en Besluit nr. 541/2014/EU (PB L 170 van 12.5.2021, blz. 69).

([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).

([16]) Uitvoeringsbesluit (EU) 2018/1993 van de Raad van 11 december 2018 inzake de geïntegreerde EU-regeling politieke crisisrespons (PB L 320 van 17.12.2018, blz. 28).

(71) EU-CyCLONe moet tijdens grootschalige cyberbeveiligingsincidenten en crises fungeren als intermediair netwerk tussen het technische en het politieke niveau, de samenwerking op operationeel niveau versterken en de besluitvorming op politiek niveau ondersteunen. EU-CyCLONe moet, in samenwerking met de Commissie vanwege haar bevoegdheid op het gebied van crisisbeheer, voortbouwen op de bevindingen van het CSIRT-netwerk en zijn eigen capaciteiten gebruiken om een effectbeoordeling van grootschalige cyberbeveiligingsincidenten en crises op te stellen.

(72) Cyberaanvallen hebben een grensoverschrijdend karakter en een significant incident kan kritieke informatie-infrastructuur waarvan de goede werking van de interne markt afhankelijk is, verstoren en beschadigen. Aanbeveling (EU) 2017/1584 heeft betrekking op de rol van alle relevante actoren. Voorts is de Commissie, in het kader van het Uniemechanisme voor civiele bescherming dat is ingesteld bij Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad ([17]), verantwoordelijk voor algemene paraatheidsacties, met inbegrip van het beheren van het Coördinatiecentrum voor respons in noodsituaties en het gemeenschappelijk noodcommunicatie- en informatiesysteem, het onderhouden en verder ontwikkelen van het situationeel bewustzijn en het analysevermogen, en het ontwikkelen en beheren van de noodzakelijke capaciteit om teams van deskundigen te kunnen mobiliseren en uit te zenden in geval van een verzoek om bijstand van een lidstaat of een derde land. De Commissie is ook verantwoordelijk voor het verstrekken van analytische verslagen voor de IPCR-regeling uit hoofde van Uitvoeringsbesluit (EU) 2018/1993, onder meer met betrekking tot situatiekennis en paraatheid op het gebied van cyberbeveiliging, alsook voor situatiekennis en crisisrespons op het gebied van de landbouw, ongunstige weersomstandigheden, het in kaart brengen van conflicten en prognoses, systemen voor vroegtijdige waarschuwing bij natuurrampen, noodsituaties op het gebied van de volksgezondheid, de bewaking van infectieziekten, plantgezondheid, chemische incidenten, de veiligheid van levensmiddelen en diervoeders, diergezondheid, migratie, douane, noodsituaties op nucleair en radiologisch gebied, en energie.

(73) De Unie kan in voorkomend geval overeenkomstig artikel 218 VWEU internationale overeenkomsten met derde landen of internationale organisaties sluiten die hun deelname aan bepaalde activiteiten van de samenwerkingsgroep, het CSIRT-netwerk en EU-CyCLONe mogelijk maken en organiseren. Dergelijke overeenkomsten moeten de belangen van de Unie en de passende bescherming van gegevens waarborgen. Dit mag geen afbreuk doen aan het recht van de lidstaten om met derde landen samen te werken op het gebied van het beheer van kwetsbaarheden en risicobeheer op het gebied van cyberbeveiliging, ter vergemakkelijking van de rapportage en het delen van algemene informatie overeenkomstig het Unierecht.

(74) Om de doeltreffende uitvoering van deze richtlijn te vergemakkelijken, onder meer wat betreft het beheer van kwetsbaarheden, maatregelen voor het beheer van cyberbeveiligingsrisico's, rapportageverplichtingen en informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging, kunnen de lidstaten samenwerken met derde landen en activiteiten ondernemen die daartoe geschikt worden geacht, waaronder informatie-uitwisseling over cyberdreigingen, incidenten, kwetsbaarheden, instrumenten en methoden, tactieken, technieken en procedures, paraatheid en oefeningen betreffende crisisbeheer op het gebied van cyberbeveiliging, opleiding, vertrouwensopbouw en gestructureerde informatie-uitwisselingsregelingen.

(75) Er moeten collegiale toetsingen worden ingevoerd om te helpen leren van gedeelde ervaringen, het wederzijdse vertrouwen te versterken en een hoog gemeenschappelijk niveau van cyberbeveiliging te bereiken. Collegiale toetsingen kunnen leiden tot waardevolle inzichten en aanbevelingen die de algehele cyberbeveiligingscapaciteiten versterken, een ander functioneel traject creëren voor de uitwisseling van beste praktijken tussen de lidstaten en bijdragen tot een hogere mate van maturiteit van de lidstaten op het gebied van cyberbeveiliging. Voorts moeten collegiale toetsingen de resultaten van soortgelijke mechanismen — zoals het systeem voor collegiale toetsing van het CSIRT-netwerk — in aanmerking nemen, en moet zij meerwaarde toevoegen en dubbel werk vermijden. De invoering van collegiale toetsingen mag geen afbreuk doen aan het Unie- of nationale recht inzake de bescherming van vertrouwelijke of gerubriceerde informatie.

(76) De samenwerkingsgroep moet een zelfbeoordelingsmethode voor de lidstaten vaststellen, waarmee wordt beoogd factoren te bestrijken zoals het niveau van uitvoering van de risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging, het capaciteitsniveau en de doeltreffendheid van de uitoefening van de taken van de bevoegde autoriteiten, de operationele capaciteiten van de CSIRT's, het uitvoeringsniveau van wederzijdse bijstand, het uitvoeringsniveau van de informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging, of specifieke kwesties van grens- of sectoroverschrijdende aard. De lidstaten moeten worden aangemoedigd om regelmatig zelfbeoordelingen uit te voeren en de resultaten van hun zelfbeoordeling binnen de samenwerkingsgroep te presenteren en te bespreken.

([17]) Besluit nr. 1313/2013/EU van het Europees Parlement en de Raad van 17 december 2013 betreffende een Uniemechanisme voor civiele bescherming (PB L 347 van 20.12.2013, blz. 924).

(77) De verantwoordelijkheid voor het waarborgen van de beveiliging van netwerk- en informatiesystemen ligt voor een groot deel bij de essentiële en belangrijke entiteiten. Er moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordelingen en de uitvoering van op de risico's afgestemde maatregelen voor het beheer van cyberbeveiligingsrisico's behelst.

(78) Maatregelen voor het beheer van cyberbeveiligingsrisico's moeten worden afgestemd op de mate waarin de essentiële of belangrijke entiteit afhankelijk is van netwerk- en informatiesystemen en moeten maatregelen omvatten om eventuele risico's van incidenten te identificeren, om incidenten te voorkomen, op te sporen, erop te reageren en ervan te herstellen en om de gevolgen ervan te beperken. De beveiliging van netwerk- en informatiesystemen moet de beveiliging van opgeslagen, verzonden en verwerkte gegevens omvatten. Maatregelen voor het beheer van cyberbeveiligingsrisico's moeten voorzien in een systemische analyse, waarbij rekening wordt gehouden met de menselijke factor, om een volledig beeld te krijgen van de beveiliging van het netwerk- en informatiesysteem.

(79) Aangezien bedreigingen voor de beveiliging van netwerk- en informatiesystemen uit verschillende hoeken kunnen komen, moeten maatregelen voor het beheer van cyberbeveiligingsrisico's gebaseerd zijn op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen te beschermen tegen gebeurtenissen die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via netwerk- en informatiesystemen worden aangeboden, in gevaar kunnen brengen, zoals diefstal, brand, overstromingen en telecommunicatie- en stroomstoringen of ongeoorloofde fysieke toegang tot, beschadiging van of interferentie met de informatie- en informatieverwerkingsfaciliteiten van een essentiële of belangrijke entiteit. Bij de maatregelen voor het beheer van cyberbeveiligingsrisico's moet daarom ook aandacht worden besteed aan de fysieke en omgevingsbeveiliging van netwerk- en informatiesystemen, door maatregelen op te nemen om dergelijke systemen te beschermen tegen systeemstoringen, menselijke fouten, kwaadwillige handelingen en natuurverschijnselen, overeenkomstig de Europese en internationale normen, zoals die in de ISO/IEC 27000-reeks. In dat verband moeten essentiële en belangrijke entiteiten in het kader van hun maatregelen voor het beheer van cyberbeveiligingsrisico's ook aandacht besteden aan beveiliging van het personeel en een passend toegangsbeleid voeren. Deze maatregelen moeten in overeenstemming zijn met Richtlijn (EU) 2022/2557.

(80) Om aan te tonen dat de maatregelen voor het beheer van cyberbeveiligingsrisico's worden nageleefd en bij gebrek aan passende Europese regelingen voor cyberbeveiligingscertificering die zijn vastgesteld overeenkomstig Verordening (EU) 2019/881 van het Europees Parlement en de Raad ([18]), moeten de lidstaten, in overleg met de samenwerkingsgroep en de Europese Groep voor cyberbeveiligingscertificering, het gebruik van de relevante Europese en internationale normen door essentiële en belangrijke entiteiten bevorderen of kunnen zij eisen dat entiteiten gecertificeerde ICT-producten, ICT-diensten en ICT-processen gebruiken.

(81) Om te voorkomen dat aan essentiële en belangrijke entiteiten onevenredige financiële en administratieve lasten worden opgelegd, moeten de maatregelen voor het beheer van cyberbeveiligingsrisico's in verhouding staan tot de risico's voor het betrokken netwerk- en informatiesysteem, rekening houdend met de stand van de techniek van dergelijke maatregelen en, in voorkomend geval, de relevante Europese en internationale normen, alsook met de kosten voor de uitvoering ervan.

(82) Maatregelen voor het beheer van cyberbeveiligingsrisico's moeten in verhouding staan tot de mate waarin de essentiële of belangrijke entiteit aan risico's is blootgesteld en de maatschappelijke en economische gevolgen die een incident zou hebben. Bij het vaststellen van maatregelen voor het beheer van cyberbeveiligingsrisico's die zijn aangepast aan essentiële en belangrijke entiteiten, moet terdege rekening worden gehouden met de uiteenlopende mate waarin essentiële en belangrijke entiteiten aan risico's zijn blootgesteld, overeenkomstig het kritieke karakter van de entiteit, de risico's, met inbegrip van maatschappelijke risico's, waaraan de entiteit is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

([18]) 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) (PB L 151 van 7.6.2019, blz. 15).

(83) Essentiële en belangrijke entiteiten moeten de beveiliging van de netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, waarborgen. Die systemen zijn voornamelijk particuliere netwerk- en informatiesystemen die door de interne IT-medewerkers van essentiële en belangrijke entiteiten worden beheerd of waarvan de beveiliging is uitbesteed. De maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen die in deze richtlijn zijn vastgesteld, moeten van toepassing zijn op de relevante essentiële en belangrijke entiteiten, ongeacht of deze entiteiten het onderhoud van hun netwerk- en informatiesystemen intern uitvoeren of uitbesteden.

(84) Gezien het grensoverschrijdende karakter ervan, moeten de regels voor DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten in hoge mate worden geharmoniseerd op het niveau van de Unie. Daarom moet de uitvoering van maatregelen voor het beheer van cyberbeveiligingsrisico's ten aanzien van deze entiteiten worden bevorderd door middel van een uitvoeringshandeling.

(85) Het aanpakken van risico's die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers, zoals leveranciers van diensten op het gebied van gegevensopslag en -verwerking of leveranciers van beheerde beveiligingsdiensten en softwareredacteuren, is bijzonder belangrijk gezien de prevalentie van incidenten waarbij entiteiten het slachtoffer zijn geweest van cyberaanvallen en waarbij kwaadwillende daders de beveiliging van de netwerk- en informatiesystemen van een entiteit in gevaar hebben kunnen brengen door gebruik te maken van kwetsbaarheden die van invloed zijn op producten en diensten van derden. Essentiële en belangrijke entiteiten moeten daarom de algemene kwaliteit en weerbaarheid van de producten en diensten, de daarin vervatte maatregelen voor het beheer van cyberbeveiligingsrisico's, en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners beoordelen en er rekening mee houden, met inbegrip van hun veilige ontwikkelingsprocedures. Essentiële en belangrijke entiteiten moeten met name worden aangespoord om maatregelen voor het beheer van cyberbeveiligingsrisico's op te nemen in de contractuele regelingen met hun directe leveranciers en dienstverleners. Die entiteiten kunnen ook risico's in aanmerking nemen die voortvloeien uit de activiteiten van leveranciers en dienstverleners op een ander niveau.

(86) Onder de dienstverleners spelen aanbieders van beheerde beveiligingsdiensten op het gebied van bijvoorbeeld incidentrespons, penetratietesten, beveiligingsaudits en consultancy een bijzonder belangrijke rol in het bijstaan van entiteiten bij hun inspanningen om incidenten te voorkomen, op te sporen, erop te reageren en ervan te herstellen. Aanbieders van beheerde beveiligingsdiensten zijn echter ook zelf het doelwit van cyberaanvallen geweest en vormen een bijzonder risico vanwege hun nauwe integratie in de activiteiten van de entiteiten. Essentiële en belangrijke entiteiten moeten daarom nog meer zorgvuldigheid betrachten bij de selectie van een aanbieder van beheerde beveiligingsdiensten.

(87) Ook de bevoegde autoriteiten kunnen, in het kader van hun toezichthoudende taken, gebruikmaken van cyberbeveiligingsdiensten zoals beveiligingsaudits, penetratietesten of incidentrespons.

(88) Essentiële en belangrijke entiteiten moeten ook aandacht besteden aan de risico's die voortvloeien uit hun interacties en relaties met andere belanghebbenden binnen een breder ecosysteem, onder meer met betrekking tot de bestrijding van industriële spionage en de bescherming van bedrijfsgeheimen. Die entiteiten moeten met name passende maatregelen nemen om ervoor te zorgen dat hun samenwerking met academische en onderzoeksinstellingen in overeenstemming is met hun cyberbeveiligingsbeleid en dat zij daarbij goede praktijken volgen met betrekking tot veilige toegang en verspreiding van informatie in het algemeen en de bescherming van de intellectuele eigendom in het bijzonder. Evenzo moeten essentiële en belangrijke entiteiten, gezien het belang en de waarde van gegevens voor de activiteiten van die entiteiten, bij het gebruik van gegevenstransformatie- en gegevensanalysediensten van derden, alle passende maatregelen voor het beheer van cyberbeveiligingsrisico's nemen.

(89) Essentiële en belangrijke entiteiten moeten een breed scala aan basispraktijken op het gebied van cyberhygiëne toepassen, zoals zero trust-beginselen, software-updates, configuratie van apparaten, netwerksegmentatie, identiteits- en toegangsbeheer of gebruikersbewustzijn, opleidingen voor hun personeel organiseren en het bewustzijn van cyberdreigingen, phishing of socialengineeringtechnieken vergroten. Voorts moeten die entiteiten hun eigen capaciteiten op het gebied van cyberbeveiliging evalueren en, in voorkomend geval, streven naar de integratie van technologieën ter bevordering van cyberbeveiliging, zoals artificiële intelligentie of machine-leersystemen, om hun capaciteiten en de beveiliging van netwerk- en informatiesystemen te verbeteren.

(90) Om de belangrijkste risico's van de toeleveringsketen verder aan te pakken en essentiële en belangrijke entiteiten die actief zijn in onder deze richtlijn vallende sectoren te helpen om de risico's van de toeleveringsketen en de leveranciers op passende wijze te beheren, moet de samenwerkingsgroep, in samenwerking met de Commissie en Enisa, en in voorkomend geval na raadpleging van de relevante belanghebbenden, onder meer uit het bedrijfsleven, gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens uitvoeren, zoals die welke worden uitgevoerd voor 5G-netwerken naar aanleiding van Aanbeveling (EU) 2019/534 van de Commissie ([19]), met als doel per sector de kritieke ICT-diensten, ICT-systemen of ICT-producten, relevante bedreigingen en kwetsbaarheden vast te stellen. Bij dergelijke gecoördineerde beveiligingsrisicobeoordelingen moeten maatregelen, mitigatieplannen en beste praktijken worden vastgesteld om kritieke afhankelijkheden, mogelijke zwakke punten, bedreigingen, kwetsbaarheden en andere risico's in verband met de toeleveringsketen tegen te gaan, en moet worden nagegaan hoe de bredere toepassing ervan door essentiële en belangrijke entiteiten verder kan worden bevorderd. Mogelijke niet-technische risicofactoren, zoals ongepaste beïnvloeding van leveranciers en dienstverleners door een derde land, met name in het geval van alternatieve governancemodellen, omvatten verborgen kwetsbaarheden of "backdoors" en mogelijke systemische verstoringen van de toelevering, met name in het geval van technologische lock-ins of afhankelijkheid van leveranciers.

(91) Bij de gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens moet er, in het licht van de kenmerken van de betrokken sector, rekening worden gehouden met zowel technische als, in voorkomend geval, niet-technische factoren, met inbegrip van die welke zijn gedefinieerd in Aanbeveling (EU) 2019/534, in de gecoördineerde risicobeoordeling van de cyberbeveiliging van 5G-netwerken in de EU en in het EU-instrumentarium voor 5G-cyberbeveiliging dat door de samenwerkingsgroep is overeengekomen. Om te bepalen welke toeleveringsketens aan een gecoördineerde beveiligingsrisicobeoordeling moeten worden onderworpen, moet rekening worden gehouden met de volgende criteria: i) de mate waarin essentiële en belangrijke entiteiten gebruikmaken van en vertrouwen op specifieke kritieke ICT-diensten, ICT-systemen of ICT-producten; ii) de relevantie van specifieke kritieke ICT-diensten, ICT-systemen of ICT-producten voor het uitvoeren van kritieke of gevoelige functies, met inbegrip van de verwerking van persoonsgegevens; iii) de beschikbaarheid van alternatieve ICT-diensten, ICT-systemen of ICT-producten; iv) de weerbaarheid van de gehele toeleveringsketen van ICT-diensten, ICT-systemen of ICT-producten tegen verstorende gebeurtenissen gedurende hun hele levenscyclus; en v) voor opkomende ICT-diensten, ICT-systemen of ICT-producten, hun potentiële toekomstige betekenis voor de activiteiten van de entiteiten. Voorts moet bijzondere nadruk worden gelegd op ICT-diensten, ICT-systemen of ICT-producten waarvoor specifieke eisen gelden die voortvloeien uit regelgeving van derde landen.

(92) Om de verplichtingen die aan aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten en verleners van vertrouwensdiensten in verband met de beveiliging van hun netwerk- en informatiesystemen worden opgelegd te stroomlijnen, en om die entiteiten en de uit hoofde van Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad ([20]) respectievelijk Verordening (EU) nr. 910/214 bevoegde autoriteiten in staat te stellen gebruik te maken van het bij deze richtlijn vastgestelde rechtskader, met inbegrip van de aanwijzing van een CSIRT dat verantwoordelijk is voor de behandeling van en incidenten, en de deelname van de betrokken bevoegde autoriteiten aan de activiteiten van de samenwerkingsgroep en het CSIRT-netwerk, moeten die entiteiten binnen het toepassingsgebied van deze richtlijn vallen. De overeenkomstige bepalingen van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 met betrekking tot het opleggen van beveiligings- en meldingsvoorschriften aan die soorten entiteiten moeten derhalve worden geschrapt. De in deze richtlijn vastgestelde rapportageverplichtingen mogen geen afbreuk doen aan Verordening (EU) 2016/679 en Richtlijn 2002/58/EG.

(93) De in deze richtlijn vastgelegde cyberbeveiligingsverplichtingen moeten worden beschouwd als een aanvulling op de eisen voor verleners van vertrouwensdiensten uit hoofde van Verordening (EU) nr. 910/2014. Verleners van vertrouwensdiensten moeten worden verplicht alle passende en evenredige maatregelen te nemen om de risico's voor hun diensten te beheren, onder meer ten aanzien van klanten en vertrouwende derden, en incidenten te melden krachtens deze richtlijn. Dergelijke cyberbeveiligings- en rapportageverplichtingen moeten ook betrekking hebben op de fysieke bescherming van de verleende diensten. De in artikel 24 van Verordening (EU) nr. 910/2014 vastgestelde eisen voor gekwalificeerde verleners van vertrouwensdiensten blijven van toepassing.

([19]) Aanbeveling (EU) 2019/534 van de Commissie van 26 maart 2019 — Cyberbeveiliging van 5G-netwerken (PB L 88 van 29.3.2019, blz. 42).

([20]) 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 17.12.2018, blz. 36).

(94) De lidstaten kunnen de rol van de bevoegde autoriteiten voor vertrouwensdiensten toewijzen aan de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 om de voortzetting van de huidige praktijken te waarborgen en voort te bouwen op de bij de toepassing van die verordening opgedane kennis en ervaring. In een dergelijk geval moeten de uit hoofde van deze richtlijn bevoegde autoriteiten nauw en tijdig samenwerken met die toezichthoudende organen door relevante informatie uit te wisselen om doeltreffend toezicht te waarborgen en om ervoor te zorgen dat verleners van vertrouwensdiensten zich houden aan de eisen van deze richtlijn en Verordening (EU) nr. 910/2014. In voorkomend geval moet het CSIRT of de bevoegde autoriteit uit hoofde van deze richtlijn het toezichthoudend orgaan uit hoofde van Verordening (EU) nr. 910/2014 onmiddellijk informeren over alle gemelde significante cyberdreigingen of -incidenten met gevolgen voor vertrouwensdiensten, evenals over alle gevallen waarin een verlener van vertrouwensdiensten inbreuk pleegt op deze richtlijn. Voor de rapportage kunnen de lidstaten in voorkomend geval een beroep doen op het centrale contactpunt dat is ingesteld om te komen tot een gemeenschappelijke en automatische melding van incidenten aan zowel het toezichthoudend orgaan uit hoofde van Verordening (EU) nr. 910/2014 als het CSIRT of de bevoegde autoriteit uit hoofde van deze richtlijn.

(95) In voorkomend geval en om onnodige verstoringen te voorkomen, moet bij de omzetting van deze richtlijn rekening worden gehouden met de bestaande nationale richtsnoeren die zijn vastgesteld voor de omzetting van de in de artikelen 40 en 41 van Richtlijn (EU) 2018/1972 vastgestelde regels met betrekking tot beveiligingsmaatregelen, waarbij moet worden voortgebouwd op de uit hoofde van Richtlijn (EU) 2018/1972 opgedane kennis en vaardigheden inzake beveiligingsmaatregelen en meldingen van incidenten. Enisa kan ook richtsnoeren inzake beveiligingseisen en inzake rapportageverplichtingen opstellen voor aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten, om de harmonisatie en overgang te vergemakkelijken en verstoringen tot een minimum te beperken. De lidstaten kunnen de rol van de bevoegde autoriteiten voor elektronische communicatie toewijzen aan de nationale regelgevende instanties uit hoofde van Richtlijn (EU) 2018/1972 om de voortzetting van de huidige praktijken te waarborgen en voort te bouwen op de met de uitvoering van die richtlijn opgedane kennis en ervaring.

(96) Gezien het toenemende belang van nummeronafhankelijke interpersoonlijke communicatiediensten als gedefinieerd in Richtlijn (EU) 2018/1972, moet ervoor worden gezorgd dat ook voor dergelijke diensten passende beveiligingseisen gelden, gelet op hun specifieke aard en economisch belang. Nu het aanvalsoppervlak blijft groeien, worden nummeronafhankelijke interpersoonlijke communicatiediensten, zoals berichtendiensten, wijdverbreide aanvalsvectoren. Kwaadwillende daders maken gebruik van platforms om te communiceren met slachtoffers en hen ertoe aan te zetten gecompromitteerde webpagina's te openen, waardoor de kans toeneemt op incidenten waarbij onrechtmatig gebruik van persoonsgegevens en, bij uitbreiding, de beveiliging van netwerk- en informatiesystemen betrokken is. Aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten moeten zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's. Aangezien aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten normaal gesproken geen daadwerkelijke controle uitoefenen op de overdracht van signalen over netwerken, kunnen de risico's in sommige opzichten als lager worden beschouwd voor dergelijke diensten dan voor traditionele elektronischecommunicatiediensten. Hetzelfde geldt voor interpersoonlijke communicatiediensten als gedefinieerd in Richtlijn (EU) 2018/1972 die gebruikmaken van nummers en die geen daadwerkelijke controle uitoefenen op de signaaloverdracht.

