Raad van de
Europese Unie

Brussel, 26 november 2021
(OR. en)

14337/21

Interinstitutioneel dossier:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOTA

van:	het secretariaat-generaal van de Raad
aan:	Raad
nr. vorig doc.:	9583/2/21, 11724/21
nr. Comdoc.:	14150/20
Betreft:	Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 - *Algemene oriëntatie*

I. INLEIDING

1. De Commissie heeft op 16 december 2020 een voorstel aangenomen voor een richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie ("de herziene NIS-richtlijn" of "NIS 2")[1], ter vervanging van de huidige richtlijn inzake de beveiliging van netwerk- en informatiesystemen ("de NIS-richtlijn")[2].

[1] Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

[2] 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.

Het voorstel was een van de maatregelen uit de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[3] om ervoor te zorgen dat burgers en bedrijven kunnen profiteren van betrouwbare digitale technologieën.

2. Het voorstel is gebaseerd op artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU) en is erop gericht de veerkracht en de responscapaciteit bij incidenten van publieke en private entiteiten, bevoegde autoriteiten en de Unie als geheel verder te verbeteren.

3. In het Europees Parlement is de voor het voorstel bevoegde commissie de Commissie industrie, onderzoek en energie (ITRE). De Commissie ITRE heeft het verslag van de rapporteur op 28 oktober 2021 goedgekeurd.

4. Het Europees Economisch en Sociaal Comité heeft op 28 april 2021 zijn advies goedgekeurd.

5. Op 3 februari 2021 besloot het Comité van permanente vertegenwoordigers het Europees Comité van de Regio's te raadplegen over het voorstel[4]. Tot dusver heeft het Europees Comité van de Regio's nog geen advies uitgebracht.

6. De Europese Toezichthouder voor gegevensbescherming heeft op 11 maart 2021 advies uitgebracht[5].

7. In zijn conclusies[6] van 22 maart 2021 over de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk nam de Raad nota van het nieuwe voorstel dat voortbouwt op de NIS-richtlijn, en herhaalde zijn steun voor sterkere en geharmoniseerde nationale cyber-beveiligingskaders en voor duurzame samenwerking tussen de lidstaten.

8. In zijn conclusies van 21-22 oktober 2021 riep de Europese Raad op om de werkzaamheden met betrekking tot het voorstel voor een herziene NIS-richtlijn voort te zetten.

---

3 Doc. 14133/20.
4 Doc. 5573/21.
5 "Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive".
6 Doc. 6722/21.

II. WERKZAAMHEDEN IN DE VOORBEREIDENDE INSTANTIES VAN DE RAAD

9. Binnen de Raad is het voorstel besproken in de Horizontale Groep cybervraagstukken (hierna "HWPCI" genoemd). De bespreking van het voorstel begon op 19 januari tijdens het Portugese voorzitterschap met een zorgvuldige lezing, zodat de lidstaten hun vragen konden formuleren en hun voornaamste bezwaren kenbaar konden maken, en ze gedetailleerde uitleg konden krijgen van de Commissie over de wijzigingen in de herziene richtlijn.

10. Onder het Portugese voorzitterschap wijdde de HWPCI 17 vergaderingen aan de presentatie en lezing van het voorstel. Op 4 juni 2021 is aan de Raad TTE een voortgangsverslag over de lezing voorgelegd.

11. Het werk is sindsdien tijdens het Sloveense voorzitterschap voortgezet en geïntensiveerd, met als doel in de zitting van de Raad (Vervoer, Telecommunicatie en Energie) op 3 december 2021 tot een algemene oriëntatie te komen. Het Sloveense voorzitterschap heeft 15 vergaderingen gewijd aan de herziening van het NIS 2-voorstel, evenals vele bilaterale besprekingen op alle niveaus.