(97) De interne markt is meer dan ooit afhankelijk van het functioneren van het internet. De diensten van vrijwel alle essentiële en belangrijke entiteiten zijn afhankelijk van via het internet verleende diensten. Om voor een soepele dienstverlening door essentiële en belangrijke entiteiten te zorgen, is het van belang dat alle aanbieders van openbare elektronischecommunicatienetwerken over passende maatregelen voor het beheer van cyberbeveiligingsrisico's beschikken en significante incidenten in verband daarmee melden. De lidstaten moeten ervoor zorgen dat de beveiliging van de openbare elektronischecommunicatienetwerken wordt gehandhaafd en dat hun wezenlijke veiligheidsbelangen worden beschermd tegen sabotage en spionage. Aangezien de internationale connectiviteit de op het concurrentievermogen gerichte digitalisering van de Unie en haar economie verbetert en versnelt, moeten incidenten in verband met onderzeese communicatiekabels worden gemeld aan het CSIRT of, in voorkomend geval, de bevoegde autoriteit. De nationale cyberbeveiligingsstrategie moet in voorkomend geval worden afgestemd op de cyberbeveiliging van onderzeese communicatiekabels en om het hoogste niveau van bescherming daarvan te waarborgen, moet zij een inventarisatie omvatten van mogelijke cyberbeveiligingsrisico's en beperkende maatregelen.

(98) Om de beveiliging van openbare elektronischecommunicatienetwerken en openbare elektronischecommunicatiediensten te waarborgen, moet het gebruik van encryptietechnologieën, met name eind-tot-eindcodering evenals gegevensgerichte beveiligingsconcepten, zoals cartografie, segmentatie, markeringen, toegangsbeleid en -beheer, en geautomatiseerde toegangsbesluiten, worden bevorderd. Waar nodig moet het gebruik van encryptie, met name eind-tot-eindcodering, verplicht worden gesteld voor aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten, overeenkomstig de beginselen van beveiliging en privacy, standaard en door het ontwerp, voor de doeleinden van deze richtlijn. Het gebruik van eind-tot-eindcodering moet aansluiten op de bevoegdheden van de lidstaten om de bescherming van hun wezenlijke veiligheidsbelangen en de openbare veiligheid te waarborgen en om de preventie, het onderzoek, de opsporing en de vervolging van strafbare feiten overeenkomstig het Unierecht mogelijk te maken. Dit mag echter niet leiden tot verzwakking van de eind-tot-eindcodering, een kritieke technologie met het oog op een doeltreffende gegevensbescherming en privacy en beveiliging van de communicatie.

(99) Om de beveiliging van openbare elektronischecommunicatienetwerken en openbare elektronischecommunicatiediensten te waarborgen en misbruik en manipulatie te voorkomen, moet het gebruik van normen voor veilige routering worden bevorderd om de integriteit en robuustheid van routeringsfuncties in het ecosysteem van aanbieders van internettoegangsdiensten te waarborgen.

(100) Om de functionaliteit en integriteit van het internet te waarborgen en de beveiliging en weerbaarheid van het DNS te bevorderen, moeten de relevante belanghebbenden, waaronder entiteiten uit de particuliere sector in de Unie, aanbieders van openbare elektronischecommunicatiediensten, met name aanbieders van internettoegangsdiensten en aanbieders van onlinezoekmachines, worden aangespoord om een strategie voor diversificatie van de DNS-omzetting vast te stellen. Daarnaast moeten de lidstaten de ontwikkeling en het gebruik van een openbare en beveiligde Europese dienst voor DNS-omzetting bevorderen.

(101) Deze richtlijn voorziet in een aanpak in meerdere fasen van de melding van significante incidenten om het juiste evenwicht te vinden tussen enerzijds een snelle melding die de potentiële verspreiding van significante incidenten helpt te beperken en essentiële en belangrijke entiteiten in staat stelt om bijstand te vragen, en anderzijds een grondige melding die het mogelijk maakt waardevolle lessen te trekken uit afzonderlijke incidenten en mettertijd de digitale weerbaarheid van afzonderlijke entiteiten en hele sectoren verbetert. In dat verband moet deze richtlijn ook de melding omvatten van incidenten die, op basis van een door de betrokken entiteit uitgevoerde initiële beoordeling, ernstige operationele verstoring van de dienstverlening of financiële verliezen voor die entiteit kunnen veroorzaken of andere natuurlijke of rechtspersonen kunnen treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Bij een dergelijke initiële beoordeling moet rekening worden gehouden met onder meer de getroffen netwerk- en informatiesystemen, en met name het belang daarvan voor de door de entiteit verleende diensten, de ernst en technische kenmerken van een cyberdreiging en eventuele onderliggende kwetsbaarheden die worden uitgebuit, alsook de ervaring van de entiteit met soortgelijke incidenten. Indicatoren zoals de mate waarin de werking van de dienst wordt aangetast, de duur van een incident of het aantal getroffen afnemers van de diensten kunnen van belang zijn om vast te stellen of er sprake is van een ernstige operationele verstoring van de dienst.

(102) Wanneer essentiële of belangrijke entiteiten zich bewust worden van een significant incident, moeten zij verplicht worden onverwijld en in elk geval binnen 24 uur een vroegtijdige waarschuwing te verstrekken. Die vroegtijdige waarschuwing moet worden gevolgd door de melding van het incident. De betrokken entiteiten moeten onverwijld en in elk geval binnen 72 uur nadat zij zich bewust worden van een significant incident, melding doen van dat incident, met name om de informatie bij te werken die bij de vroegtijdige waarschuwing is ingediend en om een initiële beoordeling van het significante incident kenbaar te maken, met inbegrip van de ernst en de gevolgen ervan, alsook, indien beschikbaar, indicatoren voor aantasting. Uiterlijk een maand na de melding van het incident moet een eindverslag worden ingediend. De vroegtijdige waarschuwing mag enkel de informatie bevatten die noodzakelijk is om het CSIRT of, in voorkomend geval, de bevoegde autoriteit op de hoogte te brengen van het significante incident en de betrokken entiteit in staat te stellen om indien nodig bijstand te vragen. In voorkomend geval moet bij deze vroegtijdige waarschuwing worden aangegeven of het significante incident vermoedelijk door onrechtmatige of kwaadwillige handelingen is veroorzaakt en of het waarschijnlijk grensoverschrijdende gevolgen heeft. De lidstaten moeten ervoor zorgen dat de verplichting om die vroegtijdige waarschuwing of de daaropvolgende melding van het incident in te dienen de middelen van de meldende entiteit niet afleidt van activiteiten die verband houden met de behandeling van het incident en die als prioritair moeten worden aangemerkt, teneinde te voorkomen dat de

verplichtingen inzake de melding van incidenten middelen onttrekken aan de respons op significante incidenten of de inspanningen van de entiteit op dat gebied anderszins in gevaar brengen. Indien het incident nog aan de gang is op het moment dat het eindverslag wordt ingediend, moeten de lidstaten ervoor zorgen dat de betrokken entiteiten op dat moment een voortgangsverslag indienen en binnen één maand nadat het significante incident is afgehandeld, een eindverslag indienen.

(103) In voorkomend geval moeten essentiële en belangrijke entiteiten de ontvangers van hun diensten onverwijld in kennis stellen van alle maatregelen of voorzieningen die hun ter beschikking staan om de uit een significante cyberdreiging voortvloeien risico's te beperken. In voorkomend geval, en met name wanneer de significante cyberdreigingen waarschijnlijk tot incidenten zullen leiden, moeten die entiteiten de ontvangers van hun dienst ook op de hoogte brengen van de dreiging zelf. De eis om die ontvangers van significante cyberdreigingen op de hoogte te brengen, moet naar best vermogen in acht worden genomen, maar mag de entiteiten niet ontslaan van de verplichting om op eigen kosten passende en onmiddellijke maatregelen te nemen om dergelijke dreigingen te voorkomen of te verhelpen en het normale beveiligingsniveau van de dienst te herstellen. Dergelijke informatie over significante cyberdreigingen aan de ontvangers van de dienst moet gratis worden verstrekt en in gemakkelijk te begrijpen taal worden opgesteld.

(104) De aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten moeten standaard en door het ontwerp beveiliging bieden en hun dienstontvangers op de hoogte brengen van significante cyberdreigingen en van de maatregelen die zij kunnen nemen om de beveiliging van hun apparaten en communicatie te beschermen, bijvoorbeeld door gebruik te maken van specifieke soorten software of encryptietechnologieën.

(105) Een proactieve aanpak van cyberdreigingen is een onmisbaar onderdeel van het beheer van cyberbeveiligingsrisico's en moet ervoor zorgen dat de bevoegde autoriteiten daadwerkelijk kunnen voorkomen dat cyberdreigingen tot incidenten leiden die aanzienlijke materiële of immateriële schade kunnen veroorzaken. Daartoe is het van cruciaal belang dat cyberdreigingen worden gemeld. Daarom worden de entiteiten aangespoord om op vrijwillige basis melding te maken van cyberdreigingen.

(106) Om de rapportage van de krachtens deze richtlijn vereiste informatie te vereenvoudigen en de administratieve lasten voor entiteiten te verminderen, moeten de lidstaten technische middelen ter beschikking stellen, zoals één centraal contactpunt, geautomatiseerde systemen, onlineformulieren, gebruikersvriendelijke interfaces, modellen en specifieke platforms ten behoeve van entiteiten, ongeacht of zij binnen het toepassingsgebied van deze richtlijn vallen, voor de indiening van de relevante te rapporteren informatie. De Uniefinanciering ter ondersteuning van de uitvoering van deze richtlijn, met name in het kader van het programma Digitaal Europa, dat is vastgesteld bij Verordening (EU) 2021/694 van het Europees Parlement en de Raad ([21]), kan steun voor centrale contactpunten omvatten. Bovendien bevinden entiteiten zich vaak in een situatie waarin een bepaald incident, vanwege de kenmerken ervan, aan verschillende autoriteiten moet worden gemeld als gevolg van meldingsverplichtingen die in verschillende rechtsinstrumenten zijn opgenomen. Dergelijke gevallen creëren extra administratieve lasten en kunnen ook leiden tot onzekerheden met betrekking tot het format en de procedures van dergelijke meldingen. Wanneer één enkel toegangspunt is ingesteld, worden de lidstaten aangespoord om dat ene centrale toegangspunt ook te gebruiken voor de melding van beveiligingsincidenten als vereist krachtens ander Unierecht zoals Verordening (EU) 2016/679 en Richtlijn 2002/58/EG. Het gebruik van het ene centrale contactpunt voor de melding van beveiligingsincidenten krachtens Verordening (EU) 2016/679 en Richtlijn 2002/58/EG mag geen afbreuk doen aan de toepassing van de bepalingen van Verordening (EU) 2016/679 en Richtlijn 2002/58/EG, en met name de bepalingen met betrekking tot de onafhankelijkheid van de daarin bedoelde autoriteiten. Enisa moet, in samenwerking met de samenwerkingsgroep, gemeenschappelijke meldingsmodellen ontwikkelen door middel van richtsnoeren om de krachtens het Unierecht te rapporteren informatie te vereenvoudigen en te stroomlijnen en de administratieve lasten voor meldende entiteiten te verminderen.

(107) Wanneer het vermoeden bestaat dat een incident verband houdt met ernstige criminele activiteiten op grond van het Unie- of nationale recht, moeten de lidstaten essentiële en belangrijke entiteiten aansporen om, op basis van de toepasselijke regels voor strafrechtelijke procedures overeenkomstig het Unierecht, incidenten met een vermoedelijk ernstig crimineel karakter aan de betrokken rechtshandhavingsinstanties te melden. In voorkomend geval en onverminderd de voor Europol geldende regels inzake de bescherming van persoonsgegevens is het wenselijk dat de coördinatie tussen de bevoegde autoriteiten en de rechtshandhavingsinstanties van de verschillende lidstaten wordt vergemakkelijkt door het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3) en Enisa.

([21]) Verordening (EU) nr. 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 (PB L 166 van 11.5.2021, blz. 1).

(108) Persoonsgegevens worden in veel gevallen in gevaar gebracht als gevolg van incidenten. In dat verband moeten de bevoegde autoriteiten samenwerken en informatie uitwisselen over alle relevante aangelegenheden met de in Verordening (EU) 2016/679 en Richtlijn 2002/58/EG bedoelde autoriteiten.

(109) Het onderhouden van nauwkeurige en volledige databases van domeinnaamregistratiegegevens ("WHOIS-gegevens") en het verlenen van rechtmatige toegang tot dergelijke gegevens is essentieel om de beveiliging, stabiliteit en weerbaarheid van het DNS te waarborgen, wat op zijn beurt bijdraagt tot een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie. Voor dat specifieke doel moeten registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verplicht worden bepaalde gegevens te verwerken die daartoe nodig zijn. Een dergelijke verwerking moet een wettelijke verplichting vormen in de zin van artikel 6, lid 1, punt c), van Verordening (EU) 2016/679. Die verplichting doet geen afbreuk aan de mogelijkheid om domeinnaamregistratiegegevens voor andere doeleinden te verzamelen, bijvoorbeeld op basis van in ander Unierecht of in het nationale recht vastgestelde wettelijke eisen of contractuele regelingen. Die verplichting heeft tot doel te komen tot een volledige en nauwkeurige reeks registratiegegevens en mag niet ertoe leiden dat dezelfde gegevens meermaals worden verzameld. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten met elkaar samenwerken om dubbel werk te voorkomen.

(110) De beschikbaarheid en tijdige toegankelijkheid van domeinnaamregistratiegegevens voor verzoekers om legitieme toegang is van essentieel belang om misbruik van het DNS te voorkomen en te bestrijden en om incidenten te voorkomen, op te sporen en erop te reageren. Onder verzoeker om legitieme toegang wordt verstaan elke natuurlijke of rechtspersoon die een verzoek indient krachtens het Unie- of nationale recht. Het kan gaan om autoriteiten die uit hoofde van deze richtlijn bevoegd zijn en om autoriteiten die krachtens het Unie- of nationale recht bevoegd zijn voor het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, evenals om CERT's of CSIRT's. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten worden verplicht om rechtmatige toegang tot specifieke domeinnaamregistratiegegevens, die nodig zijn voor de doeleinden van het toegangsverzoek, te verlenen aan verzoekers om legitieme toegang, overeenkomstig het Unierecht en het nationale recht. Het verzoek van verzoekers om legitieme toegang moet vergezeld gaan van een motivering aan de hand waarvan kan worden beoordeeld of toegang tot de gegevens noodzakelijk is.

(111) Om de beschikbaarheid van nauwkeurige en volledige domeinnaamregistratiegegevens te waarborgen, moeten registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen , domeinnaamregistratiegegevens verzamelen en de integriteit en beschikbaarheid ervan waarborgen. Met name registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten beleid en procedures vaststellen om nauwkeurige en volledige domeinnaamregistratiegegevens te verzamelen en bij te houden en om onjuiste registratiegegevens te voorkomen en te corrigeren, in overeenstemming met het Uniegegevensbeschermingsrecht. Uit hoofde van dat beleid en die procedures moet zoveel mogelijk rekening worden gehouden met de normen die zijn ontwikkeld door de structuren voor multistakeholdergovernance op internationaal niveau. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten evenredige procedures vaststellen en toepassen om domeinnaamregistratiegegevens te verifiëren. Die procedures moeten de beste praktijken in het bedrijfsleven en, voor zover mogelijk, de vooruitgang op het gebied van elektronische identificatie weerspiegelen. Voorbeelden van verificatieprocedures kunnen betrekking hebben op controles vooraf die worden uitgevoerd bij de registratie, en controles achteraf die worden uitgevoerd na de registratie. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, moeten met name ten minste een van de manieren om met de registrant contact op te nemen, verifiëren.

(112) Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten worden verplicht domeinnaamregistratiegegevens die buiten het toepassingsgebied van het Uniegegevensbeschermingsrecht vallen openbaar te maken, zoals gegevens die betrekking hebben op rechtspersonen, overeenkomstig de preambule van Verordening (EU) 2016/679. Voor rechtspersonen moeten registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen ten minste de naam en het telefoonnummer van de registrant openbaar maken. Ook het e-mailadres moet bekend worden gemaakt, op voorwaarde dat het geen persoonsgegevens bevat, zoals bij e-mailaliassen of functionele mailboxen. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten ook rechtmatige toegang tot specifieke domeinnaamregistratiegegevens over natuurlijke personen verlenen aan verzoekers om legitieme toegang, overeenkomstig het Uniegegevensbeschermingsrecht. De lidstaten moeten van registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verlangen dat zij onverwijld reageren op verzoeken van verzoekers om legitieme toegang om openbaarmaking van domeinnaamregistratiegegevens. Registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, moeten beleid en procedures vaststellen voor de bekendmaking en openbaarmaking van registratiegegevens, met inbegrip van overeenkomsten inzake het dienstverleningsniveau voor de behandeling van verzoeken om toegang van verzoekers om legitieme toegang. In het kader

van dat beleid en die procedures moet zoveel mogelijk rekening worden gehouden met alle richtsnoeren en met de normen die zijn ontwikkeld door de structuren voor multistakeholdergovernance op internationaal niveau. De toegangsprocedure kan het gebruik van een interface, een portaal of een ander technisch hulpmiddel omvatten om een efficiënt systeem te bieden voor het aanvragen en raadplegen van registratiegegevens. Met het oog op de bevordering van geharmoniseerde praktijken in de gehele interne markt kan de Commissie zonder afbreuk te doen aan de bevoegdheden van het Europees Comité voor gegevensbescherming richtsnoeren voor dergelijke procedures bepalen, waarin zoveel mogelijk rekening wordt gehouden met de normen die zijn ontwikkeld door de structuren voor multistakeholdergovernance op internationaal niveau. De lidstaten moeten ervoor zorgen dat alle vormen van toegang tot persoonsgebonden en niet-persoonsgebonden domeinnaamregistratiegegevens gratis zijn.

(113) Binnen het toepassingsgebied van deze richtlijn vallende entiteiten moeten worden geacht te vallen onder de jurisdictie van de lidstaat waar zij zijn gevestigd. Aanbieders van openbare elektronischecommunicatienetwerken of aanbieders van openbare elektronischecommunicatiediensten moeten evenwel worden geacht te vallen onder de jurisdictie van de lidstaat waar zij hun diensten verlenen. DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten moeten worden geacht te vallen onder de jurisdictie van de lidstaat waar zij hun hoofdvestiging in de Unie hebben. Overheidsinstanties moeten vallen onder de jurisdictie van de lidstaat die ze heeft opgericht. Indien de entiteit diensten verleent of gevestigd is in meer dan één lidstaat, moet zij vallen onder de afzonderlijke en gelijktijdige jurisdictie van elk van die lidstaten. De bevoegde autoriteiten van die lidstaten moeten samenwerken, elkaar wederzijds bijstand verlenen en, in voorkomend geval, gezamenlijke toezichtsacties uitvoeren. Wanneer lidstaten hun jurisdictie uitoefenen, mogen zij overeenkomstig het ne bis in idem-beginsel niet meer dan één keer handhavingsmaatregelen of sancties opleggen voor dezelfde gedraging.

(114) Om rekening te houden met het grensoverschrijdende karakter van de diensten en activiteiten van DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, mag slechts één lidstaat jurisdictie hebben over die entiteiten. Deze jurisdictie moet worden toegekend aan de lidstaat waar de betrokken entiteit haar hoofdvestiging in de Unie heeft. Het vestigingscriterium voor de toepassing van deze richtlijn houdt de daadwerkelijke uitoefening van de activiteit in door middel van stabiele regelingen. De rechtsvorm van dergelijke regelingen, hetzij via een filiaal, hetzij via een dochteronderneming met rechtspersoonlijkheid, is in dat opzicht geen bepalende factor. Of aan dat criterium wordt voldaan, mag niet afhangen van de vraag of de netwerk- en informatiesystemen zich fysiek op een bepaalde plaats bevinden; de aanwezigheid en het gebruik van dergelijke systemen vormen op zich niet een dergelijke hoofdvestiging en zijn dus geen doorslaggevende criteria voor het bepalen van de hoofdvestiging. De hoofdvestiging moet geacht worden zich te bevinden in de lidstaat waar de besluiten met betrekking tot de risicobeheersmaatregelen op het gebied van cyberbeveiliging hoofdzakelijk worden genomen in de Unie. Dit zal doorgaans overeenkomen met de plaats van de centrale administratie van de entiteiten in de Unie. Indien niet kan worden bepaald welke lidstaat dat is of indien dergelijke besluiten niet in de Unie worden genomen, moet de hoofdvestiging worden geacht zich te bevinden in de lidstaat waar cyberbeveiligingsactiviteiten worden uitgevoerd. Indien niet kan worden bepaald welke lidstaat dat is, moet de hoofdvestiging worden geacht zich te bevinden in de lidstaat waar de entiteit de vestiging met het grootste aantal werknemers in de Unie heeft. Wanneer de diensten door een groep van ondernemingen worden verricht, moet de hoofdvestiging van de zeggenschap uitoefenende onderneming worden beschouwd als de hoofdvestiging van de groep van ondernemingen.

(115) Indien een aanbieder van openbare elektronischecommunicatienetwerken of openbare elektronischecommunicatiediensten een openbare recursieve DNS-dienst enkel verricht als onderdeel van de internettoegangsdienst, moet de entiteit worden geacht te vallen onder de jurisdictie van alle lidstaten waar haar diensten worden verleend.

(116) Indien een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteiten die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentra, een aanbieder van netwerken voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten, niet in de Unie is gevestigd maar diensten in de Unie aanbiedt, moet deze een vertegenwoordiger in de Unie aanduiden. Om te bepalen of een dergelijke entiteit diensten binnen de Unie aanbiedt, moet worden nagegaan of de entiteit van plan is diensten aan te bieden aan personen in een of meer lidstaten. De loutere toegankelijkheid in de Unie van de website van de entiteit of van een tussenpersoon, of van een e-mailadres of van andere contactgegevens, of het gebruik van een taal die algemeen wordt gebruikt in het derde land waar de entiteit is gevestigd, moet als zodanig onvoldoende worden geacht om een dergelijk voornemen vast te stellen. Factoren zoals het gebruik van een taal of een valuta die in een of meer lidstaten algemeen wordt gebruikt en de mogelijkheid om diensten in die taal te bestellen, of de vermelding van klanten of gebruikers die zich in de Unie bevinden, kunnen echter duidelijk maken dat de entiteit van plan is om diensten binnen de Unie aan te bieden. De vertegenwoordiger moet namens de entiteit optreden en de bevoegde autoriteiten of de CSIRT's moeten zich kunnen wenden tot de vertegenwoordiger. De vertegenwoordiger moet uitdrukkelijk bij schriftelijke opdracht van de entiteit worden aangewezen om namens de entiteit op te treden met betrekking tot in deze richtlijn vastgelegde verplichtingen, met inbegrip van de melding van incidenten.

(117) Ten behoeve van een duidelijk overzicht van DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, die in de gehele Unie binnen het toepassingsgebied van deze richtlijn vallende diensten verlenen, moet Enisa zorgen voor de oprichting en het beheer van een register van dergelijke entiteiten, gebaseerd op de door lidstaten verstrekte informatie en indien nodig met behulp van nationale mechanismen voor zelfregistratie door entiteiten. De centrale contactpunten moeten de informatie en eventuele wijzigingen daarvan doorsturen naar Enisa. Met het oog op de nauwkeurigheid en volledigheid van de informatie die in dit register moet worden opgenomen, kunnen lidstaten Enisa de informatie verstrekken die betreffende die entiteiten beschikbaar is in hun nationale registers. Enisa en de lidstaten moeten maatregelen nemen om de interoperabiliteit van dergelijke registers te bevorderen, en tegelijkertijd de bescherming van vertrouwelijke of gerubriceerde informatie waarborgen. Enisa moet passende protocollen voor de rubricering en het beheer van informatie opstellen om de veiligheid en vertrouwelijkheid van gerapporteerde informatie te garanderen, en de toegang, opslag en doorgifte van die informatie te beperken tot de beoogde gebruikers.

(118) Wanneer er uit hoofde van deze richtlijn informatie wordt uitgewisseld, gerapporteerd of anderszins gedeeld die volgens het Unie- of nationale recht gerubriceerd is, moet toepassing worden gemaakt van de desbetreffende regels voor de behandeling van gerubriceerde informatie. Bovendien moet Enisa over de benodigde infrastructuur, procedures en regels beschikken om gevoelige en gerubriceerde informatie te kunnen verwerken overeenkomstig de toepasselijke beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie.

(119) Aangezien cyberdreigingen complexer en geavanceerder worden, zijn een goede opsporing van dergelijke dreigingen en preventiemaatregelen dienaangaande voor een groot deel afhankelijk van het regelmatige delen van inlichtingen over dreigingen en kwetsbaarheden tussen entiteiten. Het delen van informatie draagt bij aan een grotere bewustwording van cyberdreigingen, wat op zijn beurt het vermogen van entiteiten om te voorkomen dat zulke dreigingen tot echte incidenten leiden, vergroot en entiteiten in staat stelt om de gevolgen van incidenten beter in te dammen en efficiënter te herstellen. Bij gebrek aan richtsnoeren op Unieniveau lijken verschillende factoren een dergelijk delen van inlichtingen te hebben afgeremd, met name de onzekerheid over de verenigbaarheid met de mededingings- en aansprakelijkheidsregels.