12. De HWPCI heeft haar werkzaamheden toegespitst op de herformulering van de tekst van het voorstel, in eerste instantie wat betreft de interactie van de NIS 2-richtlijn met sectorale wetgeving en toepassingsgebied, met name inzake openbare besturen, DNS-rootservers en de uitsluitingsclausule en daarna onder andere wat betreft collegiale toetsingen, jurisdictie en wederzijdse bijstand, gecoördineerde bekendmaking van kwetsbaarheden, databanken van domeinnamen en registratiegegevens en internationale samenwerking.

13. Een eerste compromisvoorstel over de tekst van de voorgestelde richtlijn, op basis van de schriftelijke opmerkingen en non-papers van de lidstaten, en van de eerdere compromis-voorstellen over de interactie van de NIS 2-richtlijn met sectorale wetgeving en over het toepassingsgebied van de NIS 2-richtlijn, is op 21 september 2021 uitgebracht[7].

[7] Doc. 12019/21.

14. De meest recente herziening[8] van het compromisvoorstel van het voorzitterschap is op 22 november 2021 in de werkgroep besproken. Hoewel de delegaties over het algemeen ingenomen waren met de compromistekst, hadden enkele nog steeds een studievoorbehoud of maakten opmerkingen bij delen van het compromisvoorstel. In bepaalde delen van de tekst werd nog een aantal technische wijzigingen voorgesteld.

III. INHOUDELIJK

15. Op basis van de besprekingen in de groep zijn de volgende punten als de belangrijkste politieke kwesties aangemerkt:

a) Toepassingsgebied (artikel 2)

Sinds het begin van de besprekingen over het NIS 2-voorstel was de belangrijkste zorg van de lidstaten de aanzienlijke toename van het aantal onder de richtlijn vallende entiteiten, en met name de invoering van de "size-cap"-regel, namelijk dat alle middelgrote en grote entiteiten die in de sectoren actief zijn of diensten verlenen die onder de NIS 2-richtlijn vallen, onder het toepassingsgebied van die richtlijn vallen. Hoewel het compromisvoorstel deze algemene regel handhaaft, bevat het aanvullende bepalingen om te zorgen voor de noodzakelijke evenredigheid, een hoger niveau van risicobeheer en duidelijke kriticiteits-criteria om te bepalen welke entiteiten onder het toepassingsgebied van de richtlijn vallen. Daarnaast bevat het compromisvoorstel specifieke bepalingen over de prioritering van het gebruik van toezichtsmaatregelen volgens een risicogebaseerde benadering.

[8] Doc. 12019/5/21 REV 5.

b) Openbaar bestuur (artikel 2, lid 2a))

De opname van openbare besturen in het toepassingsgebied van de NIS 2-richtlijn was een zeer omstreden onderwerp, aangezien de overheidssector specifieker is dan andere sectoren die onder de NIS 2-richtlijn vallen. Het voorzitterschap heeft gestreefd naar een evenwichtige aanpak waarbij rekening wordt gehouden met de specifieke kenmerken van de nationale kaders voor openbare besturen en ervoor wordt gezorgd dat de lidstaten over een zekere mate van flexibiliteit beschikken bij het bepalen van de overheidsinstanties die onder het toepassingsgebied van NIS 2 vallen. Daarom is, in de compromistekst, NIS 2 van toepassing op overheidsinstanties van centrale overheden, terwijl de lidstaten ook kunnen bepalen dat de richtlijn van toepassing is op overheidsinstanties op regionaal en lokaal niveau.

c) De uitsluitingsclausule (artikel 2, punten 3a) en 3aa))

De lidstaten wensten de uitsluitingsclausule verder te verduidelijken in die zin dat de richtlijn niet van toepassing is op entiteiten die hoofdzakelijk activiteiten verrichten op het gebied van defensie, nationale veiligheid, openbare veiligheid of rechtshandhaving, noch op activiteiten die betrekking hebben op de nationale veiligheid of defensie. Ook de rechterlijke macht, parlementen en centrale banken zijn uitgesloten.