(120) Entiteiten moeten worden aangemoedigd en bijgestaan door de lidstaten om hun individuele kennis en praktische ervaring op strategisch, tactisch en operationeel niveau collectief te benutten met het oog op de verbetering van hun capaciteiten om incidenten adequaat te voorkomen, op te sporen, er een antwoord op te bieden, ervan te herstellen of de impact ervan af te beperken. Het is dus noodzakelijk om op Unieniveau de opkomst van vrijwillige regelingen voor het delen van cyberbeveiligingsinformatie mogelijk te maken. Daarom moeten de lidstaten entiteiten, zoals die welke cyberbeveiligingsdiensten en -onderzoek aanbieden, alsook niet binnen het toepassingsgebied van deze richtlijn vallende relevante entiteiten, actief bijstaan en aanmoedigen om deel te nemen aan dergelijke regelingen voor het delen van cyberbeveiligingsinformatie. Deze regelingen moeten in overeenstemming zijn met de mededingingsregels van de Unie en het Uniegegevensbeschermingsrecht.

(121) De verwerking van persoonsgegevens, voor zover noodzakelijk en evenredig met het oog op de beveiliging van netwerk- en informatiesystemen door essentiële en belangrijke entiteiten, kan als rechtmatig worden beschouwd op grond van het feit dat dergelijke verwerking voldoet aan een wettelijke verplichting waaraan de verwerkingsverantwoordelijke onderworpen is overeenkomstig de eisen van artikel 6, lid 1, punt c), en artikel 6, lid 3, van Verordening (EU) 2016/679. De verwerking van persoonsgegevens kan ook noodzakelijk zijn voor de behartiging van de gerechtvaardigde belangen van essentiële en belangrijke entiteiten, alsook van aanbieders van beveiligingstechnologieën en -diensten die namens die entiteiten optreden, op grond van artikel 6, lid 1, punt f), van Verordening (EU) 2016/679, onder meer wanneer een dergelijke verwerking noodzakelijk is voor regelingen voor het delen van cyberbeveiligingsinformatie of de vrijwillige melding van relevante informatie overeenkomstig deze richtlijn. Maatregelen met betrekking tot de preventie, opsporing, identificatie, indamming en analyse van incidenten en de reactie erop, maatregelen om het bewustzijn met betrekking tot specifieke cyberdreigingen te vergroten, uitwisseling van informatie in het kader van herstel van de kwetsbaarheid en gecoördineerde openbaarmaking van de kwetsbaarheid, de vrijwillige uitwisseling van informatie over die incidenten, alsmede cyberdreigingen en kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen kunnen de verwerking vereisen van bepaalde categorieën persoonsgegevens, zoals IP-adressen, uniforme resources locators (URL's), domeinnamen, e-mailadressen en, voor zover hieruit persoonsgegevens blijken, tijdstempels. De verwerking van persoonsgegevens door de bevoegde autoriteiten, de centrale contactpunten en de CSIRT's kan een wettelijke verplichting vormen of noodzakelijk worden geacht voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen op grond van artikel 6, lid 1, punt c) of e), en artikel 6, lid 3, van Verordening (EU) 2016/679, of voor de behartiging van een gerechtvaardigd belang van de essentiële en belangrijke entiteiten als bedoeld in artikel 6, lid 1, punt f), van die verordening. Voorts kunnen in het nationale recht regels worden vastgesteld die het de bevoegde autoriteiten, de centrale contactpunten en de CSIRT's, voor zover noodzakelijk en evenredig ten behoeve van het waarborgen van de beveiliging van netwerk- en informatiesystemen van essentiële en belangrijke entiteiten, toelaten om bijzondere categorieën van persoonsgegevens te verwerken overeenkomstig artikel 9 van Verordening (EU) 2016/679, met name door te voorzien in passende en specifieke maatregelen ter bescherming van de grondrechten en de belangen van natuurlijke personen, met inbegrip van technische beperkingen op het hergebruik van dergelijke gegevens en het gebruik van geavanceerde beveiligings- en privacybeschermingsmaatregelen, zoals pseudonimisering, of versleuteling wanneer anonimisering het nagestreefde doel aanzienlijk kan beïnvloeden.

(122) Ter versterking van de toezichtsbevoegdheden en -maatregelen die bijdragen tot een doeltreffende naleving, moet deze richtlijn voorzien in een minimumlijst van toezichtsmaatregelen en -middelen waarmee de bevoegde autoriteiten toezicht kunnen houden op essentiële en belangrijke entiteiten. Bovendien moet in deze richtlijn een onderscheid worden gemaakt tussen de toezichtsregeling voor essentiële en voor belangrijke entiteiten, teneinde te zorgen voor een billijk evenwicht tussen de verplichtingen voor die entiteiten en voor de bevoegde autoriteiten. Derhalve moeten essentiële entiteiten worden onderworpen aan een alomvattende regeling voor toezicht vooraf en achteraf, terwijl belangrijke entiteiten slechts moeten worden onderworpen aan een lichte regeling voor toezicht, uitsluitend achteraf. Van belangrijke entiteiten mag daarom niet worden verlangd dat zij systematisch de naleving van de risicobeheersmaatregelen op het gebied van cyberbeveiliging documenteren, aangezien de bevoegde autoriteiten het toezicht reactief en achteraf moeten uitvoeren en dus geen algemene verplichting hebben om toezicht te houden op die entiteiten. Het toezicht achteraf ten aanzien van belangrijke entiteiten kan worden geactiveerd wanneer bewijzen, aanwijzingen of informatie onder de aandacht van de bevoegde autoriteiten zijn gebracht en deze door die autoriteiten worden geacht te wijzen op mogelijke inbreuken op deze richtlijn. Dergelijke bewijzen, aanwijzingen of informatie kunnen bijvoorbeeld van het type zijn dat door andere autoriteiten, entiteiten, burgers, media of andere bronnen aan de bevoegde autoriteiten wordt verstrekt, kunnen openbaar beschikbare informatie zijn, of kunnen voortkomen uit andere werkzaamheden die de bevoegde autoriteiten in het kader van de uitvoering van hun taken verrichten.

(123) De uitvoering van toezichthoudende taken door de bevoegde autoriteiten mag de bedrijfsactiviteiten van de betrokken entiteit niet onnodig belemmeren. Wanneer de bevoegde autoriteiten hun toezichthoudende taken met betrekking tot essentiële entiteiten uitvoeren, met inbegrip van het uitvoeren van inspecties ter plaatse en toezicht buiten de locatie, het onderzoeken van inbreuken op deze richtlijn, en het uitvoeren van beveiligingsaudits of beveiligingsscans, moeten zij de gevolgen voor de bedrijfsactiviteiten van de betrokken entiteit tot een minimum beperken.

(124) Bij de uitoefening van het toezicht vooraf moeten de bevoegde autoriteiten op evenredige wijze kunnen beslissen over de prioritering van het gebruik van de toezichtsmaatregelen en -middelen waarover zij beschikken. Dit houdt in dat de bevoegde autoriteiten over dergelijke prioritering kunnen beslissen op basis van toezichtsmethoden die een risicogebaseerde benadering moeten volgen. Meer in het bijzonder kan het bij dergelijke methoden gaan om criteria of benchmarks voor de indeling van essentiële entiteiten in risicocategorieën en overeenkomstige toezichtsmaatregelen en -middelen die per risicocategorie worden aanbevolen, zoals het gebruik, de frequentie of de soorten van inspecties ter plaatse, gerichte beveiligingsaudits of beveiligingsscans, het soort informatie dat moet worden

opgevraagd en de mate van gedetailleerdheid van die informatie. Dergelijke toezichtsmethoden kunnen ook vergezeld gaan van werkprogramma's en regelmatig worden beoordeeld en geëvalueerd, onder meer met betrekking tot aspecten als de middelentoewijzing en de behoeften. Met betrekking tot overheidsinstanties moeten de toezichtsbevoegdheden worden uitgeoefend conform de nationale wetgevende en institutionele kaders.

(125) De bevoegde autoriteiten moeten erop toezien dat hun toezichthoudende taken met betrekking tot essentiële en belangrijke entiteiten worden uitgevoerd door opgeleide beroepsbeoefenaars, die over de noodzakelijke vaardigheden moeten beschikken om die taken uit te voeren, met name inzake het uitvoeren van inspecties ter plaatse en toezicht buiten de locatie, met inbegrip van het opsporen van zwakke punten in databases, hardware, firewalls, encryptie en netwerken. Die inspecties en dat toezicht moeten op objectieve wijze worden uitgevoerd.

(126) In naar behoren gemotiveerde gevallen waarin de bevoegde autoriteit op de hoogte is van een significante cyberdreiging of een imminent risico, moet zij onmiddellijk handhavingsbesluiten kunnen nemen om een incident te voorkomen of erop te reageren.

(127) Om de handhaving doeltreffend te maken, moet er een minimumlijst worden opgesteld van handhavingsbevoegdheden die kunnen worden uitgeoefend bij inbreuken op de bij deze richtlijn vastgestelde risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging, waarmee een duidelijk en samenhangend kader voor dergelijke handhaving in de hele Unie wordt geschapen. Er moet terdege rekening worden gehouden met de aard, de ernst en de duur van de inbreuk op deze richtlijn, de veroorzaakte materiële of immateriële schade, het opzettelijke of nalatige karakter van de inbreuk, de maatregelen die zijn genomen om de materiële of immateriële schade te voorkomen of te beperken, de mate van verantwoordelijkheid of eventuele relevante eerdere inbreuken, de mate van samenwerking met de bevoegde autoriteit en elke andere verzwarende of verzachtende omstandigheid. De handhavingsmaatregelen, met inbegrip van administratieve geldboeten, moeten evenredig zijn en het opleggen ervan moet onderworpen worden aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het Unierecht en het Handvest van de grondrechten van de Europese Unie (het "Handvest"), met inbegrip van het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van de verdediging.

(128) Deze richtlijn verplicht de lidstaten niet om te voorzien in een aansprakelijkheidsregeling op grond waarvan natuurlijke personen die ervoor moeten zorgen dat een entiteit deze richtlijn naleeft, strafrechtelijk of civielrechtelijk aansprakelijk zijn voor schade die derden als gevolg van een inbreuk op deze richtlijn hebben geleden.

(129) Met het oog op een doeltreffende handhaving van de in deze richtlijn vastgestelde verplichtingen moet elke bevoegde autoriteit de bevoegdheid hebben om administratieve geldboeten op te leggen of om te verzoeken om het opleggen ervan.

(130) Wanneer een administratieve geldboete wordt opgelegd aan een essentiële of belangrijke entiteit die een onderneming is, moet een onderneming voor die doeleinden worden opgevat als een onderneming in de zin van de artikelen 101 en 102 VWEU. Wanneer een administratieve geldboete wordt opgelegd aan een persoon die geen onderneming is, moet de bevoegde autoriteit bij het bepalen van het passende bedrag van de boete rekening houden met het algemene inkomensniveau in de lidstaat en met de economische situatie van de persoon. Het is aan de lidstaten om te bepalen of en in welke mate overheidsinstanties aan administratieve geldboeten moeten worden onderworpen. Het opleggen van een administratieve geldboete doet geen afbreuk aan de toepassing van andere bevoegdheden van de bevoegde autoriteiten of van andere sancties die zijn vastgesteld in de nationale voorschriften tot omzetting van deze richtlijn.

(131) De lidstaten moeten de regels inzake strafrechtelijke sancties voor inbreuken op de interne voorschriften tot omzetting van deze richtlijn kunnen vaststellen. Het opleggen van strafrechtelijke sancties voor inbreuken op dergelijke nationale regels en van daarmee samenhangende administratieve sancties mag echter niet leiden tot een inbreuk op het "ne bis in idem"-beginsel, zoals uitgelegd door het Hof van Justitie van de Europese Unie.

(132) Wanneer deze richtlijn niet voorziet in de harmonisatie van administratieve sancties of indien nodig in andere gevallen, bijvoorbeeld bij een ernstige inbreuk op deze richtlijn, moeten de lidstaten een systeem toepassen dat voorziet in doeltreffende, evenredige en afschrikkende sancties. De aard van die sancties en of zij strafrechtelijk of administratief zijn, moet worden bepaald door het nationale recht.

(133) Om de doeltreffendheid en het afschrikkingseffect van de handhavingsmaatregelen die van toepassing zijn op inbreuken op deze richtlijn verder te versterken, moeten de bevoegde overheden gemachtigd worden over te gaan tot een tijdelijke opschorting, of te kunnen verzoeken om tijdelijke opschorting, van een certificering of vergunning voor een deel of het geheel van de door een essentiële entiteit verleende relevante diensten of uitgevoerde activiteiten, en te kunnen verzoeken om het opleggen van een tijdelijk verbod op de uitoefening van bestuursfuncties door een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger. Gezien de ernst en het effect van dergelijke tijdelijke opschortingen of verboden op de activiteiten van de entiteiten en uiteindelijk op hun consumenten, mogen zij alleen worden toegepast in verhouding tot de ernst van de inbreuk en rekening houdend met de specifieke omstandigheden van elk individueel geval, met inbegrip van het opzettelijke of nalatige karakter van de inbreuk, en maatregelen die zijn genomen om de materiële of immateriële schade te voorkomen of te beperken. Dergelijke tijdelijke opschortingen of verboden mogen alleen worden toegepast als ultiem middel, met name alleen nadat de andere in deze richtlijn neergelegde relevante handhavingsmaatregelen zijn uitgeput, en alleen totdat de betrokken entiteit de noodzakelijke stappen zet om de tekortkomingen te verhelpen of te voldoen aan de door de bevoegde autoriteit gestelde eisen waarvoor dergelijke tijdelijke opschortingen of verboden werden toegepast. Het opleggen van dergelijke tijdelijke opschortingen of verboden moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het Unierecht en het Handvest, met inbegrip van het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van de verdediging.

(134) Om ervoor te zorgen dat entiteiten hun in deze richtlijn vastgelegde verplichtingen nakomen, moeten lidstaten met elkaar samenwerken en elkaar bijstaan op het gebied van toezicht- en handhavingsmaatregelen, met name wanneer een entiteit diensten verleent in meer dan één lidstaat of wanneer haar netwerk- en informatiesystemen zich bevinden in een andere lidstaat dan die waar zij diensten verleent. Bij het verlenen van bijstand moet de aangezochte bevoegde autoriteit toezicht- of handhavingsmaatregelen nemen overeenkomstig het nationale recht. Ten behoeve van de vlotte werking van de wederzijdse bijstand uit hoofde van deze richtlijn, moeten de bevoegde autoriteiten de samenwerkingsgroep gebruiken als forum om kwesties en specifieke verzoeken om bijstand te bespreken.

(135) Om te zorgen voor doeltreffend toezicht en doeltreffende handhaving, met name in situaties met een grensoverschrijdende dimensie, moet een lidstaat die een verzoek om wederzijdse bijstand heeft ontvangen, binnen de grenzen van dat verzoek passende toezichts- en handhavingsmaatregelen nemen ten aanzien van de entiteit die het voorwerp van dat verzoek is, en die diensten verleent of over een netwerk- en informatiesysteem op het grondgebied van die lidstaat beschikt.

(136) In deze richtlijn moeten overeenkomstig Verordening (EU) 2016/679 regels worden vastgesteld voor de samenwerking tussen de bevoegde autoriteiten en de toezichthoudende autoriteiten bij de behandeling van inbreuken op deze richtlijn in verband met persoonsgegevens.

(137) Deze richtlijn moet gericht zijn op het waarborgen van een hoge mate van verantwoordelijkheid voor de risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging op het niveau van de essentiële en belangrijke entiteiten. Daarom moeten de bestuursorganen van de essentiële en belangrijke entiteiten de risicobeheersmaatregelen op het gebied van cyberbeveiliging goedkeuren en toezicht houden op de uitvoering ervan.

(138) Teneinde te zorgen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie op basis van deze richtlijn, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 VWEU handelingen vast te stellen tot aanvulling van deze richtlijn door te specificeren welke categorieën essentiële en belangrijke entiteiten moeten worden verplicht bepaalde gecertificeerde ICT-producten, ICT-diensten en ICT-processen te gebruiken of een certificaat te verkrijgen in het kader van een Europese cyberbeveiligingscertificeringsregeling. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen gebeuren in overstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven ([22]). Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen, ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

([22]) PB L 123 van 12.5.2016, blz. 1.

(139) Om eenvormige voorwaarden te waarborgen voor de uitvoering van deze richtlijn, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend om de procedurele regelingen die nodig zijn voor de werking van de samenwerkingsgroep alsmede de technische, methodologische en sectorale voorschriften met betrekking tot de risicobeheersmaatregelen op het gebied van cyberbeveiliging vast te stellen, en om nadere toelichting te geven over het soort informatie, het format en de procedure voor de melding van incidenten, cyberdreigingen en bijna-incidenten alsook van significante cyberdreigingsberichten, en over gevallen waarin een incident als significant moet worden beschouwd. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad ([23]).

(140) De Commissie moet deze richtlijn op gezette tijden geëvalueerd, na raadpleging van belanghebbenden, met name om vast te stellen of het passend is wijzigingen voor te stellen in het licht van veranderingen in de maatschappelijke, politieke, technologische of marktomstandigheden. In het kader van die evaluaties moet door de Commissie worden beoordeeld wat de relevantie is van de omvang van de betrokken entiteiten, en de in de bijlagen bij deze richtlijn bedoelde sectoren, subsectoren en types van entiteiten voor het functioneren van de economie en de samenleving in samenhang met cyberbeveiliging. De Commissie moet onder meer beoordelen of binnen het toepassingsgebied van deze richtlijn vallende aanbieders die zijn aangewezen als zeer grote onlineplatforms in de zin van artikel 33 van Verordening (EU) 2022/2065 van het Europees Parlement en de Raad ([24]), kunnen worden aangemerkt als essentiële entiteiten uit hoofde van deze richtlijn.

(141) Deze richtlijn creëert nieuwe taken voor Enisa, waardoor het een grotere rol krijgt, en zou er ook toe kunnen leiden dat Enisa zijn bestaande taken uit hoofde van Verordening (EU) 2019/881 op een hoger niveau dan voorheen moet uitvoeren. Om ervoor te zorgen dat Enisa over de noodzakelijke financiële en personele middelen beschikt om bestaande en nieuwe taken uit te voeren, en om te voldoen aan een hoger uitvoeringsniveau van die taken als gevolg van zijn grotere rol, moet zijn begroting dienovereenkomstig worden verhoogd. Bovendien moet Enisa, met het oog op een efficiënt gebruik van de middelen, meer flexibiliteit krijgen zodat het in staat is middelen intern toe te wijzen om zijn taken doeltreffend uit te voeren en aan de verwachtingen te voldoen.

(142) Daar de doelstelling van deze richtlijn, namelijk het bereiken van een hoog gemeenschappelijk niveau van cyberbeveiliging in de gehele Unie, niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de gevolgen van het optreden beter door de Unie kan worden bereikt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie bepaalde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze richtlijn niet verder dan nodig is om deze doelstelling te verwezenlijken.

(143) Deze richtlijn eerbiedigt de grondrechten en neemt de beginselen in acht die bij het Handvest zijn erkend, met name het recht op de eerbiediging van het privéleven en communicatie, het recht op de bescherming van persoonsgegevens, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van de verdediging. Het recht op een doeltreffende voorziening in rechte geldt ook voor de ontvangers van door essentiële en belangrijke entiteiten verleende diensten. Deze richtlijn moet worden uitgevoerd overeenkomstig die rechten en beginselen.

(144) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([25]) en heeft op 11 maart 2021 advies uitgebracht ([26]),

---

([23]) 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).

([24]) Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (verordening inzake digitale diensten) (PB L 277 van 27.10.2022, blz. 1).

([25]) 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 van 21.11.2018, blz. 39).

([26]) PB C 183 van 11.5.2021, blz. 3.

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

1. Deze richtlijn voorziet in maatregelen die erop gericht zijn een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie te bereiken, teneinde de werking van de interne markt te verbeteren.

2. Met het oog hierop voorziet deze richtlijn in:

a) verplichtingen die de lidstaten voorschrijven dat zij nationale cyberbeveiligingsstrategieën vaststellen, en bevoegde autoriteiten, cybercrisisbeheerautoriteiten, centrale contactpunten op het gebied van cyberbeveiliging (centrale contactpunten) en computer security incident response teams (CSIRT's) aanwijzen of instellen;

b) risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging voor entiteiten van het type waarnaar in bijlage I of II wordt verwezen alsmede voor entiteiten die uit hoofde van Richtlijn (EU) 2022/2557 als kritieke entiteiten worden aangemerkt;

c) regels en verplichtingen met betrekking tot het delen van cyberbeveiligingsinformatie;

d) toezichts- en handhavingsverplichtingen voor de lidstaten.

Artikel 2

Toepassingsgebied

1. Deze richtlijn is van toepassing op publieke of particuliere entiteiten van een in de bijlagen I en II bedoeld type die in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG, of de in lid 1 van dat artikel vastgestelde plafonds voor middelgrote ondernemingen overschrijden, en die hun diensten verlenen of hun activiteiten verrichten in de Unie.

Artikel 3, lid 4, van de bijlage bij die aanbeveling geldt niet voor de toepassing van deze richtlijn.

2. Deze richtlijn is ook van toepassing op entiteiten van het in bijlage I of II bedoelde soort, ongeacht hun omvang, wanneer:

a) de diensten verleend worden door:

   i) aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten;

   ii) aanbieders van vertrouwensdiensten;

   iii) registers voor topleveldomeinnamen en verleners van domeinnaamregistratiediensten;

b) de entiteit in een lidstaat de enige aanbieder is van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten;

c) verstoring van de door de entiteit verleende dienst aanzienlijke gevolgen kan hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

d) verstoring van de door de entiteit verleende dienst een aanzienlijk systeemrisico met zich kan brengen, met name voor sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

e) de entiteit kritiek is vanwege het specifieke belang ervan op nationaal of regionaal niveau voor de specifieke sector of het specifieke type dienst, of voor andere onderling afhankelijke sectoren in de lidstaat;

f) de entiteit een overheidsinstantie is:

i) van de centrale overheid zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht, of

ii) op regionaal niveau zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht, die, na een risicobeoordeling, diensten verleent waarvan de verstoring aanzienlijke gevolgen kan hebben voor kritieke maatschappelijke of economische activiteiten.

3. Deze richtlijn is van toepassing op entiteiten die worden aangemerkt als een kritieke entiteit uit hoofde van Richtlijn (EU) 2022/2557, ongeacht hun omvang.

4. Deze richtlijn is van toepassing op entiteiten die domeinnaamregistratiediensten verrichten, ongeacht hun omvang.

5. De lidstaten kunnen bepalen dat deze richtlijn van toepassing is op:

a) overheidsinstanties op lokaal niveau;

b) onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten.

6. Deze richtlijn laat de verantwoordelijkheid van de lidstaten om de nationale veiligheid te beschermen en hun bevoegdheid om andere essentiële staatsfuncties te beschermen, waaronder het verdedigen van de territoriale integriteit van de staat en het handhaven van de openbare orde, onverlet.

7. Deze richtlijn is niet van toepassing op overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.

8. De lidstaten kunnen specifieke entiteiten die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, of die uitsluitend diensten verlenen aan de in lid 7 van dit artikel bedoelde overheidsinstanties, met betrekking tot die activiteiten of diensten vrijstellen van de in artikel 21 of artikel 23 vastgestelde verplichtingen. In dergelijke gevallen zijn de in hoofdstuk VII bedoelde toezicht- en handhavingsmaatregelen niet van toepassing op die specifieke activiteiten of diensten. Wanneer de entiteiten uitsluitend activiteiten verrichten of diensten verlenen van het in dit lid bedoelde type kunnen de lidstaten besluiten om die entiteiten ook vrij te stellen van de in de artikelen 3 en 27 vastgestelde verplichtingen.

9. De leden 7 en 8 zijn niet van toepassing wanneer een entiteit optreedt als aanbieder van vertrouwensdiensten.

10. Deze richtlijn is niet van toepassing op entiteiten die door lidstaten zijn uitgesloten van het toepassingsgebied van Verordening (EU) 2022/2554 in overeenstemming met artikel 2, lid 4, van die verordening.

11. De in deze richtlijn vastgelegde verplichtingen omvatten niet de verstrekking van informatie waarvan de bekendmaking strijdig zou zijn met de wezenlijke belangen van nationale veiligheid van de lidstaten, openbare veiligheid of defensie.

12. Deze richtlijn is van toepassing onverminderd Verordening (EU) 2016/679, Richtlijn 2002/58/EG, Richtlijnen 2011/93/EU ([27]) en 2013/40/EU ([28]) van het Europees Parlement en de Raad, en Richtlijn (EU) 2022/2557.

13. Onverminderd artikel 346 VWEU wordt informatie die krachtens Unie- of nationale voorschriften vertrouwelijk is, zoals de voorschriften inzake de vertrouwelijkheid van bedrijfsinformatie, alleen met de Commissie en andere bevoegde autoriteiten overeenkomstig deze richtlijn uitgewisseld wanneer die uitwisseling noodzakelijk is voor de toepassing van deze richtlijn. De uitgewisselde informatie blijft beperkt tot de informatie die relevant is en evenredig staat tot het doel van die uitwisseling. Bij de uitwisseling van informatie wordt de vertrouwelijkheid van die informatie gewaarborgd en worden de veiligheids- en commerciële belangen van betrokken entiteiten beschermd.

([27]) Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 335 van 17.12.2011, blz. 1).

([28]) Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (PB L 218 van 14.8.2013, blz. 8).

14. Entiteiten, de bevoegde autoriteiten, de centrale contactpunten en de CSIRT's verwerken persoonsgegevens voor zover dat nodig is voor de toepassing van deze richtlijn en in overeenstemming met Verordening (EU) 2016/679, en met name berust een dergelijke verwerking op artikel 6 daarvan.

De verwerking van persoonsgegevens uit hoofde van deze richtlijn door aanbieders van openbare elektronischecommunicatienetwerken of aanbieders van openbare elektronischecommunicatiediensten wordt uitgevoerd overeenkomstig het Unierecht inzake gegevensbescherming en het Unierecht inzake privacy, met name Richtlijn 2002/58/EG.

Artikel 3

Essentiële en belangrijke entiteiten

1. Voor de toepassing van deze richtlijn worden de volgende entiteiten als essentiële entiteiten beschouwd:

a) entiteiten van een in bijlage I bedoeld type die de in artikel 2, lid 1, van de bijlage bij Aanbeveling 2003/361/EG vastgestelde plafonds voor middelgrote ondernemingen overschrijden;

b) gekwalificeerde aanbieders van vertrouwensdiensten en registers voor topleveldomeinnamen alsook DNS-dienstverleners, ongeacht hun omvang;

c) aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten die in aanmerking komen als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;

d) in artikel 2, lid 2, punt f), i), bedoelde overheidsinstanties;

e) alle andere entiteiten van een in bijlage I of II bedoeld type die door een lidstaat aangemerkt zijn als essentiële entiteiten krachtens artikel 2, lid 2, punten b) tot en met e);

f) entiteiten die aangemerkt zijn als kritieke entiteiten uit hoofde van Richtlijn (EU) 2022/2557, zoals bedoeld in artikel 2, lid 3, van deze richtlijn;

g) indien de lidstaat daartoe besluit, entiteiten die vóór 16 januari 2023 door die lidstaat aangemerkt zijn als aanbieders van essentiële diensten overeenkomstig Richtlijn (EU) 2016/1148 of het nationale recht.

2. Voor de toepassing van deze richtlijn worden entiteiten van een in bijlage I of II bedoeld type die niet in aanmerking komen als essentiële entiteiten krachtens lid 1 van dit artikel, als belangrijke entiteiten beschouwd. Hiertoe behoren entiteiten die door lidstaten aangemerkt zijn als belangrijke entiteiten krachtens artikel 2, lid 2, punten b) tot en met e).

3. Uiterlijk op 17 april 2025 stellen de lidstaten een lijst op van essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. De lidstaten evalueren die lijst regelmatig, en daarna ten minste om de twee jaar, en werken deze zo nodig bij.

4. Met het oog op het opstellen van de in lid 3 bedoelde lijst vereisen de lidstaten van de in dat lid bedoelde entiteiten dat zij ten minste de volgende informatie aan de bevoegde autoriteiten verstrekken:

a) de naam van de entiteit;

b) het adres en actuele contactgegevens, waaronder e-mailadressen, IP-bereiken en telefoonnummers;

c) indien van toepassing, de relevante sector en subsector als bedoeld in bijlage I of II, en

d) indien van toepassing, een lijst van de lidstaten waar zij diensten verlenen die binnen het toepassingsgebied van deze richtlijn vallen.

De in lid 3 bedoelde entiteiten melden onmiddellijk elke wijziging in de bijzonderheden die zij op grond van de eerste alinea van dit lid hebben ingediend, en in elk geval binnen twee weken na de datum van de wijziging.

De Commissie bepaalt, met hulp van het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), zonder onnodige vertraging richtsnoeren en modellen met betrekking tot de in dit lid vastgelegde verplichtingen.

De lidstaten kunnen nationale mechanismen instellen waarmee entiteiten zichzelf kunnen registreren.

5. Uiterlijk op 17 april 2025 en vervolgens om de twee jaar, melden de bevoegde autoriteiten:

a) aan de Commissie en de samenwerkingsgroep: het aantal essentiële en belangrijke entiteiten die op grond van lid 3 in een lijst zijn opgenomen voor elke sector en subsector als bedoeld in bijlage I of II, en

b) aan de Commissie: relevante informatie over het aantal essentiële en belangrijke entiteiten die op grond van artikel 2, lid 2, punten b) tot en met e), als dusdanig zijn aangemerkt, de in bijlage I of II bedoelde sector en subsector waartoe zij behoren, het type dienst dat zij verlenen, en de bepaling van artikel 2, lid 2, punten b) tot en met e), op grond waarvan zij als dusdanig zijn aangemerkt.

6. Tot 17 april 2025 en op verzoek van de Commissie, mogen lidstaten aan de Commissie de namen melden van de essentiële en belangrijke entiteiten als bedoeld in lid 5, punt b).

Artikel 4

Sectorspecifieke rechtshandelingen van de Unie

1. Indien sectorspecifieke rechtshandelingen van de Unie voorschrijven dat essentiële of belangrijke entiteiten risicobeheersmaatregelen op het gebied van cyberbeveiliging moeten nemen of significante incidenten moeten melden, en indien deze eisen ten minste gelijkwaardig zijn aan de in deze richtlijn vastgestelde verplichtingen, zijn de relevante bepalingen van deze richtlijn, met inbegrip van de in hoofdstuk VII bedoelde toezichts- en handhavingsbepalingen, niet van toepassing op dergelijke entiteiten. Indien sectorspecifieke rechtshandelingen van de Unie niet alle entiteiten bestrijken in een binnen het toepassingsgebied van deze richtlijn vallende specifieke sector, blijven de desbetreffende bepalingen van deze richtlijn van toepassing op entiteiten die niet onder die sectorspecifieke rechtshandelingen van de Unie vallen.

2. De in lid 1 van dit artikel bedoelde eisen worden geacht gelijkwaardig te zijn aan de in deze richtlijn vastgestelde verplichtingen wanneer:

a) de risicobeheersmaatregelen op het gebied van cyberbeveiliging ten minste een vergelijkbare uitwerking hebben als die welke zijn vastgesteld in artikel 21, leden 1 en 2, of

b) de sectorspecifieke rechtshandeling van de Unie voorziet in onmiddellijke toegang, in voorkomend geval automatisch en rechtstreeks, tot de meldingen van incidenten door de CSIRT's, de bevoegde autoriteiten of de centrale contactpunten uit hoofde van deze richtlijn, en wanneer de eisen voor het melden van significante incidenten ten minste een vergelijkbare uitwerking hebben als die van artikel 23, leden 1 tot en met 6, van deze richtlijn.

3. Uiterlijk op 17 juli 2023 bepaalt de Commissie richtsnoeren ter verduidelijking van de toepassing van de leden 1 en 2. Die richtsnoeren worden regelmatig geëvalueerd door de Commissie. Bij de opstelling van die richtsnoeren houdt de Commissie rekening met alle opmerkingen van de samenwerkingsgroep en Enisa.

Artikel 5

Minimumharmonisatie

Deze richtlijn belet de lidstaten niet om bepalingen vast te stellen of te handhaven die een hoger cyberbeveiligingsniveau waarborgen, mits dergelijke bepalingen stroken met de in het Unierecht vastgelegde verplichtingen van de lidstaten.

Artikel 6

Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

1) "netwerk- en informatiesysteem":

   a) een elektronischecommunicatienetwerk in de zin van artikel 2, punt 1), van Richtlijn (EU) 2018/1972;

b) elk apparaat of elke groep van onderling verbonden of verwante apparaten, waarvan er een of meer, op grond van een programma, een automatische verwerking van digitale gegevens uitvoeren, of

c) digitale gegevens die worden opgeslagen, verwerkt, opgehaald of verzonden met behulp van de in punten a) en b) bedoelde elementen met het oog op de werking, het gebruik, de bescherming en het onderhoud ervan;

2) "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen;

3) "cyberbeveiliging": cyberbeveiliging zoals gedefinieerd in artikel 2, punt 1), van Verordening (EU) 2019/881;

4) "nationale cyberbeveiligingsstrategie": een samenhangend kader van een lidstaat met strategische doelstellingen en prioriteiten op het vlak van cyberbeveiliging en de governance om die doelstellingen en prioriteiten in die lidstaat te verwezenlijken;

5) "bijna-incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan;

6) "incident": een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt;

7) "grootschalig cyberbeveiligingsincident": een incident dat leidt tot een verstoringsniveau dat te groot is om door een getroffen lidstaat alleen te worden verholpen of dat significante gevolgen heeft voor ten minste twee lidstaten;

8) "incidentenbehandeling": alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een incident;

9) "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident, wat wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of verstoring en de waarschijnlijkheid dat het incident zich voordoet;

10) "cyberdreiging": een cyberdreiging zoals gedefinieerd in artikel 2, punt 8), van Verordening (EU) 2019/881;

11) "significante cyberdreiging": een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade;

12) "ICT-product": een ICT-product zoals gedefinieerd in artikel 2, punt 12), van Verordening (EU) 2019/881;

13) "ICT-dienst": een ICT-dienst zoals gedefinieerd in artikel 2, punt 13), van Verordening (EU) 2019/881;

14) "ICT-proces": een ICT-proces zoals gedefinieerd in artikel 2, punt 14), van Verordening (EU) 2019/881;

15) "kwetsbaarheid": een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit;

16) "norm": een norm zoals gedefinieerd in artikel 2, punt 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad ([29]);

17) "technische specificatie": een technische specificatie in de zin van artikel 2, punt 4), van Verordening (EU) nr. 1025/2012;

([29]) 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).

18) "internetknooppunt": een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, voornamelijk ter vergemakkelijking van de uitwisseling van internetverkeer, die alleen interconnectie voor autonome systemen biedt en die niet vereist dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat verkeer wijzigt of anderszins verstoort;

19) "domeinnaamsysteem (DNS)": een hiërarchisch gedistribueerd naamgevingssysteem dat het mogelijk maakt internetdiensten en -bronnen te identificeren, waardoor eindgebruikersapparaten in staat worden gesteld routing- en connectiviteitsdiensten op het internet te gebruiken om die diensten en bronnen te bereiken;

20) "DNS-dienstverlener": een entiteit die de volgende diensten verleent:

    a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers, of

    b) gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamservers;

21) "register voor topleveldomeinnamen": een entiteit waaraan een specifieke topleveldomeinnaam is gedelegeerd en die verantwoordelijk is voor het beheer van de topleveldomeinnaam, met inbegrip van de registratie van domeinnamen onder de topleveldomeinnaam en de technische exploitatie van de topleveldomeinnaam, met inbegrip van de exploitatie van de naamservers, het onderhoud van de databases en de verdeling van de zonebestanden van de topleveldomeinnaam over de naamservers, ongeacht of die activiteiten door de entiteit zelf worden uitgevoerd of worden uitbesteed, maar met uitzondering van situaties waarin topleveldomeinnamen uitsluitend voor eigen gebruik worden aangewend door een register;

22) "entiteit die domeinnaamregistratiediensten aanbiedt": een registrator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

23) "digitale dienst": een dienst zoals gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad ([30]);

24) "vertrouwensdienst": een vertrouwensdienst zoals gedefinieerd in artikel 3, punt 16), van Verordening (EU) nr. 910/2014;

25) "verlener van vertrouwensdiensten": een verlener van vertrouwensdiensten zoals gedefinieerd in artikel 3, punt 19), van Verordening (EU) nr. 910/2014;

26) "gekwalificeerde vertrouwensdienst": een gekwalificeerde vertrouwensdienst zoals gedefinieerd in van artikel 3, punt 17), van Verordening (EU) nr. 910/2014;

27) "gekwalificeerde verlener van vertrouwensdiensten": een gekwalificeerde verlener van vertrouwensdiensten zoals gedefinieerd in artikel 3, punt 20), van Verordening (EU) nr. 910/2014;

28) "onlinemarktplaats": een onlinemarktplaats zoals gedefinieerd in artikel 2, punt n), van Richtlijn 2005/29/EG van het Europees Parlement en de Raad ([31]);

29) "onlinezoekmachine": een onlinezoekmachine zoals gedefinieerd in artikel 2, punt 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad ([32]);

30) "cloudcomputingdienst": een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van deelbare computerbronnen mogelijk maakt, ook wanneer die bronnen over verschillende locaties verspreid zijn;

([30]) 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).

([31]) Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad ("Richtlijn oneerlijke handelspraktijken") (PB L 149 van 11.6.2005, blz. 22).

([32]) Verordening (EU) 2019/1150 van het Europees Parlement en de Raad van 20 juni 2019 ter bevordering van billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten (PB L 186 van 11.7.2019, blz. 57).

31) “datacentrumdienst”: een dienst die structuren of groepen van structuren omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van IT en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole;

32) “netwerk voor de levering van inhoud”: een netwerk van geografisch verspreide servers met het oog op een hoge beschikbaarheid, toegankelijkheid of snelle levering van digitale inhoud en diensten aan internetgebruikers ten behoeve van aanbieders van inhoud en diensten;

33) “platform voor socialenetwerkdiensten”: een platform dat eindgebruikers in staat stelt zich met elkaar te verbinden, te delen, te ontdekken en met elkaar te communiceren via meerdere apparaten, met name via chats, posts, video’s en aanbevelingen;

34) “vertegenwoordiger”: een in de Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een DNS-dienstverlener, een register voor topleveldomeinnamen, een entiteit die domeinnaamregistratiediensten verleent, een aanbieder van cloudcomputingdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de levering van inhoud, een aanbieder van beheerde diensten, een aanbieder van beheerde beveiligingsdiensten, of een aanbieder van een onlinemarktplaats, van een onlinezoekmachine of van een platform voor socialenetwerkdiensten die niet in de Unie is gevestigd, en die door een bevoegde autoriteit of een CSIRT kan worden aangesproken in plaats van de entiteit zelf met betrekking tot de verplichtingen van die entiteit uit hoofde van deze richtlijn;

35) “overheidsinstantie”: een entiteit die overeenkomstig het nationale recht als zodanig in een lidstaat is erkend, met uitzondering van de rechterlijke macht, parlementen en centrale banken, en die aan de volgende criteria voldoet:

   a) zij is opgericht om te voorzien in behoeften van algemeen belang en heeft geen industrieel of commercieel karakter;

   b) zij heeft rechtspersoonlijkheid of mag volgens de wet namens een andere entiteit met rechtspersoonlijkheid optreden;

   c) zij wordt grotendeels gefinancierd door de staat, regionale autoriteiten of andere publiekrechtelijke organen, is onderworpen aan beheerstoezicht door die autoriteiten of organen, of heeft een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, regionale autoriteiten of andere publiekrechtelijke organen worden benoemd;

   d) zij heeft de bevoegdheid om ten aanzien van natuurlijke of rechtspersonen administratieve of regelgevende besluiten te nemen die van invloed zijn op hun rechten op het grensoverschrijdende verkeer van personen, goederen, diensten of kapitaal;

36) “openbaar elektronischecommunicatienetwerk”: een openbaar elektronischecommunicatienetwerk zoals gedefinieerd in artikel 2, punt 8), van Richtlijn (EU) 2018/1972;

37) “elektronischecommunicatiedienst”: een elektronischecommunicatiedienst zoals gedefinieerd in van artikel 2, punt 4), van Richtlijn (EU) 2018/1972;

38) “entiteit”: een natuurlijke of rechtspersoon die als zodanig is opgericht en erkend volgens het nationale recht van zijn vestigingsplaats, en die in eigen naam rechten kan uitoefenen en aan verplichtingen kan worden onderworpen;

39) “aanbieder van beheerde diensten”: een entiteit die diensten verleent die verband houden met de installatie, het beheer, de exploitatie of het onderhoud van ICT-producten, -netwerken, -infrastructuur, -toepassingen of andere netwerk- en informatiesystemen, via bijstand of actieve administratie bij de consument ter plaatse of op afstand;

40) “aanbieder van beheerde beveiligingsdiensten”: een aanbieder van beheerde diensten die bijstand biedt of verleent voor activiteiten die verband houden met risicobeheer op het gebied van cyberbeveiliging;

41) “onderzoeksorganisatie”: een entiteit die als hoofddoel heeft het verrichten van toegepast onderzoek of experimentele ontwikkeling met het oog op de exploitatie van de resultaten van dat onderzoek voor commerciële doeleinden, met uitsluiting van onderwijsinstellingen.

HOOFDSTUK II

GECOÖRDINEERDE KADERS OP HET GEBIED VAN CYBERBEVEILIGING

Artikel 7

Nationale cyberbeveiligingsstrategie

1. Elke lidstaat moet een nationale cyberbeveiligingsstrategie vaststellen die voorziet in de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven. De nationale cyberbeveiligingsstrategie omvat:

a) doelstellingen en prioriteiten van de cyberbeveiligingsstrategie van de lidstaat, met name inzake de in de bijlagen I en II bedoelde sectoren;

b) een governancekader om de in punt a) van dit lid bedoelde doelstellingen en prioriteiten te verwezenlijken, met inbegrip van het in lid 2 bedoelde beleid;

c) een governancekader dat de taken en verantwoordelijkheden van relevante belanghebbenden op nationaal niveau verduidelijkt, ter onderbouwing van de samenwerking en coördinatie op nationaal niveau tussen de bevoegde autoriteiten, de centrale contactpunten en de CSIRT's uit hoofde van deze richtlijn, alsmede van de coördinatie en samenwerking tussen die organen en uit hoofde van sectorspecifieke rechtshandelingen van de Unie bevoegde autoriteiten;

d) een mechanisme om relevante activa vast te stellen en een beoordeling van de risico's in die lidstaat;

e) een inventarisatie van de maatregelen om te zorgen voor paraatheid, respons en herstel bij incidenten, met inbegrip van samenwerking tussen de publieke en de particuliere sector;

f) een lijst van de verschillende autoriteiten en belanghebbenden die betrokken zijn bij de uitvoering van de nationale cyberbeveiligingsstrategie;

g) een beleidskader voor versterkte coördinatie tussen de uit hoofde van deze richtlijn bevoegde autoriteiten en de uit hoofde van Richtlijn (EU) 2022/2557 bevoegde autoriteiten, met als doel het delen van informatie over risico's, cyberdreigingen, en incidenten alsook over niet-cyberrisico's, -dreigingen en -incidenten, en in voorkomend geval de uitoefening van toezichthoudende taken;

h) een plan, met inbegrip van de noodzakelijke maatregelen, om het algemene niveau van cyberbeveiligingsbewustzijn bij de burgers te verbeteren.

2. In het kader van de nationale cyberbeveiligingsstrategie stellen de lidstaten met name beleid vast:

a) inzake cyberbeveiliging in de toeleveringsketen voor ICT-producten en ICT-diensten die door entiteiten worden gebruikt voor het verlenen van hun diensten;

b) inzake het opnemen en specificeren van cyberbeveiligingsgerelateerde eisen voor ICT-producten en ICT-diensten bij overheidsopdrachten, onder meer met betrekking tot cyberbeveiligingscertificering, versleuteling en het gebruik van open-source-cyberbeveiligingsproducten;

c) voor het beheer van kwetsbaarheden, met inbegrip van de bevordering en vergemakkelijking van de gecoördineerde bekendmaking van kwetsbaarheden uit hoofde van artikel 12, lid 1;

d) inzake het in stand houden van de algemene beschikbaarheid, integriteit en vertrouwelijkheid van de openbare kern van het open internet, in voorkomend geval met inbegrip van de cyberbeveiliging van onderzeese communicatiekabels;

e) voor het bevorderen van de ontwikkeling en integratie van relevante geavanceerde technologieën met het oog op de toepassing van geavanceerde risicobeheersmaatregelen op het gebied van cyberbeveiliging;

f) voor het bevorderen en ontwikkelen van onderwijs en opleiding op het gebied van cyberbeveiliging, cyberbeveiligings-vaardigheden, -bewustmakings- en -onderzoeks- en ontwikkelingsinitiatieven, alsook van richtsnoeren voor goede praktijken en controles op het gebied van cyberhygiëne, gericht op burgers, belanghebbenden en entiteiten;

g) voor het ondersteunen van academische en onderzoeksinstellingen bij de ontwikkeling, versterking en bevordering van de uitrol van instrumenten voor cyberbeveiliging en een veilige netwerkinfrastructuur;

h) met inbegrip van relevante procedures en passende instrumenten voor het delen van informatie, ter ondersteuning van het vrijwillige delen van cyberbeveiligingsinformatie tussen entiteiten overeenkomstig het Unierecht;

i) voor het versterken van de digitale weerbaarheid en het basisniveau van cyberhygiëne van kleine en middelgrote ondernemingen, met name die welke van het toepassingsgebied van deze richtlijn zijn uitgesloten, door te voorzien in gemakkelijk toegankelijke richtsnoeren en bijstand voor hun specifieke behoeften;

j) voor het bevorderen van actieve cyberbescherming.

3. De lidstaten stellen de Commissie in kennis van hun nationale cyberbeveiligingsstrategieën binnen drie maanden na de vaststelling ervan. De lidstaten kunnen informatie die verband houdt met hun nationale veiligheid uitsluiten van dergelijke kennisgevingen.

4. De lidstaten beoordelen hun nationale cyberbeveiligingsstrategieën regelmatig en ten minste om de vijf jaar op basis van kernprestatie-indicatoren, en werken deze zo nodig bij. Op verzoek van de lidstaten krijgen zij van Enisa bijstand bij het ontwikkelen of bijwerken van een nationale cyberbeveiligingsstrategie en van kernprestatie-indicatoren voor de beoordeling van die strategie, teneinde deze in overeenstemming te brengen met de in deze richtlijn vastgelegde eisen en verplichtingen.

Artikel 8

Bevoegde autoriteiten en centrale contactpunten

1. Elke lidstaat gaat over tot het aanwijzen of instellen van een of meer bevoegde autoriteiten, verantwoordelijk voor cyberbeveiliging en voor de in hoofdstuk VII van deze richtlijn bedoelde toezichthoudende taken (bevoegde autoriteiten).

2. De in lid 1 bedoelde bevoegde autoriteiten monitoren op de tenuitvoerlegging van deze richtlijn op nationaal niveau.

3. Elke lidstaat gaat over tot het aanwijzen of instellen van een centraal contactpunt. Wanneer een lidstaat slechts één bevoegde autoriteit aanwijst of instelt uit hoofde van lid 1, is die bevoegde autoriteit ook het centrale contactpunt voor die lidstaat.

4. Elk centraal contactpunt vervult een verbindingsfunctie om te zorgen voor grensoverschrijdende samenwerking van de autoriteiten van zijn lidstaat met de relevante autoriteiten van andere lidstaten en in voorkomend geval met de Commissie en Enisa, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde autoriteiten binnen zijn lidstaat.

5. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten en centrale contactpunten over voldoende middelen beschikken om de hun toegewezen taken doeltreffend en efficiënt uit te voeren en aldus de doelstellingen van deze richtlijn te verwezenlijken.

6. Elke lidstaat stelt de Commissie onverwijld in kennis van de identiteit van de in lid 1 bedoelde bevoegde autoriteit en van het in lid 3 bedoelde centrale contactpunt, van de taken van die autoriteiten en van alle latere wijzigingen ervan. Elke lidstaat maakt de identiteit van zijn bevoegde autoriteit openbaar. De Commissie maakt een lijst met de centrale contactpunten voor het publiek beschikbaar.

Artikel 9

Nationale kaders voor cybercrisisbeheer

1. Elke lidstaat gaat over tot het aanwijzen of instellen van een of meer bevoegde autoriteiten die verantwoordelijk zijn voor het beheer van grootschalige cyberbeveiligingsincidenten en crises (cybercrisisbeheerautoriteiten). De lidstaten zien erop toe dat die autoriteiten beschikken over voldoende middelen om de hun toegewezen taken doeltreffend en efficiënt uit te voeren. De lidstaten zorgen voor samenhang met de bestaande kaders voor algemene nationale crisisbeheersing.

2. Wanneer een lidstaat meer dan één cybercrisisbeheerautoriteit aanwijst of instelt uit hoofde van lid 1, moet hij duidelijk aangeven welke van die bevoegde autoriteiten moet dienen als coördinator voor het beheer van grootschalige cyberbeveiligingsincidenten en crises.

3. Elke lidstaat stelt vast welke capaciteiten, middelen en procedures in het geval van een crisis voor de toepassing van deze richtlijn kunnen worden ingezet.