d) Interactie met sectorale wetgeving

De lidstaten benadrukten dat de NIS 2-richtlijn moet worden afgestemd op sectorale wetgeving, met name de verordening betreffende digitale operationele veerkracht voor de financiële sector ("de DORA-verordening") en de richtlijn betreffende de veerkracht van kritieke entiteiten ("de CER-richtlijn"). De NIS 2-richtlijn, die de basis moet vormen voor minimale harmonisatie op het gebied van cyberbeveiliging, bevat een specifiek artikel over sectorspecifieke handelingen van de Unie (artikel 2 ter). Wat de interactie met de CER-richtlijn betreft, zorgt het compromisvoorstel voor meer duidelijkheid over de "alle risico's"-benadering. Andere belangrijke aanvullingen houden verband met samenwerkingsregelingen tussen de bevoegde autoriteiten in het kader van de respectieve rechtshandelingen.

e) Intercollegiaal leren (artikel 16)

Op enkele uitzonderingen na waren de lidstaten gekant tegen de verplichte collegiale toetsingen die de Commissie wil invoeren. Het voorgestelde compromis zorgt ervoor dat het nieuwe mechanisme voor intercollegiaal leren voortbouwt op wederzijds vertrouwen, en een vrijwillig en door de lidstaten gestuurd proces is.

f) Jurisdictie en territorialiteit (artikel 24) en wederzijdse bijstand (artikel 34)

De lidstaten hebben hun bezorgdheid geuit over de gevolgen van een gedifferentieerde jurisdictie voor entiteiten in de ICT-sector, zoals voorgesteld door de Commissie. De compromistekst heeft jurisdictie op basis van het soort entiteiten verduidelijkt en de formulering inzake wederzijdse bijstand aangescherpt.

g) Rapportageverplichtingen (artikel 20)

Inspelend op het bezwaar van de lidstaten dat dit de onder de NIS 2-richtlijn vallende entiteiten zal overbelasten en tot overrapportering zal leiden, is de verplichte melding voor significante cyberbedreigingen niet in de compromistekst opgenomen.

IV. CONCLUSIE

16. Het Comité van permanente vertegenwoordigers heeft op 24 november 2021 overeenstemming bereikt over de compromistekst in de bijlage en besloten deze voor te leggen aan de Raad (Vervoer, Telecommunicatie en Energie) met het oog op de vaststelling van een algemene oriëntatie.

17. De Raad wordt derhalve verzocht de compromistekst van het voorzitterschap in de bijlage goed te keuren en in zijn zitting op 3 december 2021 een algemene oriëntatie vast te stellen.

BIJLAGE

Voorstel voor een

RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD

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

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

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

Gezien het voorstel van de Europese Commissie,

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

Gezien het advies van het Europees Economisch en Sociaal Comité[9],

Gezien het advies van het Comité van de Regio's[10],

Handelend volgens de gewone wetgevingsprocedure,

[9] PB C , , blz. .
[10] PB C , , blz. .

Overwegende hetgeen volgt:

(1) Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad[11] 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 cyberbeveiligings-incidenten, en aldus bij te dragen tot een doeltreffende werking van de economie en de samenleving van de Unie.

(2) Sinds de inwerkingtreding van Richtlijn (EU) 2016/1148 is er aanzienlijke vooruitgang geboekt bij het vergroten van de veerkracht van de Unie op het gebied van cyberbeveiliging. 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 het sluitstuk van de nationale kaders, door nationale [...] strategieën **voor beveiliging van netwerk- en informatiesystemen** te definiëren, nationale capaciteiten vast te stellen en regelgevende maatregelen uit te voeren die betrekking hebben op essentiële infrastructuren en actoren die elke lidstaat heeft bepaald. Zij heeft ook bijgedragen aan de samenwerking op het niveau van de Unie door de oprichting van de Samenwerkingsgroep[12] en **het** [...] netwerk van nationale computer security incident response teams ("CSIRT-netwerk")[13]. Ondanks deze resultaten heeft de herziening van Richtlijn (EU) 2016/1148 inherente tekortkomingen aan het licht gebracht die verhinderen dat met deze richtlijn de hedendaagse en opkomende uitdagingen op het gebied van cyber-beveiliging effectief worden aangepakt.