4. Elke lidstaat stelt een nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons vast, waarin de doelstellingen van en regelingen voor het beheer van grootschalige cyberbeveiligingsincidenten en crises zijn vastgelegd. In dat plan wordt in het bijzonder het volgende vastgelegd:

a) de doelstellingen van nationale paraatheidsmaatregelen en -activiteiten;

b) de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;

c) de cybercrisisbeheerprocedures, met inbegrip van de integratie ervan in het algemene nationale crisisbeheerkader en in de informatie-uitwisselingskanalen;

d) de nationale paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten;

e) de relevante publieke en particuliere belanghebbenden en betrokken infrastructuur;

f) de nationale procedures en regelingen tussen de betrokken nationale autoriteiten en instanties om de effectieve deelname van de lidstaat aan het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en crises op Unieniveau en de ondersteuning daarvan te waarborgen.

5. Binnen drie maanden na de aanwijzing of instelling van de in lid 1 bedoelde cybercrisisbeheerautoriteit stelt elke lidstaat de Commissie in kennis van de identiteit van zijn autoriteit en van alle latere wijzigingen ervan. Binnen drie maanden na de vaststelling van hun nationale plannen voor grootschalige cyberbeveiligingsincidenten en crisisrespons, dienen de lidstaten bij de Commissie en bij het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) relevante informatie in met betrekking tot de eisen van lid 4 inzake die plannen. De lidstaten kunnen informatie weglaten indien en voor zover een dergelijke weglating noodzakelijk is voor hun nationale veiligheid.

Artikel 10

Computer security incident response teams (CSIRT's)

1. Elke lidstaat gaat over tot het aanwijzen of instellen van een of meer CSIRT's. De CSIRT's kunnen worden aangewezen of ingesteld binnen een bevoegde autoriteit. De CSIRT's voldoen aan de in artikel 11, lid 1, opgenomen eisen, bestrijken ten minste de in bijlagen I en II bedoelde sectoren, subsectoren en types entiteiten, en zijn verantwoordelijk voor incidentenbehandeling volgens een welbepaald proces.

2. De lidstaten zorgen ervoor dat elk CSIRT over voldoende middelen beschikt om zijn in artikel 11, lid 3, omschreven taken doeltreffend uit te voeren.

3. De lidstaten zorgen ervoor dat elk CSIRT over een passende, veilige en weerbare communicatie- en informatie-infrastructuur beschikt waardoor informatie kan worden uitgewisseld met essentiële en belangrijke entiteiten en andere relevante belanghebbenden. Daartoe zien de lidstaten erop toe dat elk CSIRT bijdraagt aan de uitrol van veilige instrumenten voor het delen van informatie.

4. De CSIRT's werken samen en wisselen in voorkomend geval relevante informatie uit overeenkomstig artikel 29 met sectorale of sectoroverschrijdende gemeenschappen van essentiële en belangrijke entiteiten.

5. De CSIRT's nemen deel aan de overeenkomstig artikel 19 georganiseerde collegiale toetsingen.

6. De lidstaten zorgen voor een doeltreffende, efficiënte en veilige samenwerking van hun CSIRT's in het CSIRT-netwerk.

7. De CSIRT's kunnen samenwerkingsrelaties tot stand brengen met de nationale computer security incident response teams van derde landen. In het kader van dergelijke samenwerkingsrelaties vergemakkelijken de lidstaten doeltreffende, efficiënte en veilige informatie-uitwisseling met die nationale computer security incident response teams van derde landen, met gebruikmaking van relevante informatie-uitwisselingsprotocollen, waaronder het verkeerslichtprotocol ("*traffic light protocol*"). De CSIRT's kunnen relevante informatie uitwisselen met nationale computer security incident response teams van derde landen, met inbegrip van persoonsgegevens overeenkomstig het Unierecht inzake gegevensbescherming.

8. De CSIRT's kunnen samenwerken met nationale computer security incident response teams van derde landen of gelijkwaardige organen van derde landen, met name om hen bijstand op het gebied van cyberbeveiliging te verlenen.

9. Elke lidstaat stelt de Commissie onverwijld in kennis van de identiteit van het in lid 1 van dit artikel bedoelde CSIRT en van het CSIRT dat als coördinator is aangewezen op grond van artikel 12, lid 1, van hun respectieve taken met betrekking tot essentiële en belangrijke entiteiten, en van elke latere wijziging ervan.

10. De lidstaten kunnen bij de ontwikkeling van hun CSIRT's de hulp van Enisa inroepen.

Artikel 11

Eisen, technische capaciteiten en taken van de CSIRT's

1. De CSIRT's voldoen aan de volgende eisen:

a) de CSIRT's garanderen een hoge mate van beschikbaarheid van hun communicatiekanalen door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse middelen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen; ze specificeren communicatiekanalen duidelijk en delen ze mee aan de gebruikersgroep en de samenwerkingspartners;

b) de lokalen en werkruimten van de CSIRT's en de ondersteunende informatiesystemen bevinden zich op beveiligde locaties;

c) de CSIRT's worden, met het oog op doeltreffende en efficiënte overdrachten, uitgerust met een adequaat systeem voor het beheren en routeren van verzoeken;

d) de CSIRT's waarborgen de vertrouwelijkheid en betrouwbaarheid van hun activiteiten;

e) de CSIRT's beschikken over voldoende personeel om te allen tijde de beschikbaarheid van hun diensten te garanderen, en zij zorgen ervoor dat hun personeel naar behoren wordt opgeleid;

f) de CSIRT's zijn uitgerust met redundante systemen en reservewerkruimten om de continuïteit van hun diensten te waarborgen.

De CSIRT's kunnen deelnemen aan internationale samenwerkingsnetwerken.

2. De lidstaten zorgen ervoor dat hun CSIRT's gezamenlijk over de noodzakelijke technische capaciteiten beschikken om de in lid 3 bedoelde taken uit te voeren. De lidstaten zorgen ervoor dat voldoende middelen worden toegekend aan hun CSIRT's, om ervoor te zorgen dat de CSIRT's voldoende personeel hebben zodat zij hun technische capaciteiten kunnen ontwikkelen.

3. De CSIRT's hebben de volgende taken:

a) het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk en informatiesystemen;

b) het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk;

c) het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;

d) het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;

e) op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen;

f) het deelnemen aan het CSIRT-netwerk en, in overeenstemming met hun capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van het netwerk op hun verzoek;

g) indien van toepassing, het optreden als coördinator ten behoeve van het in artikel 12, lid 1 bedoelde proces van gecoördineerde bekendmaking van kwetsbaarheden;

h) het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie op grond van artikel 10, lid 3.

De CSIRT's kunnen overgaan tot het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen van essentiële en belangrijke entiteiten. Een dergelijk scannen wordt uitgevoerd om kwetsbare of onveilig geconfigureerde netwerk- en informatiesystemen op te sporen en de betrokken entiteiten te informeren. Een dergelijk scannen mag geen negatieve gevolgen hebben voor de werking van de diensten van de entiteiten.

Bij de uitvoering van de in de eerste alinea bedoelde taken kunnen de CSIRT's, op grond van een risicogebaseerde benadering, prioriteit geven aan bepaalde taken.

4. De CSIRT's brengen samenwerkingsrelaties tot stand met relevante belanghebbenden in de particuliere sector, teneinde de doelstellingen van deze richtlijn te verwezenlijken.

5. Om de in lid 4 bedoelde samenwerking te vergemakkelijken, bevorderen de CSIRT's de invoering en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën met betrekking tot:

a) procedures voor de incidentenbehandeling;

b) crisisbeheer, en

c) gecoördineerde bekendmaking van kwetsbaarheden uit hoofde van artikel 12, lid 1.

Artikel 12

Gecoördineerde bekendmaking van de kwetsbaarheden en een Europese kwetsbaarheidsdatabase

1. Elke lidstaat wijst een van zijn CSIRT's aan als coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. Het als coördinator aangewezen CSIRT treedt op als een betrouwbare tussenpersoon en vergemakkelijkt, waar nodig, de interactie tussen de natuurlijke of rechtspersoon die een kwetsbaarheid meldt enerzijds en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten anderzijds, op verzoek van een van beide partijen. De taken van het als coördinator aangewezen CSIRT omvatten:

a) het identificeren van en contact opnemen met de betrokken entiteiten;

b) het bijstaan van de natuurlijke of rechtspersonen die een kwetsbaarheid melden; en

c) het onderhandelen over tijdschema's voor de bekendmaking, en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten.

De lidstaten zorgen ervoor dat natuurlijke of rechtspersonen, desgevraagd anoniem, melding kunnen maken van een kwetsbaarheid aan het als coördinator aangewezen CSIRT. Het als coördinator aangewezen CSIRT ziet erop toe dat zorgvuldige follow-up wordt gegeven aan de gemelde kwetsbaarheid en waarborgt de anonimiteit van de natuurlijke of rechtspersoon die de kwetsbaarheid meldt. Wanneer een gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat, werkt het als coördinator aangewezen CSIRT van iedere betrokken lidstaat, in voorkomend geval, samen met andere als coördinator aangewezen CSIRT's binnen het CSIRT-netwerk.

2. Enisa ontwikkelt en onderhoudt, na raadpleging van de samenwerkingsgroep, een Europese kwetsbaarheidsdatabase. Daartoe stelt Enisa de passende informatiesystemen, beleidsmaatregelen en procedures vast en onderhoudt deze, alsook de noodzakelijke technische en organisatorische maatregelen om de veiligheid en integriteit van de Europese kwetsbaarheidsdatabase te waarborgen, met name om entiteiten, ongeacht of zij binnen het toepassingsgebied van deze richtlijn vallen, en hun leveranciers van netwerk- en informatiesystemen, in staat te stellen de in ICT-producten of ICT-diensten aanwezige algemeen bekende kwetsbaarheden op een vrijwillige basis bekend te maken en te registreren. Alle belanghebbenden krijgen toegang tot de informatie over de kwetsbaarheden die in de Europese kwetsbaarheidsdatabase is opgenomen. Die database omvat:

a) informatie die de kwetsbaarheid beschrijft;

b) de betrokken ICT-producten of ICT-diensten en de ernst van de kwetsbaarheid in het licht van de omstandigheden waarin deze kan worden uitgebuit;

c) de beschikbaarheid van gerelateerde patches en, bij gebrek aan beschikbare patches, door de bevoegde autoriteiten of de CSIRT's bepaalde richtsnoeren voor gebruikers van kwetsbare ICT-producten en ICT-diensten over de wijze waarop de risico's die voortvloeien uit bekendgemaakte kwetsbaarheden kunnen worden beperkt.

Artikel 13

Samenwerking op nationaal niveau

1. Wanneer zij afzonderlijk bestaan, werken de bevoegde autoriteiten, het centrale contactpunt en de CSIRT's van dezelfde lidstaat met elkaar samen om de in deze richtlijn vastgestelde verplichtingen na te komen.

2. De lidstaten zorgen ervoor dat hun CSIRT's of, in voorkomend geval, hun bevoegde autoriteiten, meldingen ontvangen van significante incidenten op grond van artikel 23, en van incidenten, cyberdreigingen en bijna-incidenten op grond van artikel 30.

3. De lidstaten zorgen ervoor dat hun CSIRT's of, in voorkomend geval, hun bevoegde autoriteiten, hun centrale contactpunten in kennis stellen van de op grond van deze richtlijn ingediende meldingen van incidenten, cyberdreigingen en bijna-incidenten.

4. Om te garanderen dat de taken en verplichtingen van de bevoegde autoriteiten, de centrale contactpunten en de CSIRT's doeltreffend worden uitgevoerd, zorgen de lidstaten, voor zover mogelijk, voor passende samenwerking tussen die organen en rechtshandhavingsautoriteiten, gegevensbeschermingsautoriteiten, de nationale autoriteiten uit hoofde van Verordeningen (EG) nr. 300/2008 en (EU) 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014, de bevoegde autoriteiten uit hoofde van Verordening (EU) 2022/2554, de nationale regulerende instanties uit hoofde van Richtlijn (EU) 2018/1972, de bevoegde autoriteiten uit hoofde van Richtlijn (EU) 2022/2557, alsmede de bevoegde autoriteiten uit hoofde van andere sectorspecifieke rechtshandelingen van de Unie, in die lidstaat.

5. De lidstaten zien erop toe dat hun uit hoofde van deze richtlijn bevoegde autoriteiten en hun uit hoofde van Richtlijn (EU) 2022/2557 bevoegde autoriteiten samenwerken en regelmatig informatie uitwisselen inzake het als kritiek aanmerken van entiteiten, over risico's, cyberdreigingen, en incidenten, alsook over niet-cyberrisico's, -dreigingen en -incidenten die gevolgen hebben voor essentiële entiteiten die uit hoofde van Richtlijn (EU) 2022/2557 als kritieke entiteiten zijn aangemerkt, en over de maatregelen die in reactie op dergelijke risico's, dreigingen en incidenten zijn genomen. De lidstaten zien er tevens op toe dat hun uit hoofde van deze richtlijn bevoegde autoriteiten en hun uit hoofde van Verordening (EU) nr. 910/2014, Verordening (EU) 2022/2554 en Richtlijn (EU) 2018/1972 bevoegde autoriteiten regelmatig relevante informatie uitwisselen, onder meer met betrekking tot relevante incidenten en cyberdreigingen.

6. De lidstaten vereenvoudigen de rapportage met technische middelen voor de in de artikelen 23 en 30 bedoelde meldingen.

HOOFDSTUK III

SAMENWERKING OP UNIE- EN INTERNATIONAAL NIVEAU

Artikel 14

Samenwerkingsgroep

1. Om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te vergemakkelijken, alsook om het vertrouwen te vergroten, wordt een samenwerkingsgroep opgericht.

2. De samenwerkingsgroep voert zijn taken uit op basis van de in lid 7 bedoelde tweejaarlijkse werkprogramma's.

3. De samenwerkingsgroep bestaat uit vertegenwoordigers van de lidstaten, de Commissie en Enisa. De Europese Dienst voor extern optreden neemt als waarnemer deel aan de activiteiten van de samenwerkingsgroep. De Europese toezichthoudende autoriteiten (ETA's) en de uit hoofde van Verordening (EU) 2022/2554 bevoegde autoriteiten kunnen deelnemen aan de activiteiten van de samenwerkingsgroep overeenkomstig artikel 47, lid 1, van die verordening.

In voorkomend geval kan de samenwerkingsgroep het Europees Parlement en vertegenwoordigers van relevante belanghebbenden uitnodigen om deel te nemen aan zijn werkzaamheden.

Het secretariaat wordt verzorgd door de diensten van de Commissie.

4. De samenwerkingsgroep heeft de volgende taken:

a) het verstrekken van richtsnoeren aan de bevoegde autoriteiten met betrekking tot de omzetting en uitvoering van deze richtlijn;

b) het verstrekken van richtsnoeren aan de bevoegde autoriteiten met betrekking tot de ontwikkeling en uitvoering van het beleid inzake gecoördineerde bekendmaking van kwetsbaarheden, als bedoeld in artikel 7, lid 2, punt c);

c) het uitwisselen van beste praktijken en informatie met betrekking tot de uitvoering van deze richtlijn, onder meer inzake cyberdreigingen, incidenten, kwetsbaarheden, bijna-incidenten, bewustmakingsinitiatieven, opleidingen, oefeningen en vaardigheden, capaciteitsopbouw, normen en technische specificaties, alsook inzake het als dusdanig aanmerken van essentiële en belangrijke entiteiten op grond van artikel 2, lid 2, punten b) tot en met e);

d) het uitwisselen van advies en samenwerken met de Commissie rondom opkomende beleidsinitiatieven op het gebied van cyberbeveiliging en rondom de algehele samenhang van sectorspecifieke cyberbeveiligingseisen;

e) het uitwisselen van advies en samenwerken met de Commissie rondom ontwerpen van uitvoeringshandelingen of gedelegeerde handelingen die op grond van deze richtlijn worden vastgesteld;

f) het uitwisselen van beste praktijken en informatie met de betrokken instellingen, organen en instanties van de Unie;

g) het van gedachten wisselen over de uitvoering van sectorspecifieke rechtshandelingen van de Unie die bepalingen inzake cyberbeveiliging bevatten;

h) indien van toepassing, het bespreken van de verslagen van de in artikel 19, lid 9, bedoelde collegiale toetsing en het opstellen van conclusies en aanbevelingen;

i) het uitvoeren van gecoördineerde veiligheidsrisicobeoordelingen van kritieke toeleveringsketens overeenkomstig artikel 22, lid 1;

j) het bespreken van gevallen van wederzijdse bijstand, met inbegrip van ervaringen en resultaten van grensoverschrijdende gezamenlijke toezichtsacties als bedoeld in artikel 37;

k) op verzoek van een of meer betrokken lidstaten, het bespreken van specifieke verzoeken om wederzijdse bijstand als bedoeld in artikel 37;

l) het verstrekken van strategische richtsnoeren over specifieke opkomende kwesties aan het CSIRT-netwerk en EU-CyCLONe;

m) het van gedachten wisselen over het beleid inzake de follow-up die wordt gegeven aan grootschalige cyberbeveiligingsincidenten en crises, op basis van de uit het CSIRT-netwerk en EU-CyCLONe getrokken lessen;

n) het bijdragen tot de cyberbeveiligingscapaciteiten in de hele Unie door de uitwisseling van nationale ambtenaren te vergemakkelijken via een programma voor capaciteitsopbouw waarbij personeel van de bevoegde autoriteiten of van de CSIRT's betrokken is;

o) het organiseren van regelmatige en gezamenlijke bijeenkomsten met relevante particuliere belanghebbenden uit de hele Unie om de activiteiten van de samenwerkingsgroep te bespreken en input te verzamelen over nieuwe beleidsuitdagingen;

p) het bespreken van de werkzaamheden in verband met cyberbeveiligingsoefeningen, met inbegrip van het werk van Enisa;

q) het vaststellen van de methodologie en organisatorische aspecten van de in artikel 19, lid 1, bedoelde collegiale toetsingen, alsook het vastleggen van de zelfevaluatiemethode voor lidstaten overeenkomstig artikel 19, lid 5, met bijstand van de Commissie en Enisa, en, in samenwerking met de Commissie en Enisa, het ontwikkelen van gedragscodes ter onderbouwing van de werkmethoden van aangewezen cyberbeveiligingsdeskundigen overeenkomstig artikel 19, lid 6;

r) het opstellen van verslagen over de ervaringen die zijn opgedaan op strategisch niveau en bij collegiale toetsingen, met het oog op de in artikel 40 bedoelde evaluatie;

s) het regelmatig beoordelen van de stand van zaken met betrekking tot cyberdreigingen of -incidenten, zoals gijzelsoftware.

De samenwerkingsgroep dient de in de eerste alinea, punt r), bedoelde verslagen in bij de Commissie, het Europees Parlement en de Raad.

5. De lidstaten zorgen ervoor dat hun vertegenwoordigers op doeltreffende, efficiënte en veilige wijze samenwerken binnen de samenwerkingsgroep.

6. De samenwerkingsgroep kan het CSIRT-netwerk verzoeken om een technisch verslag over geselecteerde onderwerpen.

7. Uiterlijk op 1 februari 2024, en vervolgens om de twee jaar, stelt de samenwerkingsgroep een werkprogramma op over te nemen maatregelen ter uitvoering van zijn doelstellingen en taken.

8. De Commissie kan uitvoeringshandelingen vaststellen met de voor de werking van de samenwerkingsgroep noodzakelijke procedurele regelingen.

Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

De Commissie wisselt advies uit en werkt samen met de samenwerkingsgroep rond de in de eerste en tweede alinea van dit artikel bedoelde ontwerpuitvoeringshandelingen, overeenkomstig lid 4, punt e).

9. De samenwerkingsgroep komt regelmatig en in ieder geval ten minste eenmaal per jaar bijeen met de krachtens Richtlijn (EU) 2022/2557 opgerichte groep voor de weerbaarheid van kritieke entiteiten, om de strategische samenwerking en de uitwisseling van informatie te bevorderen en te vergemakkelijken.

Artikel 15

CSIRT-netwerk

1. Om aan de ontwikkeling van het vertrouwen bij te dragen en een snelle en doeltreffende operationele samenwerking tussen de lidstaten te bevorderen, wordt een netwerk van nationale CSIRT's opgericht.

2. Het CSIRT-netwerk bestaat uit vertegenwoordigers van de krachtens artikel 10 aangewezen of ingestelde CSIRT's en het computercrisisresponsteam voor de instellingen, organen en instanties van de Unie (CERT-EU). De Commissie neemt als waarnemer deel aan het CSIRT-netwerk. Enisa verzorgt het secretariaat en verleent bijstand aan de samenwerking tussen de CSIRT's.

3. Het CSIRT-netwerk heeft de volgende taken:

a) het uitwisselen van informatie over de capaciteiten van de CSIRT's;

b) het vergemakkelijken van het delen, overdragen en uitwisselen van technologie en relevante maatregelen, beleidsmaatregelen, instrumenten, processen, beste praktijken, en kaders tussen de CSIRT's;

c) het uitwisselen van relevante informatie over incidenten, bijna-incidenten, cyberdreigingen, risico's en kwetsbaarheden;

d) het uitwisselen van informatie over publicaties en aanbevelingen op het gebied van cyberbeveiliging;

e) het zorgen voor interoperabiliteit met betrekking tot specificaties en protocollen voor informatie-uitwisseling;

f) op verzoek van een lid van het CSIRT-netwerk dat mogelijkerwijs gevolgen ondervindt van een incident, het uitwisselen en bespreken van informatie over dat incident en de daarmee samenhangende cyberdreigingen, risico's en kwetsbaarheden;

g) op verzoek van een lid van het CSIRT-netwerk, het bespreken en waar mogelijk uitvoeren van een gecoördineerde respons op een incident dat binnen de jurisdictie van die lidstaat is vastgesteld;

h) het verlenen van bijstand aan de lidstaten bij de aanpak van grensoverschrijdende incidenten uit hoofde van deze richtlijn;

i) het samenwerken, uitwisselen van beste praktijken en verlenen van bijstand aan de CSIRT's die op grond van artikel 12, lid 1, zijn aangewezen als coördinatoren, waar het gaat om het beheer van de gecoördineerde openbaarmaking van kwetsbaarheden die aanzienlijke gevolgen kunnen hebben voor entiteiten in meer dan één lidstaat;

j) het bespreken en identificeren van verdere vormen van operationele samenwerking, ook met betrekking tot:

   i) categorieën van cyberdreigingen en -incidenten;

   ii) vroegtijdige waarschuwingen;

   iii) wederzijdse bijstand;

   iv) beginselen en regelingen voor coördinatie als antwoord op grensoverschrijdende risico's en incidenten;

   v) op verzoek van een lidstaat, bijdragen aan het in artikel 9, lid 4, bedoelde nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons;

k) het informeren van de samenwerkingsgroep over zijn activiteiten en over de verdere vormen van operationele samenwerking, besproken op grond van punt j), en zo nodig het verzoeken om richtsnoeren in dat verband;

l) het opmaken van de balans van cyberbeveiligingsoefeningen, ook van de door Enisa georganiseerde oefeningen;

m) op verzoek van een individueel CSIRT, het bespreken van de capaciteiten en de paraatheid van dat CSIRT;

n) het samenwerken en uitwisselen van informatie met centra voor beveiligingsoperaties ("*Security Operations Centres*" — SOC's) op regionaal en Unieniveau om het gemeenschappelijk situationeel bewustzijn inzake incidenten en cyberdreigingen in de hele Unie te verbeteren;

o) indien van toepassing, het bespreken van de in artikel 19, lid 9, bedoelde collegiale-toetsingsverslagen;

p) het verstrekken van richtsnoeren om de convergentie van de operationele praktijken te vergemakkelijken waar het gaat om de toepassing van de bepalingen van dit artikel inzake operationele samenwerking.

4. Uiterlijk op 17 januari 2025, en vervolgens om de twee jaar, beoordeelt het CSIRT-netwerk, met het oog op de in artikel 40 bedoelde evaluatie, de vooruitgang die werd geboekt op het gebied van de operationele samenwerking en stelt het een verslag op. In het verslag worden met name conclusies en aanbevelingen geformuleerd op basis van het resultaat van de in artikel 19 bedoelde collegiale toetsingen, die worden uitgevoerd met betrekking tot de nationale CSIRT's. Dit verslag wordt voorgelegd aan de samenwerkingsgroep.

5. Het CSIRT-netwerk stelt zijn reglement van orde vast.

6. Het CSIRT-netwerk en EU-CyCLONe komen procedurele regelingen overeen en werken op basis daarvan samen.

Artikel 16

Het Europese netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe)

1. EU-CyCLONe wordt opgericht om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en crises op operationeel niveau te ondersteunen en te zorgen voor een regelmatige uitwisseling van relevante informatie tussen de lidstaten en de instellingen, organen en agentschappen van de Unie.

2. EU-CyCLONe bestaat uit de vertegenwoordigers van de cybercrisisbeheerautoriteiten van de lidstaten alsmede, in gevallen waarin een potentieel of aan de gang zijnd grootschalig cyberbeveiligingsincident een aanzienlijke impact heeft of dreigt te hebben op diensten en activiteiten die binnen het toepassingsgebied van deze richtlijn vallen, de Commissie. In andere gevallen neemt de Commissie als waarnemer deel aan de activiteiten van EU-CyCLONe.

Enisa verzorgt het secretariaat van EU-CyCLONe, ondersteunt de veilige uitwisseling van informatie en voorziet in de noodzakelijke instrumenten ter ondersteuning van de samenwerking tussen de lidstaten met het oog op een veilige uitwisseling van informatie.

Indien nodig kan EU-CyCLONe vertegenwoordigers van belanghebbenden uitnodigen om als waarnemers deel te nemen aan zijn werkzaamheden.

3. EU-CyCLONe heeft tot taak:

a) het niveau van de paraatheid te verhogen bij het beheer van grootschalige cyberbeveiligingsincidenten en crises;

b) een gedeeld situationeel bewustzijn voor grootschalige cyberbeveiligingsincidenten en crises te ontwikkelen;

c) de gevolgen en de impact van relevante grootschalige cyberbeveiligingsincidenten en crises te beoordelen en mogelijke beperkende maatregelen voor te stellen;

d) het beheer van grootschalige cyberbeveiligingsincidenten en crises te coördineren en de besluitvorming op politiek niveau met betrekking tot dergelijke incidenten en crises te ondersteunen;

e) op verzoek van een betrokken lidstaat de in artikel 9, lid 4, bedoelde nationale plannen voor grootschalige cyberbeveiligingsincidenten en crisisrespons te bespreken.

4. EU-CyCLONe stelt zijn reglement van orde vast.

5. EU-CyCLONe brengt regelmatig verslag uit aan de samenwerkingsgroep over het beheer van grootschalige cyberbeveiligingsincidenten en crises, alsook trends, waarbij met name aandacht wordt besteed aan de gevolgen ervan voor essentiële en belangrijke entiteiten.

6. EU-CyCLONe werkt samen met het CSIRT-netwerk op basis van overeengekomen procedurele regelingen als bepaald in artikel 15, lid 6.

7. Uiterlijk op 17 juli 2024 en vervolgens om de 18 maanden dient EU-CyCLONe bij het Europees Parlement en de Raad een beoordelingsverslag over zijn werkzaamheden in.

Artikel 17

Internationale samenwerking

De Unie kan indien nodig overeenkomstig artikel 218 VWEU internationale overeenkomsten met derde landen of internationale organisaties sluiten die hun deelname aan bepaalde activiteiten van de samenwerkingsgroep, het CSIRT-netwerk en EU-CyCLONe mogelijk maken en organiseren. Dergelijke overeenkomsten moeten in overeenstemming zijn met het Uniegegevensbeschermingsrecht.

Artikel 18

Verslag over de stand van zaken op het gebied van de cyberbeveiliging in de Unie

1. Enisa stelt in samenwerking met de Commissie en de samenwerkingsgroep een tweejaarlijks verslag over de stand van zaken op het gebied van cyberbeveiliging in de Unie op en legt dat verslag voor aan het Europees Parlement. Het verslag wordt onder meer in machinaal leesbare data beschikbaar gesteld en bevat het volgende:

a) een beoordeling van de cyberbeveiligingsrisico's op het niveau van de Unie, rekening houdend met het cyberdreigingslandschap;

b) een beoordeling van de ontwikkeling van cyberbeveiligingscapaciteiten in de publieke en private sectoren in de hele Unie;

c) een beoordeling van het algemene niveau van bewustzijn van cyberbeveiliging en cyberhygiëne bij burgers en entiteiten, met inbegrip van kleine en middelgrote ondernemingen;

d) een geaggregeerde beoordeling van het resultaat van de in artikel 19 bedoelde collegiale toetsingen;

e) een geaggregeerde beoordeling van het volwassenheidsniveau van de cyberbeveiligingscapaciteiten en -middelen in de hele Unie, met inbegrip van die op sectorniveau, en van de mate waarin de nationale cyberbeveiligingsstrategieën van de lidstaten op elkaar zijn afgestemd.

2. Het verslag bevat specifieke beleidsaanbevelingen om tekortkomingen te verhelpen en het cyberbeveiligingsniveau in de Unie te verhogen, en een samenvatting van de bevindingen over incidenten en cyberdreigingen voor de specifieke periode uit de overeenkomstig artikel 7, lid 6, van Verordening (EU) 2019/881 door Enisa opgestelde technische situatieverslagen inzake de EU-cyberbeveiliging Enisa.

3. In samenwerking met de Commissie, de samenwerkingsgroep en het CSIRT-netwerk ontwikkelt Enisa de methodologie, met inbegrip van de relevante variabelen, zoals kwantitatieve en kwalitatieve indicatoren, van de in lid 1, punt e), bedoelde geaggregeerde beoordeling.

Artikel 19

Collegiale toetsingen

1. Uiterlijk op 17 januari 2025 stelt de samenwerkingsgroep – met bijstand van de Commissie, Enisa en, voor zover relevant, het CSIRT-netwerk — de methodologie en de organisatorische aspecten van collegiale toetsingen vast teneinde lessen te trekken uit gedeelde ervaringen, het wederzijdse vertrouwen te versterken, een hoog gemeenschappelijk cyberbeveiligingsniveau te bewerkstelligen, en de cyberbeveiligingscapaciteiten en het cyberbeveiligingsbeleid van de lidstaten die voor de tenuitvoerlegging van deze richtlijn nodig zijn, te versterken. Deelname aan collegiale toetsingen is vrijwillig. De collegiale toetsingen worden uitgevoerd door cyberbeveiligingsdeskundigen. De cyberbeveiligingsdeskundigen worden aangewezen door ten minste twee andere lidstaten dan de lidstaat die wordt geëvalueerd.

De collegiale toetsingen hebben betrekking op ten minste een van de volgende zaken:

a) de mate van uitvoering van de in de artikelen 21 en 23 bedoelde risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging;

b) het niveau van de capaciteiten, met inbegrip van de beschikbare financiële, technische en personele middelen, en de doeltreffendheid van de uitoefening van de taken van de bevoegde autoriteiten;

c) de operationele capaciteit van de CSIRT's;

d) de mate van uitvoering van de in artikel 37 bedoelde wederzijdse bijstand;

e) de mate van uitvoering van het in artikel 29 bedoelde kader voor de uitwisseling van informatie over cyberbeveiliging;

f) specifieke kwesties van grens- of sectoroverschrijdende aard.

2. De in lid 1 bedoelde methodologie omvat objectieve, niet-discriminerende, eerlijke en transparante criteria op basis waarvan de lidstaten cyberbeveiligingsdeskundigen aanwijzen die in aanmerking komen om de collegiale toetsingen uit te voeren. De Commissie en Enisa nemen als waarnemers deel aan de collegiale toetsingen.

3. De lidstaten kunnen specifieke kwesties als bedoeld in lid 1, punt f), ter collegiale toetsing voorleggen.

4. Vóór de aanvang van een collegiale toetsing als bedoeld in lid 1, stellen de lidstaten de deelnemende lidstaten in kennis van de reikwijdte ervan, met inbegrip van de krachtens lid 3 voorgelegde specifieke kwesties.

5. Vóór de aanvang van de collegiale toetsing kunnen de lidstaten een zelfbeoordeling van de geëvalueerde aspecten verrichten en die zelfbeoordeling aan de aangewezen cyberbeveiligingsdeskundigen verstrekken. De samenwerkingsgroep stelt, bijgestaan door de Commissie en Enisa, de methodologie voor de zelfbeoordeling van de lidstaten vast.

6. De collegiale toetsingen omvatten fysieke of virtuele bezoeken ter plaatse en informatie-uitwisselingen elders. In overeenstemming met het beginsel van goede samenwerking verstrekt de aan een collegiale toetsing onderworpen lidstaat de aangewezen cyberbeveiligingsdeskundigen de informatie die nodig is voor de beoordeling, onverminderd het Unie- of nationale recht inzake de bescherming van vertrouwelijke of gerubriceerde informatie en de bescherming van essentiële staatsfuncties, zoals de nationale veiligheid. De samenwerkingsgroep ontwikkelt in samenwerking met de Commissie en Enisa passende gedragscodes ter ondersteuning van de werkmethoden van de aangewezen cyberbeveiligingsdeskundigen. Alle informatie die via de collegiale toetsing wordt verkregen, wordt uitsluitend voor dat doel gebruikt. De cyberbeveiligingsdeskundigen die aan de collegiale toetsing deelnemen, maken geen gevoelige of vertrouwelijke informatie die zij uit hoofde van die collegiale toetsing hebben verkregen, bekend aan derden.

7. Nadat een lidstaat aan een collegiale toetsing is onderworpen, worden dezelfde in die lidstaat geëvalueerde aspecten niet meer aan een collegiale toetsing onderworpen gedurende de twee jaar die volgen op de afsluiting van de collegiale toetsing, tenzij de lidstaat daarom verzoekt of tenzij dat wordt overeengekomen na een voorstel van de samenwerkingsgroep.

8. De lidstaten zorgen ervoor dat elk risico van belangenconflicten met betrekking tot de aangewezen cyberbeveiligingsdeskundigen aan de andere lidstaten, de samenwerkingsgroep, de Commissie en Enisa wordt gemeld voordat met de collegiale toetsing wordt begonnen. De aan een collegiale toetsing onderworpen lidstaat kan bezwaar maken tegen de aanwijzing van bepaalde cyberbeveiligingsdeskundigen om naar behoren gemotiveerde redenen die worden meegedeeld aan de lidstaat die de deskundigen aanwijst.

9. Cyberbeveiligingsdeskundigen die deelnemen aan collegiale toetsingen stellen verslagen op over de bevindingen en conclusies van de collegiale toetsingen. De aan een collegiale toetsing onderworpen lidstaten kunnen opmerkingen maken over de hen betreffende ontwerpverslagen en die opmerkingen worden bij de verslagen gevoegd. De verslagen bevatten aanbevelingen om verbetering mogelijk te maken van de aspecten die onderdeel zijn van de collegiale toetsing. De verslagen worden voorgelegd aan de samenwerkingsgroep en het CSIRT-netwerk wanneer dat relevant is. Een aan een collegiale toetsing onderworpen lidstaat kan besluiten zijn verslag of een bewerkte versie daarvan openbaar te maken.

HOOFDSTUK IV

RISICOBEHEERSMAATREGELEN EN RAPPORTAGEVERPLICHTINGEN OP HET GEBIED VAN CYBERBEVEILIGING

Artikel 20

Governance

1. De lidstaten zorgen ervoor dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreukendoor de entiteiten op dat artikel.

De toepassing van dit lid doet geen afbreuk aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.

2. De lidstaten zorgen ervoor dat de leden van de bestuursorganen van essentiële en belangrijke entiteiten een opleiding moeten volgen, en moedigen essentiële en belangrijke entiteiten aan om regelmatig een soortgelijke opleiding aan hun werknemers aan te bieden, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen.

Artikel 21

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in de eerste alinea bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

2. De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

3. De lidstaten zorgen ervoor dat de entiteiten, wanneer zij overwegen welke maatregelen als bedoeld in lid 2, punt d), van dit artikel passend zijn, rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures. De lidstaten zorgen er ook voor dat de entiteiten, wanneer zij overwegen welke maatregelen als bedoeld in lid 2, punt d), passend zijn, rekening moeten houden met de resultaten van de overeenkomstig artikel 22, lid 1, uitgevoerde gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

4. De lidstaten zien erop toe dat een entiteit die vaststelt dat zij niet voldoet aan de in lid 2 bedoelde maatregelen, onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen neemt.

5. Uiterlijk op 17 oktober 2024 stelt de Commissie uitvoeringshandelingen vast met de technische en methodologische vereisten van de in lid 2 bedoelde maatregelen met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten en aanbieders van vertrouwensdiensten.

De Commissie kan uitvoeringshandelingen vaststellen met de technische en methodologische vereisten en, zo nodig, de sectorale vereisten voor de in lid 2 bedoelde maatregelen met betrekking tot andere dan de in de eerste alinea van dit lid bedoelde essentiële en belangrijke entiteiten.

Bij de voorbereiding van de in de eerste en de tweede alinea van dit lid bedoelde uitvoeringshandelingen volgt de Commissie zoveel mogelijk de Europese en internationale normen en de relevante technische specificaties. De Commissie wisselt advies uit en werkt samen met de samenwerkingsgroep en Enisa rond de ontwerpuitvoeringshandelingen overeenkomstig artikel 14, lid 4, punt e).

Die uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 22

Op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens

1. De samenwerkingsgroep kan, in samenwerking met de Commissie en Enisa, gecoördineerde beveiligingsrisicobeoordelingen van specifieke kritieke ICT-diensten, ICT-systemen of ICT-producttoeleveringsketens uitvoeren, waarbij rekening wordt gehouden met technische en, indien van toepassing, niet-technische risicofactoren.

2. Na raadpleging van de samenwerkingsgroep en Enisa en, indien nodig, van relevante belanghebbenden stelt de Commissie vast welke specifieke kritieke ICT-diensten, ICT-systemen of ICT-producten aan de in lid 1 bedoelde gecoördineerde beveiligingsrisicobeoordeling kunnen worden onderworpen.

Artikel 23

Rapportageverplichtingen

1. Elke lidstaat zorgt ervoor dat essentiële en belangrijke entiteiten elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten als bedoeld in lid 3 (significant incident) onverwijld meldt bij zijn CSIRT of, indien van toepassing, zijn bevoegde autoriteit overeenkomstig lid 4. In voorkomend geval stellen de betrokken entiteiten de ontvangers van hun diensten onverwijld in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. Elke lidstaat zorgt ervoor dat die entiteiten onder meer alle informatie rapporteren die het CSIRT of, indien van toepassing, de bevoegde autoriteit in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen. Melding leidt niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.

Wanneer de betrokken entiteiten een significant incident overeenkomstig de eerste alinea melden bij de bevoegde autoriteit, zorgt de lidstaat ervoor dat die bevoegde autoriteit de melding na ontvangst doorstuurt naar het CSIRT.

In het geval van een grensoverschrijdend of sectoroverschrijdend significant incident zorgen de lidstaten ervoor dat relevante informatie die overeenkomstig lid 4 is gemeld, tijdig aan hun centrale contactpunten wordt verstrekt.

2. Indien van toepassing zorgen de lidstaten ervoor dat essentiële en belangrijke entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberdreiging worden getroffen, onverwijld meedelen welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stellen de entiteiten die ontvangers ook in kennis van de significante cyberdreiging zelf.

3. Een incident wordt als significant beschouwd als het:

a) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken;

b) andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

4. De lidstaten zorgen ervoor dat de betrokken entiteiten, voor de in lid 1 bedoelde melding, bij het CSIRT of, indien van toepassing, de bevoegde autoriteit:

a) onverwijld en in elk geval binnen 24 uur nadat zij kennis hebben gekregen van het significante incident, een vroegtijdige waarschuwing geven, waarin, indien van toepassing, wordt aangegeven of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt, dan wel grensoverschrijdende gevolgen zou kunnen hebben;

b) onverwijld en in elk geval binnen 72 uur nadat zij kennis hebben gekregen van het significante incident, een incidentmelding indienen met, indien van toepassing, een update van de in punt a) bedoelde informatie, een initiële beoordeling van het significante incident, met inbegrip van de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting;

c) op verzoek van het CSIRT of, indien van toepassing, de bevoegde autoriteit, een tussentijds verslag indienen over relevante updates van de situatie;

d) uiterlijk één maand na de indiening van het in punt b) bedoelde incidentmelding, een eindverslag indienen waarin het volgende is opgenomen:

   i) een gedetailleerde beschrijving van het incident, met inbegrip van de ernst en de gevolgen ervan;

   ii) het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;

   iii) toegepaste en lopende risicobeperkende maatregelen;

   iv) in voorkomend geval, de grensoverschrijdende gevolgen van het incident;

e) indien het incident nog aan de gang is op het moment dat het in punt d) bedoelde eindverslag wordt ingediend, zorgen de lidstaten ervoor dat de betrokken entiteiten op dat moment een voortgangsverslag indienen en binnen één maand nadat zij het incident hebben afgehandeld, een eindverslag indienen.

In afwijking van de eerste alinea, punt b), meldt een verlener van vertrouwensdiensten significante incidenten die gevolgen hebben voor de verlening van zijn vertrouwensdiensten onverwijld, en in elk geval binnen 24 uur nadat hij kennis heeft gekregen van het significante incident, bij het CSIRT of, indien van toepassing, de bevoegde autoriteit.

5. Het CSIRT of de bevoegde autoriteit verstrekt onverwijld en zo mogelijk binnen 24 uur na ontvangst van de in lid 4, punt a) bedoelde vroegtijdige waarschuwing een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het significante incident en, op verzoek van de entiteit, richtsnoeren of operationeel advies voor de uitvoering van mogelijke risicobeperkende maatregelen. Wanneer het CSIRT de in de lid 1 bedoelde melding niet als eerste heeft ontvangen, worden de richtsnoeren door de bevoegde autoriteit in samenwerking met het CSIRT verstrekt. Het CSIRT verleent aanvullende technische ondersteuning indien de betrokken entiteit daarom verzoekt. Wanneer wordt vermoed dat het significante incident van criminele aard is, geeft het CSIRT of de bevoegde autoriteit ook richtsnoeren voor het melden van het significante incident aan de rechtshandhavingsinstanties.

6. In voorkomend geval, en met name wanneer het significante incident betrekking heeft op twee of meer lidstaten, stelt het CSIRT, de bevoegde autoriteit of het centrale contactpunt de andere getroffen lidstaten en Enisa onverwijld in kennis van het significante incident. Die informatie omvat het soort informatie dat overeenkomstig lid 4 is ontvangen. Daarbij beschermen het CSIRT, de bevoegde autoriteit of het centrale contactpunt, overeenkomstig het Unie of het nationale recht, de beveiligings- en commerciële belangen van de entiteit, alsmede de vertrouwelijkheid van de verstrekte informatie.

7. Wanneer publieke bewustmaking nodig is om een significant incident te voorkomen of een lopend incident aan te pakken, of wanneer de bekendmaking van het significante incident anderszins in het algemeen belang is, kunnen het CSIRT van een lidstaat of, indien van toepassing, zijn bevoegde autoriteit , en in voorkomend geval de CSIRT's of de bevoegde autoriteiten van andere betrokken lidstaten, na raadpleging van de betrokken entiteit, het publiek over het significante incident informeren of van de entiteit verlangen dat zij dit doet.

8. Op verzoek van het CSIRT of de bevoegde autoriteit stuurt het centrale contactpunt de op grond van lid 1 ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten.

9. Het centrale contactpunt dient om de drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die overeenkomstig lid 1 van dit artikel en overeenkomstig artikel 30 zijn gemeld. Om bij te dragen tot het verstrekken van vergelijkbare informatie kan Enisa technische richtsnoeren vaststellen over de parameters van de informatie die in het samenvattend verslag moet worden opgenomen. Enisa stelt de samenwerkingsgroep en het CSIRT-netwerk om de zes maanden in kennis van zijn bevindingen over de ontvangen meldingen.

10. De CSIRT's of, indien van toepassing, de bevoegde autoriteiten verstrekken de uit hoofde van Richtlijn (EU) 2022/2557 bevoegde autoriteiten informatie over significante incidenten, en cyberdreigingen en bijna-incidenten die overeenkomstig lid 1 van dit artikel en overeenkomstig artikel 30 zijn gemeld door entiteiten die uit hoofde van Richtlijn (EU) 2022/2557 zijn aangemerkt als kritieke entiteiten.

11. De Commissie kan uitvoeringshandelingen vaststellen waarin het soort informatie, het format en de procedure van een op grond van lid 1 van dit artikel en op grond van artikel 30 ingediende melding en van een op grond van lid 2 van dit artikel gedane mededeling nader worden gespecificeerd.

Uiterlijk op 17 oktober 2024 stelt de Commissie met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsook aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, uitvoeringshandelingen vast waarin nader wordt gespecificeerd in welke gevallen een incident als significant wordt beschouwd als bedoeld in lid 3. De Commissie kan dergelijke uitvoeringshandelingen vaststellen met betrekking tot andere essentiële en belangrijke entiteiten.

De Commissie wisselt advies uit en werkt samen met de samenwerkingsgroep rond de in de eerste en tweede alinea van dit artikel bedoelde ontwerpuitvoeringshandelingen overeenkomstig artikel 14, lid 4, punt e).

Die uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 39, lid 2, bedoelde onderzoeksprocedure.

Artikel 24

Gebruik van Europese cyberbeveiligingscertificeringsregelingen

1. Om aan te tonen dat aan bepaalde eisen van artikel 21 wordt voldaan, kunnen de lidstaten eisen dat essentiële en belangrijke entiteiten bepaalde ICT-producten, ICT -diensten en ICT -processen gebruiken die door de essentiële of belangrijke entiteit zijn ontwikkeld of zijn gekocht bij derden die zijn gecertificeerd in het kader van Europese cyberbeveiligingscertificeringsregelingen die op grond van artikel 49 van Verordening (EU) 2019/881 zijn vastgesteld. Voorts moedigen de lidstaten essentiële en belangrijke entiteiten aan om gebruik te maken van gekwalificeerde vertrouwensdiensten.

2. De Commissie is bevoegd om overeenkomstig artikel 38 gedelegeerde handelingen vast te stellen om deze richtlijn aan te vullen door te bepalen welke categorieën van essentiële en belangrijke entiteiten verplicht zijn om bepaalde ICT-producten, ICT -diensten en ICT -processen te gebruiken of een certificaat te verkrijgen in het kader van een Europese cyberbeveiligingsregeling die op grond van artikel 49 van Verordening (EU) 2019/881 is vastgesteld. Die gedelegeerde handelingen worden vastgesteld indien is vastgesteld dat het niveau van cyberbeveiliging onvoldoende is en voorzien in een uitvoeringsperiode.

Alvorens dergelijke gedelegeerde handelingen vast te stellen, voert de Commissie een effectbeoordeling uit en pleegt zij overleg overeenkomstig artikel 56 van Verordening (EU) 2019/881.

3. Indien er geen passende Europese cyberbeveiligingscertificeringsregeling voor de toepassing van lid 2 van dit artikel beschikbaar is, kan de Commissie, na raadpleging van de samenwerkingsgroep en de Europese Groep voor cyberbeveiligingscertificering, Enisa verzoeken een potentiële regeling op te stellen op grond van artikel 48, lid 2, van Verordening (EU) 2019/881.

Artikel 25

Normalisatie

1. Om de convergente uitvoering van artikel 21, leden 1 en 2, te bevorderen, moedigen de lidstaten, zonder het gebruik van een bepaald type technologie op te leggen of te bevoordelen, het gebruik aan van Europese en internationale normen en technische specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen.

2. Enisa stelt in samenwerking met de lidstaten en, in voorkomend geval, na overleg met de relevante belanghebbenden adviezen en richtsnoeren op over de technische gebieden die in verband met lid 1 in aanmerking moeten worden genomen, alsmede over de reeds bestaande normen, met inbegrip van nationale normen, die het mogelijk maken deze gebieden te bestrijken.

HOOFDSTUK V

JURISDICTIE EN REGISTRATIE

Artikel 26

Jurisdictie en territorialiteit

1. Binnen het toepassingsgebied van deze richtlijn vallende entiteiten worden geacht onder de jurisdictie te vallen van de lidstaat waar zij zijn gevestigd, behalve in het geval van:

a) aanbieders van openbare elektronischecommunicatienetwerken of aanbieders van openbare elektronischecommunicatiediensten, die worden geacht te vallen onder de jurisdictie van de lidstaat waar zij hun diensten aanbieden;

b) DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines of van platforms voor socialenetwerkdiensten, die worden geacht onder de jurisdictie te vallen van de lidstaat waar zij hun hoofdvestiging in de Unie overeenkomstig lid 2 hebben;

c) overheidsinstanties, die worden geacht te vallen onder de jurisdictie van de lidstaat die ze heeft opgericht.

2. Voor de toepassing van deze richtlijn wordt een in lid 1, punt b), bedoelde entiteit geacht haar hoofdvestiging in de Unie te hebben in de lidstaat waar de beslissingen met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's hoofdzakelijk worden genomen. Indien niet kan worden bepaald welke lidstaat dat is of indien dergelijke besluiten niet in de Unie worden genomen, wordt de hoofdvestiging geacht zich te bevinden in de lidstaat waar cyberbeveiligingsactiviteiten worden uitgevoerd. Indien niet kan worden bepaald welke lidstaat dat is, wordt de hoofdvestiging geacht zich te bevinden in de lidstaat waar de betrokken entiteit de vestiging met het grootste aantal werknemers in de Unie heeft.

3. Indien een entiteit als bedoeld in lid 1, punt b), niet in de Unie is gevestigd, maar diensten in de Unie aanbiedt, wijst zij een vertegenwoordiger in de Unie aan. De vertegenwoordiger is gevestigd in een van de lidstaten waar de diensten worden aangeboden. Deze entiteit wordt geacht onder de jurisdictie te vallen van de lidstaat waar de vertegenwoordiger is gevestigd. Bij ontstentenis van een overeenkomstig dit lid aangewezen vertegenwoordiger in de Unie kan elke lidstaat waar de entiteit diensten verricht, juridische stappen ondernemen tegen de entiteit wegens inbreuk op deze richtlijn.

4. De aanwijzing van een vertegenwoordiger door een entiteit als bedoeld in lid 1, punt b), doet geen afbreuk aan juridische stappen die tegen de entiteit zelf kunnen worden ingesteld.

5. Lidstaten die een verzoek om wederzijdse bijstand hebben ontvangen met betrekking tot een entiteit als bedoeld in lid 1, punt b), kunnen, binnen de grenzen van dat verzoek, passende toezichts- en handhavingsmaatregelen nemen ten aanzien van de betrokken entiteit die op hun grondgebied diensten verleent of waarvan een netwerk- en informatiesysteem zich op hun grondgebied bevindt.

Artikel 27

Register van entiteiten

1. Enisa creëert en onderhoudt een register van DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, op basis van de informatie die is ontvangen van de centrale contactpunten in overeenstemming met lid 4. Op verzoek geeft Enisa bevoegde autoriteiten toegang tot dat register, waarbij zij er zo nodig voor zorgt dat de vertrouwelijkheid van de informatie wordt beschermd.

2. De lidstaten vereisen van de in lid 1 bedoelde entiteiten dat zij de volgende informatie uiterlijk op 17 januari 2025 bij de bevoegde autoriteiten indienen:

a) de naam van de entiteit;

b) de relevante sector, subsector en soort entiteit bedoeld in bijlage I of II, waar van toepassing;

c) het adres van de hoofdvestiging van de entiteit en haar andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van haar op grond van artikel 26, lid 3, aangewezen vertegenwoordiger;

d) actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers van de entiteit en, indien van toepassing, haar op grond van artikel 26, lid 3, aangewezen vertegenwoordiger;

e) de lidstaten waar de entiteit diensten verleent, en

f) de IP-bereiken van de entiteit.

3. De lidstaten zorgen ervoor dat de in lid 1 bedoelde entiteiten de bevoegde autoriteit onverwijld en in elk geval binnen drie maanden na de datum waarop de wijziging van kracht is geworden, in kennis stellen van eventuele wijzigingen in de gegevens die zij op grond van lid 2 hebben ingediend.

4. Na ontvangst van de in de leden 2 en 3 bedoelde informatie, met uitzondering van de in lid 2, punt f), bedoelde informatie, zendt het centrale contactpunt van de betrokken lidstaat deze zonder onnodige vertraging door naar Enisa.

5. Indien van toepassing wordt de in de leden 2 en 3 van dit artikel bedoelde informatie ingediend via het in artikel 3, lid 4, vierde alinea, bedoelde nationale mechanisme.

Artikel 28

Database met domeinnaamregistratiegegevens

1. Om bij te dragen aan de beveiliging, stabiliteit en weerbaarheid van het DNS schrijven de lidstaten voor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, met de nodige zorgvuldigheid nauwkeurige en volledige domeinnaamregistratiegegevens verzamelen en bijhouden in een speciale database overeenkomstig de het Unierecht inzake gegevensbescherming voor wat betreft gegevens die persoonsgegevens zijn.

2. Voor de toepassing van lid 1 schrijven de lidstaten voor dat de database met domeinnaamregistratiegegevens over de registratie van domeinnamen de noodzakelijke informatie bevat om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren. Die informatie omvat:

a) de domeinnaam;

b) de registratiedatum van registratie;

c) de naam, het e-mailadres en het telefoonnummer van de registrant;

d) het e-mailadres en het telefoonnummer van het contactpunt dat de domeinnaam beheert, indien deze verschillen van die van de registrant.

3. De lidstaten schrijven voor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, over beleidslijnen en procedures, waaronder verificatieprocedures, beschikken om ervoor te zorgen dat de in lid 1 bedoelde databases juiste en volledige informatie bevatten. De lidstaten schrijven voor dat deze beleidslijnen en procedures openbaar worden gemaakt.

4. De lidstaten schrijven voor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, onverwijld na de registratie van een domeinnaam, de domeinnaamregistratiegegevens die geen persoonsgegevens zijn, openbaar maken.

5. De lidstaten schrijven voor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, op rechtmatige en naar behoren gemotiveerde verzoeken van legitieme toegangvragende partijen toegang verlenen tot specifieke met gegevens over de registratie van domeinnamen, overeenkomstig het Uniegegevensbeschermingsrecht van de Unie. De lidstaten schrijven voor dat registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verzoeken om toegang onverwijld en in elk geval binnen 72 uur na ontvangst van het verzoek beantwoorden. De lidstaten schrijven voor dat het beleid en de procedures met betrekking tot de bekendmaking van dergelijke gegevens openbaar worden gemaakt.

6. De naleving van de in de leden 1 tot en met 5 vastgestelde verplichtingen mag er niet toe leiden dat domeinnaamregistratiegegevens tweemaal moeten worden verzameld. Daartoe schrijven de lidstaten voor dat registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, met elkaar samenwerken.

HOOFDSTUK VI

INFORMATIE-UITWISSELING

Artikel 29

Informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging

1. De lidstaten zorgen ervoor dat binnen het toepassingsgebied van deze richtlijn vallende entiteiten en, indien van toepassing, andere entiteiten die niet binnen het toepassingsgebied van deze richtlijn vallen, op vrijwillige basis onderling relevante informatie over cyberbeveiliging kunnen uitwisselen, met inbegrip van informatie over cyberdreigingen, bijnaincidenten, kwetsbaarheden, technieken en procedures, indicatoren voor aantasting, vijandige tactieken, dreigingsactorspecifieke informatie, cyberbeveiligingswaarschuwingen en aanbevelingen betreffende de configuratie van cyberbeveiligingsinstrumenten om cyberaanvallen te detecteren, wanneer dat uitwisselen van informatie:

a) beoogt incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken;

b) het niveau van de cyberbeveiliging verhoogt, met name door de bewustwording met betrekking tot cyberdreigingen te vergroten, het vermogen van dergelijke dreigingen om zich te verspreiden te beperken of te belemmeren, een reeks verdedigingscapaciteiten, het herstel en openbaarmaking van kwetsbaarheden, het opsporen van dreigingen, beheersings- en preventietechnieken, beperkingsstrategieën of respons- en herstelfasen te ondersteunen of gezamenlijk onderzoek naar cyberdreigingen door publieke en particuliere entiteiten te bevorderen.

2. De lidstaten zorgen ervoor dat de informatie-uitwisseling plaatsvindt binnen gemeenschappen van essentiële en belangrijke entiteiten en, indien van toepassing, hun leveranciers of dienstverleners. Die uitwisseling wordt uitgevoerd door middel van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie.

3. De lidstaten faciliteren de vaststelling van de in lid 2 van dit artikel bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging. In dergelijke regelingen kunnen de operationele elementen, met inbegrip van het gebruik van specifieke ICT-platforms en automatiseringshulpmiddelen, de inhoud en de voorwaarden van de informatie-uitwisselingsregelingen worden gespecificeerd. Bij het vaststellen van de details van de betrokkenheid van de overheid bij dergelijke regelingen kunnen de lidstaten voorwaarden opleggen aan de informatie die door de bevoegde autoriteiten of de CSIRT's ter beschikking wordt gesteld. De lidstaten bieden bijstand aan voor de toepassing van dergelijke regelingen overeenkomstig hun in artikel 7, lid 2, punt h), bedoelde beleid.

4. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten de bevoegde autoriteiten in kennis stellen van hun deelname aan de in lid 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

5. Enisa ondersteunt de invoering van de in lid 2 bedoelde informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging door beste praktijken uit te wisselen en richtsnoeren te verstekken.

Artikel 30

Vrijwillige melding van relevante informatie

1. De lidstaten zorgen ervoor dat, naast de in artikel 23 geregelde meldingsplicht, op vrijwillige basis meldingen bij de CSIRT's of, indien van toepassing, de bevoegde autoriteiten kunnen worden ingediend door:

a) essentiële en belangrijke entiteiten betreffende cyberdreigingen en bijna-incidenten;

b) andere dan in punt a) bedoelde entiteiten, ongeacht of zij binnen het toepassingsgebied van deze richtlijn vallen, wat significante incidenten, cyberdreigingen en bijna-incidenten betreft.

2. De lidstaten verwerken de in lid 1 van dit artikel bedoelde meldingen volgens de in artikel 23 vastgestelde procedure. De lidstaten kunnen voorrang geven aan de verwerking van verplichte meldingen boven vrijwillige meldingen.

Indien nodig verstrekken de CSIRT's en, waar dit van toepassing is, de bevoegde autoriteiten, de centrale contactpunten de informatie over de meldingen die op grond van dit artikel zijn ontvangen, met inachtneming van de vertrouwelijkheid en passende bescherming van de door de meldende entiteit verstrekte informatie. Onverminderd de voorkoming van, het onderzoek naar en de opsporing en de vervolging van strafbare feiten, mag vrijwillige melding er niet toe leiden dat de meldende entiteit bijkomende verplichtingen worden opgelegd waaraan zij niet onderworpen zou zijn geweest indien zij de melding niet had ingediend.

HOOFDSTUK VII

TOEZICHT EN HANDHAVING

Artikel 31

Algemene aspecten van het toezicht en de handhaving

1. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten effectief toezicht houden op en de noodzakelijke maatregelen nemen om te zorgen voor de naleving van deze richtlijn.

2. De lidstaten kunnen hun bevoegde autoriteiten toestaan prioriteit te geven aan toezichtstaken. Deze prioritering is gebaseerd op een risicogebaseerde benadering. Daartoe kunnen de bevoegde autoriteiten bij de uitvoering van hun in de artikelen 32 en 33 bedoelde toezichthoudende taken toezichtmethoden vaststellen aan de hand waarvan dergelijke taken volgens een risicogebaseerde benadering kunnen worden geprioriteerd.

3. Bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens, werken de bevoegde autoriteiten nauw samen met de toezichthoudende autoriteiten uit hoofde van Verordening (EU) 2016/679, onverminderd de bevoegdheid en taken van de toezichthoudende autoriteiten krachtens die verordening.

4. Onverminderd de nationale wettelijke en institutionele kaders zorgen de lidstaten ervoor dat de bevoegde autoriteiten bij het toezicht op de naleving door overheidsinstanties van deze richtlijn en bij het opleggen van handhavingsmaatregelen inzake inbreuken op deze richtlijn over passende bevoegdheden beschikken om bij de uitvoering van deze taken operationeel onafhankelijk te zijn van de overheidsinstanties waarop zij toezicht houden. De lidstaten kunnen besluiten passende, evenredige en doeltreffende toezichts- en handhavingsmaatregelen ten aanzien van die instanties te nemen in overeenstemming met de nationale wetgevings- en institutionele kaders.

Artikel 32

Toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten

1. De lidstaten zorgen ervoor dat de toezichts- of handhavingsmaatregelen die met betrekking tot de in deze richtlijn vastgestelde verplichtingen aan essentiële entiteiten worden opgelegd, doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van elk afzonderlijk geval.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot essentiële entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:

a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles die worden uitgevoerd door daartoe opgeleide professionals;

b) regelmatige en gerichte beveiligingsaudits die worden uitgevoerd door een onafhankelijke instantie of een bevoegde autoriteit;

c) ad-hocaudits, ook in gevallen waarin dat gerechtvaardigd is op grond van een significant incident of inbreuk op deze richtlijn door de essentiële entiteit;

d) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

e) verzoeken om informatie die nodig is om de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting op grond van artikel 27 om bij de bevoegde autoriteiten informatie in te dienen;

f) verzoeken om toegang tot gegevens, documenten en informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;

g) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in de eerste alinea, punt b), bedoelde gerichte beveiligingsaudits zijn gebaseerd op door de bevoegde autoriteit of de gecontroleerde entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.

De resultaten van een gerichte beveiligingsaudit worden ter beschikking gesteld van de bevoegde autoriteit. De kosten van een dergelijke gerichte door een onafhankelijke instantie uitgevoerde beveiligingsaudit worden betaald door de gecontroleerde entiteit, behalve in naar behoren gemotiveerde gevallen waarin de bevoegde autoriteit anders besluit.

3. Bij de uitoefening van hun bevoegdheden uit hoofde van lid 2, punt e), f) of g), vermelden de bevoegde autoriteiten het doel van het verzoek en specificeren zij de gevraagde informatie.

4. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten bij de uitoefening van hun handhavingsbevoegdheden ten aanzien van essentiële entiteiten, de bevoegdheid hebben om ten minste:

a) waarschuwingen te geven over inbreuken door de betrokken entiteiten op deze richtlijn;

b) bindende aanwijzingen vast te stellen, met inbegrip van aanwijzingen inzake de noodzakelijke maatregelen om een incident te voorkomen of te verhelpen alsook uiterste termijnen voor de uitvoering van dergelijke maatregelen en voor verslaggeving over de uitvoering ervan, of een bevel uit te vaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op deze richtlijn te verhelpen;

c) de betrokken entiteiten te gelasten een einde te maken aan gedragingen die inbreuk maken op deze richtlijn en af te zien van herhaling van die gedragingen;

d) de betrokken entiteiten te gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met artikel 21 of te voldoen aan de in artikel 23 vastgestelde rapportageverplichtingen;

e) de betrokken entiteiten te gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;

f) de betrokken entiteiten te gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

g) een controlefunctionaris aan te wijzen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteiten aan de artikelen 21 en 23 voldoen;

h) de betrokken entiteiten te gelasten aspecten van inbreuken op deze richtlijn op een bepaalde manier openbaar te maken;

i) op grond van artikel 34 een administratieve geldboete op te leggen of de oplegging ervan door de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht te verzoeken bovenop een of meer van de in punten a) tot en met h) van dit lid bedoelde maatregelen.

5. Indien de op grond van lid 4, punten a) tot en met d) en punt f), genomen handhavingsmaatregelen ondoeltreffend zijn, zorgen de lidstaten ervoor dat hun bevoegde autoriteiten de bevoegdheid hebben om een termijn vast te stellen waarbinnen de essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen of aan de eisen van die autoriteiten te voldoen. Indien de gevraagde actie niet binnen de gestelde termijn wordt ondernomen, zorgen de lidstaten ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om:

a) een certificering of vergunning tijdelijk op te schorten of een certificerings- of vergunningsinstantie of een rechterlijke instantie overeenkomstig het nationale recht te verzoeken deze tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de essentiële entiteit verleende diensten of verrichte activiteiten;

b) verzoeken dat de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

Op grond van dit lid opgelegde tijdelijke opschortingen of verboden worden slechts toegepast totdat de betrokken entiteit de noodzakelijke maatregelen neemt om de tekortkomingen te verhelpen of voldoet aan de vereisten van de bevoegde autoriteit waarvoor dergelijke handhavingsmaatregelen zijn opgelegd. Het opleggen van dergelijke tijdelijke opschortingen of verboden moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het Unierecht en het Handvest, waaronder het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het vermoeden van onschuld en de rechten van de verdediging.

De in dit lid bedoelde handhavingsmaatregelen zijn niet van toepassing op onder deze richtlijn vallende overheidsinstanties.

6. De lidstaten zorgen ervoor dat elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, de bevoegdheid heeft om ervoor te zorgen dat deze entiteit deze richtlijn nakomt. De lidstaten zorgen ervoor dat dergelijke natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze richtlijn.

Wat overheidsinstanties betreft, doet dit lid geen afbreuk aan het nationale recht inzake de aansprakelijkheid van ambtenaren en gekozen of benoemde overheidsfunctionarissen.

7. Bij het nemen van de in lid 4 of 5 bedoelde handhavingsmaatregelen eerbiedigen de bevoegde autoriteiten de rechten van de verdediging en houden zij rekening met de omstandigheden van elk afzonderlijk geval, en houden zij ten minste naar behoren rekening met:

a) de ernst van de inbreuk en het belang van de geschonden bepalingen, waarbij onder meer het volgende in ieder geval een ernstige inbreuk vormt:

   i) herhaalde inbreuken;

   ii) niet melden of niet verhelpen van significante incidenten;

   iii) niet verhelpen van tekortkomingen naar aanleiding van bindende aanwijzingen van de bevoegde autoriteiten;

   iv) het belemmeren van audits of monitoringsactiviteiten waartoe de bevoegde autoriteit opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk;

   v) het verstrekken van valse of zeer onnauwkeurige informatie met betrekking tot de in de artikelen 21 en 23 vastgelegde cyberbeveiligingsrisicobeheersmaatregelen of rapportageverplichtingen;

b) de duur van de inbreuk;

c) eventuele relevante eerdere inbreuken door de betrokken entiteit;

d) elke veroorzaakte materiële of immateriële schade, met inbegrip van elke financiële of economische schade, effecten op andere diensten en het aantal getroffen gebruikers;

e) opzet of nalatigheid van de pleger van de inbreuk;

f) door de entiteit genomen maatregelen om de materiële of immateriële schade te voorkomen of te beperken;

g) de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;

h) de mate waarin de aansprakelijk gestelde natuurlijke of rechtspersonen meewerken met de bevoegde autoriteiten.

8. De bevoegde autoriteiten geven een gedetailleerde motivering van hun handhavingsmaatregelen. Alvorens dergelijke maatregelen vast te stellen, stellen de bevoegde autoriteiten de betrokken entiteiten in kennis van hun voorlopige bevindingen. Ook geven zij die entiteiten een redelijke termijn om opmerkingen te maken, behalve in naar behoren gemotiveerde gevallen waarin onmiddellijk optreden om incidenten te voorkomen of erop te reageren anders zou worden belemmerd.

9. De lidstaten zorgen ervoor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten de relevante uit hoofde van Richtlijn (EU) 2022/2557 bevoegde autoriteiten binnen dezelfde lidstaat in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een entiteit die op grond van Richtlijn (EU) 2022/2557 als kritieke entiteit wordt aangemerkt, voldoet aan deze richtlijn. In voorkomend geval kunnen de uit hoofde van Richtlijn (EU) 2022/2557 bevoegde autoriteiten de uit hoofde van deze richtlijn bevoegde autoriteiten verzoeken hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een entiteit die is aangemerkt als kritieke entiteit uit hoofde van Richtlijn (EU) 2022/2557.

10. De lidstaten zorgen ervoor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten samenwerken met de relevante uit hoofde van Verordening (EU) 2022/2554 bevoegde autoriteiten van de betrokken lidstaat. De lidstaten zorgen er met name voor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten het oversightforum dat is opgericht op grond van artikel 32, lid 1, van Verordening (EU) 2022/2554 in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële entiteit die op grond van artikel 31 van Verordening (EU) 2022/2554 als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze richtlijn.

Artikel 33

Toezichts- en handhavingsmaatregelen met betrekking tot belangrijke entiteiten

1. Wanneer het bewijs, de aanwijzing of informatie wordt geleverd dat een belangrijke entiteit beweerdelijk deze richtlijn, en met name de artikelen 21 en 23, niet nakomt, zorgen de lidstaten ervoor dat de bevoegde autoriteiten zo nodig maatregelen nemen door middel van toezichtmaatregelen achteraf. De lidstaten zorgen ervoor dat die maatregelen doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van ieder afzonderlijk geval.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezichthoudende taken met betrekking tot belangrijke entiteiten de bevoegdheid hebben om deze entiteiten te onderwerpen aan ten minste:

a) inspecties ter plaatse en toezicht elders achteraf, uitgevoerd daartoe door opgeleide professionals;

b) door een onafhankelijke instantie of een bevoegde autoriteit uitgevoerde gerichte beveiligingsaudits;

c) beveiligingsscans op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit;

d) verzoeken om informatie die nodig is om de door de betrokken entiteit genomen maatregelen voor het beheer van cyberbeveiligingsrisico's achteraf te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid, alsmede de naleving van de verplichting op grond van artikel 27 om informatie in te dienen bij de bevoegde autoriteiten;

e) verzoeken om toegang tot gegevens, documenten en informatie die nodig zijn voor de uitoefening van hun toezichthoudende taken;

f) verzoeken om bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van beveiligingsaudits die door een gekwalificeerde auditor zijn uitgevoerd en de respectieve onderliggende bewijzen.

De in de eerste alinea, punt b), bedoelde gerichte beveiligingsaudits zijn gebaseerd op door de bevoegde autoriteit of de gecontroleerde entiteit uitgevoerde risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.

De resultaten van een gerichte beveiligingsaudit worden ter beschikking gesteld van de bevoegde autoriteit. De kosten van een dergelijke gerichte door onafhankelijke instantie uitgevoerde beveiligingsaudit, worden betaald door de gecontroleerde entiteit, behalve in naar behoren gemotiveerde gevallen waarin de bevoegde autoriteit anders besluit.

3. Bij de uitoefening van hun bevoegdheden uit hoofde van lid 2, punt d), e) of f), vermelden de bevoegde autoriteiten het doel van het verzoek en de gevraagde informatie.

4. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun handhavingsbevoegdheden ten aanzien van belangrijke entiteiten, ten minste de bevoegdheid hebben om:

a) waarschuwingen te geven over inbreuken op deze richtlijn door de betrokken entiteiten;

b) bindende aanwijzingen vast te stellen of een bevel uit te vaardigen waarin de betrokken entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuk op deze richtlijn te verhelpen;

c) de betrokken entiteiten te gelasten een einde te maken aan gedragingen die inbreuk maken op deze richtlijn en af te zien van herhaling van die gedragingen;

d) de betrokken entiteiten te gelasten er op een gespecificeerde wijze en binnen een gespecificeerde termijn voor te zorgen dat hun maatregelen voor het beheer van cyberbeveiligingsrisico's in overeenstemming zijn met artikel 21 of te voldoen aan de in artikel 23 vastgestelde rapportageverplichtingen;

e) de betrokken entiteiten te gelasten de natuurlijke of rechtspersonen ten aanzien van wie zij diensten verlenen of activiteiten uitvoeren die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke of rechtspersonen kunnen nemen als reactie op die dreiging;

f) de betrokken entiteiten te gelasten de naar aanleiding van een beveiligingsaudit gedane aanbevelingen binnen een redelijke termijn uit te voeren;

g) de betrokken entiteiten te gelasten aspecten van inbreuken op deze richtlijn op een bepaalde manier openbaar te maken;

h) op grond van artikel 34 een administratieve geldboete op te leggen of de oplegging ervan door de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht te verzoeken bovenop een van de in de punten a) tot en met g) van dit lid bedoelde maatregelen.

5. *Artikel 32*, leden 6 tot en met 8, is van overeenkomstige toepassing op de toezichts- en handhavingsmaatregelen waarin dit artikel voorziet voor belangrijke entiteiten.

6. De lidstaten zorgen ervoor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten samenwerken met de relevante uit hoofde van Verordening (EU) 2022/2554 bevoegde autoriteiten van de betrokken lidstaat. De lidstaten zorgen er met name voor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten het oversightforum dat is opgericht op grond van artikel 32, lid 1, van Verordening (EU) 2022/2554 in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een belangrijke entiteit die op grond van artikel 31 van Verordening (EU) 2022/2554 als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan deze richtlijn.

Artikel 34

Algemene voorwaarden voor het opleggen van administratieve geldboeten aan essentiële en belangrijke entiteiten

1. De lidstaten zorgen ervoor dat de administratieve geldboeten die uit hoofde van dit artikel aan essentiële en belangrijke entiteiten worden opgelegd wegens inbreuken op deze richtlijn, doeltreffend, evenredig en afschrikkend zijn, rekening houdend met de omstandigheden van elk afzonderlijk geval.

2. Administratieve geldboeten worden opgelegd bovenop een of meer van de in artikel 32, lid 4, punten a) tot en met h), artikel 32, lid 5, en artikel 33, lid 4, punten a) tot en met g), bedoelde maatregelen.

3. Bij het besluit om een administratieve geldboete op te leggen en bij de vaststelling van het bedrag ervan in elk afzonderlijk geval wordt er ten minste naar behoren rekening gehouden met de in artikel 32, lid 7, genoemde elementen.

4. De lidstaten zorgen ervoor dat essentiële entiteiten die inbreuk maken op artikel 21 of 23 overeenkomstig de leden 2 en 3 van dit artikel onderworpen worden aan administratieve geldboeten met een maximumbedrag van ten minste 10 000 000 EUR of ten minste 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort, afhankelijk van welk bedrag hoger is.

5. De lidstaten zorgen ervoor dat belangrijke entiteiten die inbreuk maken op artikel 21 of 23 overeenkomstig de leden 2 en 3 van dit artikel onderworpen worden aan administratieve geldboeten met een maximumbedrag van ten minste 7 000 000 EUR of ten minste 1,4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort, afhankelijk van welk bedrag hoger is.

6. De lidstaten kunnen voorzien in de bevoegdheid om dwangsommen op te leggen om een essentiële of belangrijke entiteit te dwingen een inbreuk op deze richtlijn te staken in overeenstemming met een voorafgaand besluit van de bevoegde autoriteit.

7. Onverminderd de bevoegdheden van de bevoegde autoriteiten uit hoofde van de artikelen 32 en 33 kan elke lidstaat bepalen of en in welke mate administratieve geldboeten kunnen worden opgelegd aan overheidsinstanties.

8. Indien het rechtsstelsel van een lidstaat niet in administratieve geldboeten voorziet, zorgt die lidstaat ervoor dat dit artikel aldus wordt toegepast dat de geldboete wordt geïnitieerd door de bevoegde autoriteit en wordt opgelegd door de bevoegde nationale rechterlijke instanties, waarbij wordt gewaarborgd dat die wettelijke voorzieningen doeltreffend zijn en van gelijke werking zijn als de door bevoegde autoriteiten opgelegde administratieve geldboeten. De opgelegde geldboeten zijn in elk geval doeltreffend, evenredig en afschrikkend. De lidstaat stelt de Commissie uiterlijk op 17 oktober 2024 in kennis van de wettelijke bepalingen die hij op grond van dit lid vaststelt, en onverwijld van eventuele latere wijzigingswetten of wijzigingen die daarop van invloed zijn.

Artikel 35

Inbreuken die een inbreuk in verband met persoonsgegevens inhouden

1. Wanneer de bevoegde autoriteiten er bij toezicht of handhaving kennis van krijgen dat de inbreuk door een essentiële of belangrijke entiteit op de in de artikelen 21 en 23 van deze richtlijn vastgestelde verplichtingen een inbreuk in verband met persoonsgegevens zoals gedefinieerd in artikel 4, punt 12, van Verordening (EU) 2016/679 kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stellen zij de bevoegde toezichthoudende autoriteiten als bedoeld in de artikelen 55 en 56 van die verordening daarvan onverwijld in kennis.

2. Indien de toezichthoudende autoriteiten als bedoeld in artikel 55 of 56 van Verordening (EU) 2016/679 een administratieve geldboete op grond van artikel 58, lid 2, punt i), van die verordening opleggen, leggen de bevoegde autoriteiten geen administratieve geldboete op grond van artikel 34 van deze richtlijn op voor een inbreuk als bedoeld in lid 1 van dit artikel die voortvloeit uit dezelfde gedraging als die waarvoor de administratieve geldboete uit hoofde van artikel 58, lid 2, punt i), van Verordening (EU) 2016/679 is opgelegd. De bevoegde autoriteiten kunnen echter de handhavingsmaatregelen opleggen waarin artikel 32, lid 4, punten a) tot en met h), artikel 32, lid 5, en artikel 33, lid 4, punten a) tot en met g), van deze richtlijn voorzien.

3. Wanneer de op grond van Verordening (EU) 2016/679 bevoegde toezichthoudende autoriteit in een andere lidstaat dan de bevoegde autoriteit is gevestigd, stelt de bevoegde autoriteit de in haar eigen lidstaat gevestigde toezichthoudende autoriteit in kennis van de in lid 1 bedoelde potentiële inbreuk in verband met persoonsgegevens.

Artikel 36

Sancties

De lidstaten stellen regels vast voor de sancties die van toepassing zijn op inbreuken op de krachtens deze richtlijn vastgestelde nationale bepalingen en nemen alle noodzakelijke maatregelen om ervoor te zorgen dat deze worden uitgevoerd. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn. De lidstaten stellen de Commissie uiterlijk op 17 januari 2025 in kennis van deze regels en maatregelen en stellen haar onverwijld in kennis van eventuele latere wijzigingen daarvan.

Artikel 37

Wederzijdse bijstand

1. Wanneer een entiteit diensten verricht in meer dan één lidstaat, of indien zij diensten verricht in een of meer lidstaten en haar netwerk- en informatiesystemen zich in een of meer andere lidstaten bevinden, werken de bevoegde autoriteiten van de betrokken lidstaten met elkaar samen en verlenen ze elkaar indien nodig bijstand. Die samenwerking houdt ten minste in dat:

a) de bevoegde autoriteiten die in een lidstaat toezichts- of handhavingsmaatregelen toepassen, via het centrale contactpunt de bevoegde autoriteiten in de andere betrokken lidstaten informeren en raadplegen over de genomen toezichts- en handhavingsmaatregelen;

b) een bevoegde autoriteit een andere bevoegde autoriteit kan verzoeken toezichts- of handhavingsmaatregelen te nemen;

c) een bevoegde autoriteit, na ontvangst van een gemotiveerd verzoek van een andere bevoegde autoriteit, de andere bevoegde autoriteit wederzijdse bijstand verleent in verhouding tot haar eigen middelen, zodat de toezichts- of handhavingsmaatregelen op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd.

De in punt c) van de eerste alinea bedoelde wederzijdse bijstand kan betrekking hebben op verzoeken om informatie en toezichtsmaatregelen, met inbegrip van verzoeken om inspecties ter plaatse of toezicht elders of gerichte beveiligingsaudits uit te voeren. Een bevoegde autoriteit waaraan een verzoek om bijstand is gericht, mag dat verzoek niet weigeren, tenzij wordt vastgesteld dat zij niet bevoegd is om de gevraagde bijstand te verlenen, dat de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van de bevoegde autoriteit, of dat het verzoek betrekking heeft op informatie of activiteiten inhoudt die, indien ze openbaar zouden worden gemaakt of zouden worden uitgevoerd, in strijd zouden zijn met de wezenlijke belangen van zijn nationale veiligheid, de openbare veiligheid of de defensie van die lidstaat. Alvorens een dergelijk verzoek af te wijzen, raadpleegt de bevoegde autoriteit de andere betrokken bevoegde autoriteiten alsmede, op verzoek van een van de betrokken lidstaten, de Commissie en Enisa.

2. In voorkomend geval kunnen de bevoegde autoriteiten van verschillende lidstaten in onderlinge overeenstemming gezamenlijke toezichtsacties uitvoeren.

HOOFDSTUK VIII

GEDELEGEERDE HANDELINGEN EN UITVOERINGSHANDELINGEN

Artikel 38

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.

2. De in artikel 24, lid 2, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor een termijn van vijf jaar met ingang van 16 januari 2023.

3. Het Europees Parlement of de Raad kan de in artikel 24, lid 2, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel akkoord van 13 april 2016 over beter wetgeven.

5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.

6. Een op grond van artikel 24, lid 2, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van twee maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben meegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met twee maanden verlengd.

Artikel 39

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 van Verordening (EU) nr. 182/2011 van toepassing.

3. Wanneer het advies van het comité via een schriftelijke procedure moet worden verkregen, wordt deze procedure zonder gevolg beëindigd wanneer de voorzitter van het comité binnen de termijn voor het uitbrengen van het advies daartoe besluit of wanneer een lid van het comité daarom verzoekt.

HOOFDSTUK IX

SLOTBEPALINGEN

Artikel 40

Evaluatie

Uiterlijk op 17 oktober 2027 en vervolgens om de 36 maanden evalueert de Commissie de werking van deze richtlijn en brengt zij daarover verslag uit aan het Europees Parlement en aan de Raad. In het verslag wordt met name de relevantie van de omvang van de betrokken entiteiten, en de sectoren, subsectoren en types van de in de bijlagen I en II bedoelde entiteiten voor het functioneren van de economie en de samenleving met betrekking tot cyberbeveiliging beoordeeld. Daartoe en teneinde de strategische en operationele samenwerking verder te bevorderen, houdt de Commissie rekening met de verslagen van de samenwerkingsgroep en het CSIRT-netwerk over de opgedane ervaring op strategisch en operationeel niveau. Het verslag gaat zo nodig vergezeld van een wetgevingsvoorstel.

Artikel 41

Omzetting

1. Uiterlijk op 17 oktober 2024 gaan de lidstaten over tot de vaststelling en bekendmaking van de noodzakelijke bepalingen om aan deze richtlijn te voldoen. Zij stellen de Commissie daarvan onmiddellijk in kennis.

Zij passen die bepalingen toe met ingang van 18 oktober 2024.

2. Wanneer de lidstaten de in lid 1 bedoelde bepalingen vaststellen, wordt in de bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor de verwijzing worden vastgesteld door de lidstaten.

Artikel 42

Wijziging van Verordening (EU) nr. 910/2014

In Verordening (EU) nr. 910/2014 wordt artikel 19 geschrapt met ingang van 18 oktober 2024.

Artikel 43

Wijziging van Richtlijn (EU) 2018/1972

In Richtlijn (EU) 2018/1972 worden de artikelen 40 en 41 geschrapt met ingang van 18 oktober 2024.

Artikel 44

Intrekking

Richtlijn (EU) 2016/1148 wordt ingetrokken met ingang van 18 oktober 2024.

Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar de onderhavige richtlijn en worden gelezen volgens de concordantietabel in bijlage III.

Artikel 45

Inwerkingtreding

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

Artikel 46

Adressaten

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Straatsburg, 14 december 2022.

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*
R. METSOLA	M. BEK

BIJLAGE I

ZEER KRITIEKE SECTOREN

Sector	Subsector	Soort entiteit
1. Energie	a) Elektriciteit	— Elektriciteitsbedrijven zoals gedefinieerd in artikel 2, punt 57, van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad ([1]), die de functie verrichten van "levering" zoals gedefinieerd in artikel 2, punt 12, van die richtlijn
		— Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 29, van Richtlijn (EU) 2019/944
		— Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 35, van Richtlijn (EU) 2019/944
		— Producenten zoals gedefinieerd in artikel 2, punt 38, van Richtlijn (EU) 2019/944
		— Benoemde elektriciteitsmarktbeheerders zoals gedefinieerd in artikel 2, punt 8, van Verordening (EU) 2019/943 van het Europees Parlement en de Raad ([2]) — Marktdeelnemers zoals gedefinieerd in artikel 2, punt 25, van Verordening (EU) 2019/943 die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken zoals gedefinieerd in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944 — Exploitanten van een laadpunt die verantwoordelijk zijn voor het beheer en de exploitatie van een laadpunt dat een laaddienst levert aan eindgebruikers, onder meer namens en voor rekening van een aanbieder van mobiliteitsdiensten
	b) Stadsverwarming en -koeling	— Exploitanten van stadsverwarming of stadskoeling zoals gedefinieerd in artikel 2, punt 19, van Richtlijn (EU) 2018/2001van het Europees Parlement en de Raad ([3])
	c) Aardolie	— Exploitanten van oliepijpleidingen
		— Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport
		— Centrale entiteiten voor de voorraadvorming zoals gedefinieerd in artikel 2, punt f), van Richtlijn 2009/119/EG van de Raad ([4])
	d) Aardgas	— Leveringsbedrijven zoals gedefinieerd in artikel 2, punt 8, van Richtlijn 2009/73/EG van het Europees Parlement en de Raad ([5])
		— Distributiesysteembeheerders zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 2009/73/EG
		— Transmissiesysteembeheerders zoals gedefinieerd in artikel 2, punt 4, van Richtlijn 2009/73/EG
		— Opslagsysteembeheerders zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 2009/73/EG
		— LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG
		— Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG
		— Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
	e) Waterstof	— Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof

Sector	Subsector	Soort entiteit
2. Vervoer	a) Lucht	— Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) nr. 300/2008 die voor commerciële doeleinden worden gebruikt
		— Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad ([6]), luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad ([7]) zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden
		— Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad ([8]) aanbieden
	b) Spoor	— Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad ([9])
		— Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die richtlijn
	c) Water	— Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht, die in bijlage I bij Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad ([10]) als bedrijven in maritiem vervoer worden gedefinieerd, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen
		— Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2005/65/EG van het Europees Parlement en de Raad ([11]), inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004; alsook entiteiten die werken en uitrusting in havens beheren
		— Exploitanten van verkeersbegeleidingssystemen (VBS) zoals gedefinieerd in artikel 3, punt o), van Richtlijn 2002/59/EG van het Europees Parlement en de Raad ([12])
	d) Weg	— Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie ([13]) die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties waarvoor verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteit is
		— Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad ([14])
3. Bankwezen		Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ([15])
4. Infrastructuur voor de financiële markt		— Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad ([16])
		— Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad ([17])

Sector	Subsector	Soort entiteit
5. Gezondheidszorg		— Zorgaanbieders zoals gedefinieerd in artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad ([18])
		— EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad inzake ernstige grensoverschrijdende bedreigingen van de gezondheid ([19])
		— Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zoals gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG van het Europees Parlement en de Raad ([20]) — Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 vervaardigen — Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") in de zin van artikel 22 van Verordening (EU) 2022/123 van het Europees Parlement en de Raad ([21])
6. Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in artikel 2, punt 1, a), van Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad ([22]), met uitzondering van distributeurs waarvoor de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële of belangrijke diensten
7. Afvalwater		Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater zoals gedefinieerd in artikel 2, punten 1, 2 en 3, van Richtlijn 91/271/EEG van de Raad ([23]) opvangen, lozen of behandelen, met uitzondering van ondernemingen waarvoor het opvangen, lozen of behandelen van stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater een niet-essentieel onderdeel van hun algemene activiteit is
8. Digitale infrastructuur		— Aanbieders van internetknooppunten
		— DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers
		— Register voor topleveldomeinnamen
		— Aanbieders van cloudcomputingdiensten
		— Aanbieders van datacenterdiensten
		— Aanbieders van netwerken voor de levering van inhoud
		— Verleners van vertrouwensdiensten
		— Aanbieders van openbare elektronischecommunicatienetwerken
		— Aanbieders van openbare elektronischecommunicatiediensten
9. Beheer van ICT-diensten (business-to-business)		— Aanbieders van beheerde diensten — Aanbieders van beheerde beveiligingsdiensten

Sector	Subsector	Soort entiteit
10. Overheid		— Overheidsinstanties van centrale overheden zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht
		— Overheidsinstanties op regionaal niveau zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht
11. Ruimtevaart		Exploitanten van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronischecommunicatienetwerken

([1]) Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (PB L 158 van 14.6.2019, blz. 125).

([2]) Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit (PB L 158 van 14.6.2019, blz. 54).

([3]) Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad van 11 december 2018 ter bevordering van het gebruik van energie uit hernieuwbare bronnen (PB L 328 van 21.12.2018, blz. 82).

([4]) Richtlijn 2009/119/EG van de Raad van 14 september 2009 houdende verplichting voor de lidstaten om minimumvoorraden ruwe aardolie en/of aardolieproducten in opslag te houden (PB L 265 van 9.10.2009, blz. 9).

([5]) Richtlijn 2009/73/EG van het Europees Parlement en de Raad van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG (PB L 211 van 14.8.2009, blz. 94).

([6]) Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden (PB L 70 van 14.3.2009, blz. 11).

([7]) Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU (PB L 348 van 20.12.2013, blz. 1).

([8]) Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim (de kaderverordening) (PB L 96 van 31.3.2004, blz. 1).

([9]) Richtlijn 2012/34/EU van het Europees Parlement en de Raad van 21 november 2012 tot instelling van één Europese spoorwegruimte, (PB L 343 van 14.12.2012, blz. 32).

([10]) Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten (PB L 129 van 29.4.2004, blz. 6).

([11]) Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens (PB L 310 van 25.11.2005, blz. 28).

([12]) Richtlijn 2002/59/EG van het Europees Parlement en de Raad van 27 juni 2002 betreffende de invoering van een communautair monitoring en informatiesysteem voor de zeescheepvaart en tot intrekking van Richtlijn 93/75/EEG van de Raad (PB L 208 van 5.8.2002, blz. 10).

([13]) Gedelegeerde verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft (PB L 157 van 23.6.2015, blz. 21).

([14]) Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen (PB L 207 van 6.8.2010, blz. 1).

([15]) Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en tot wijziging van Verordening (EU) nr. 648/2012, PB L 176 van 27.6.2013, blz. 1.

([16]) Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).

([17]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).

([18]) Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PB L 88 van 4.4.2011, blz. 45).

([19]) Verordening (EU) 2022/2371 van het Europees Parlement en de Raad van 23 november 2022 inzake ernstige grensoverschrijdende bedreigingen van de gezondheid en houdende intrekking van Besluit nr. 1082/2013/EU (PB L 314 van 6.12.2022, blz. 26).

([20]) Richtlijn 2001/83/EG van het Europees Parlement en de Raad van 6 november 2001 tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik (PB L 311 van 28.11.2001, blz. 67).

([21]) Verordening (EU) 2022/123 van het Europees Parlement en de Raad van 25 januari 2022 betreffende een grotere rol van het Europees Geneesmiddelenbureau inzake crisisparaatheid en -beheersing op het gebied van geneesmiddelen en medische hulpmiddelen (PB L 20 van 31.1.2022, blz. 1).

([22]) Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water (PB L 435 van 23.12.2020, blz. 1).

([23]) Richtlijn 91/271/EEG van de Raad van 21 mei 1991 inzake de behandeling van stedelijk afvalwater (PB L 135 van 30.5.1991, blz. 40).

BIJLAGE II

ANDERE KRITIEKE SECTOREN

Sector	Subsector	Soort entiteit
1. Post- en koeriersdiensten		Aanbieders van postdiensten zoals gedefinieerd in artikel 2, punt 1 bis, van Richtlijn 97/67/EG, met inbegrip van aanbieders van koeriersdiensten
2. Afvalstoffenbeheer		Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren zoals gedefinieerd in artikel 3, punt 9, van Richtlijn 2008/98/EG van het Europees Parlement en de Raad ([1]), met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is
3. Vervaardiging, productie en distributie van chemische stoffen		Ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren als bedoeld in artikel 3, punten 9 en 14, van Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad ([2]) en ondernemingen die voorwerpen zoals gedefinieerd in artikel 3, punt 3, van die verordening produceren uit stoffen of mengsels
4. Productie, verwerking en distributie van levensmiddelen		Levensmiddelenbedrijven zoals gedefinieerd in artikel 3, punt 2, Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad ([3]) die zich bezighouden met groothandel en industriële productie en verwerking
5. Vervaardiging	a) Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek	Entiteiten die medische hulpmiddelen zoals gedefinieerd in artikel 2, punt 1, van Verordening (EU) 2017/745 van het Europees Parlement en de Raad ([4]) vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek zoals gedefinieerd in artikel 2, punt 2, van Verordening (EU) 2017/746 van het Europees Parlement en de Raad ([5]) vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, punt 5, vijfde streepje, van deze richtlijn
	b) Vervaardiging van informaticaproducten en van elektronische en optische producten	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 26, van NACE Rev. 2
	c) Vervaardiging van elektrische apparatuur	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 27, van NACE Rev. 2
	d) Vervaardiging van machines, apparaten en werktuigen, n.e.g.	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2
	e) Vervaardiging van motorvoertuigen, aanhangers en opleggers	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2
	f) Vervaardiging van andere transportmiddelen	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2

Sector	Subsector	Soort entiteit
6. Digitale aanbieders		— Aanbieders van onlinemarktplaatsen
		— Aanbieders van onlinezoekmachines
		— Aanbieders van platforms voor socialenetwerkdiensten
7. Onderzoek		Onderzoeksorganisaties

([1]) Richtlijn 2008/98/EG van het Europees Parlement en de Raad van 19 november 2008 betreffende afvalstoffen en tot intrekking van een aantal richtlijnen (PB L 312 van 22.11.2008, blz. 3).

([2]) Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad van 18 december 2006 inzake de registratie en beoordeling van en de autorisatie en beperkingen ten aanzien van chemische stoffen (REACH), tot oprichting van een Europees Agentschap voor chemische stoffen, houdende wijziging van Richtlijn 1999/45/EG en houdende intrekking van Verordening (EEG) nr. 793/93 van de Raad en Verordening (EG) nr. 1488/94 van de Commissie alsmede Richtlijn 76/769/EEG van de Raad en de Richtlijnen 91/155/EEG, 93/67/EEG, 93/105/EG en 2000/21/EG van de Commissie (PB L 396 van 30.12.2006, blz. 1).

([3]) Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad van 28 januari 2002 tot vaststelling van de algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tot vaststelling van procedures voor voedselveiligheidsaangelegenheden (PB L 31 van 1.2.2002, blz. 1).

([4]) Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (PB L 117 van 5.5.2017, blz. 1).

([5]) Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176).

BIJLAGE III

CONCORDANTIETABEL

Richtlijn (EU) 2016/1148	Deze richtlijn
Artikel 1, lid 1	Artikel 1, lid 1
Artikel 1, lid 2	Artikel 1, lid 2
Artikel 1, lid 3	—
Artikel 1, lid 4	Artikel 2, lid 12
Artikel 1, lid 5	Artikel 2, lid 13
Artikel 1, lid 6	Artikel 2, leden 6 en 11
Artikel 1, lid 7	Artikel 4
Artikel 2	Artikel 2, lid 14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	—
Artikel 6	—
Artikel 7, lid 1	Artikel 7, leden 1 en 2
Artikel 7, lid 2	Artikel 7, lid 4
Artikel 7, lid 3	Artikel 7, lid 3
Artikel 8, leden 1 tot en met 5	Artikel 8, leden 1 tot en met 5
Artikel 8, lid 6	Artikel 13, lid 4
Artikel 8, lid 7	Artikel 8, lid 6
Artikel 9, leden 1, 2 en 3	Artikel 10, leden 1, 2 en 3
Artikel 9, lid 4	Artikel 10, lid 9
Artikel 9, lid 5	Artikel 10, lid 10
Artikel 10, lid 1, lid 2 en lid 3, eerste alinea	Artikel 13, leden 1, 2 en 3
Artikel 10, lid 3, tweede alinea	Artikel 23, lid 9
Artikel 11, lid 1	Artikel 14, leden 1 en 2
Artikel 11, lid 2	Artikel 14, lid 3
Artikel 11, lid 3	Artikel 14, lid 4, eerste alinea, punten a) tot en met q) en s), en lid 7
Artikel 11, lid 4	Artikel 14, lid 4, eerste alinea, punt r), en tweede alinea
Artikel 11, lid 5	Artikel 14, lid 8
Artikel 12, leden 1 tot en met 5	Artikel 15, leden 1 tot en met 5
Artikel 13	Artikel 17
Artikel 14, leden 1 en 2	Artikel 21, leden 1 tot en met 4
Artikel 14, lid 3	Artikel 23, lid 1
Artikel 14, lid 4	Artikel 23, lid 3
Artikel 14, lid 5	Artikel 23, leden 5, 6 en 8

Richtlijn (EU) 2016/1148	Deze richtlijn
Artikel 14, lid 6	Artikel 23, lid 7
Artikel 14, lid 7	Artikel 23, lid 11
Artikel 15, lid 1	Artikel 31, lid 1
Artikel 15, lid 2, eerste alinea, punt a)	Artikel 32, lid 2, punt e)
Artikel 15, lid 2, eerste alinea, punt b)	Artikel 32, lid 2, punt g)
Artikel 15, lid 2, tweede alinea	Artikel 32, lid 3
Artikel 15, lid 3	Artikel 32, lid 4, punt b)
Artikel 15, lid 4	Artikel 31, lid 3
Artikel 16, leden 1 en 2	Artikel 21, leden 1 tot en met 4
Artikel 16, lid 3	Artikel 23, lid 1
Artikel 16, lid 4	Artikel 23, lid 3
Artikel 16, lid 5	—
Artikel 16, lid 6	Artikel 23, lid 6
Artikel 16, lid 7	Artikel 23, lid 7
Artikel 16, leden 8 en 9	Artikel 21, lid 5, en artikel 23, lid 11
Artikel 16, lid 10	—
Artikel 16, lid 11	Artikel 2, leden 1, 2 en 3
Artikel 17, lid 1	Artikel 33, lid 1
Artikel 17, lid 2, punt a)	Artikel 32, lid 2, punt e)
Artikel 17, lid 2, punt b)	Artikel 32, lid 4, punt b)
Artikel 17, lid 3	Artikel 37, lid 1, punten a) en b)
Artikel 18, lid 1	Artikel 26, lid 1, punt b), en lid 2
Artikel 18, lid 2	Artikel 26, lid 3
Artikel 18, lid 3	Artikel 26, lid 4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	—
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Bijlage I, punt 1	Artikel 11, lid 1
Bijlage I, punt 2, punt a), i)-iv)	Artikel 11, lid 2, punten a) tot en met d)

Richtlijn (EU) 2016/1148	Deze richtlijn
Bijlage I, punt 2, punt a), v)	Artikel 11, lid 2, punt f)
Bijlage I, punt 2, punt b)	Artikel 11, lid 4
Bijlage I, punt 2, punt c), i)-ii)	Artikel 11, lid 5, punt a)
Bijlage II	Bijlage I
Bijlage III, punten 1 en 2	Bijlage II, punt 6
Bijlage III, punt 3	Bijlage I, punt 8