---

11 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 194/1 van 19.7.2016, blz. 1).

12 Artikel 11 van Richtlijn (EU) 2016/1148.

13 Artikel 12 van Richtlijn (EU) 2016/1148.

(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 bedreigingslandschap voor de cyberbeveiliging, wat nieuwe uitdagingen met zich meebrengt, die in alle lidstaten een aangepaste, gecoördineerde en innovatieve respons vereist. Het aantal, de omvang, de complexiteit, de frequentie en de impact van cyberbeveiligingsincidenten nemen toe en vormen een grote bedreiging voor het functioneren van netwerk- en informatiesystemen. Daardoor kunnen cyberincidenten de uitoefening van economische activiteiten in de interne markt belemmeren, financiële verliezen 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.

(4) De rechtsgrondslag voor Richtlijn (EU) 1148/2016 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 relevante activiteiten verrichten, verschillen aanzienlijk van lidstaat tot lidstaat wat betreft het soort eis, de mate van gedetailleerdheid en de wijze van toezicht. Deze verschillen brengen extra kosten met zich mee en leveren problemen op voor ondernemingen die goederen of diensten grensoverschrijdend aanbieden. De eisen die door de ene lidstaat worden gesteld en die verschillen van of zelfs in strijd zijn met de eisen die door een andere lidstaat worden gesteld, kunnen een aanzienlijke invloed hebben op deze grensoverschrijdende activiteiten.

Bovendien zal de mogelijkheid van een suboptimaal ontwerp of een suboptimale uitvoering van cyberbeveiligings**maatregelen** [...] in een lidstaat waarschijnlijk gevolgen hebben voor het niveau van de cyberbeveiliging in andere lidstaten, met name gezien de intensieve grensoverschrijdende uitwisselingen. Bij de herziening 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 opgenomen verplichtingen inzake beveiliging en incidentenmelding. Deze verplichtingen zijn dan ook op nationaal niveau op sterk uiteenlopende wijze uitgevoerd. Soortgelijke verschillen in de uitvoering hebben zich voorgedaan met betrekking tot de bepalingen van die richtlijn 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, met gevolgen voor met name de grensoverschrijdende dienstverlening, en op de veerkracht van cyberbeveiliging als gevolg van de toepassing van verschillende [...] **maatregelen**. 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 cyberbeveiligingverplichtingen gelden bij te werken en door te voorzien in doeltreffende rechtsmiddelen en sancties die bijdragen tot een doeltreffende handhaving van deze verplichtingen. Daarom moet Richtlijn (EU) 2016/1148 worden ingetrokken en door deze richtlijn worden vervangen.

(6) [...] De lidstaten moeten de nodige maatregelen **kunnen nemen** om de bescherming van de wezenlijke belangen van hun veiligheid te waarborgen, de openbare orde en de openbare veiligheid te garanderen, en het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken[...]. [...]**De richtlijn mag niet van toepassing zijn op bepaalde publieke of private entiteiten die activiteiten op deze gebieden uitoefenen. De richtlijn mag evenmin van toepassing zijn op de activiteiten van entiteiten die op deze gebieden actief zijn. Voorts** is geen enkele lidstaat verplicht inlichtingen te verstrekken waarvan de verbreiding in strijd zou zijn met de wezenlijke belangen van zijn openbare veiligheid. [...]**N**ationale [...] **of** uniale regels voor de bescherming van gerubriceerde informatie, geheimhoudingsovereenkomsten en informele geheimhoudingsovereenkomsten, zoals het verkeerslichtprotocol[14], zijn van belang.

(6a) Het recht van de Unie inzake de bescherming van persoonsgegevens en de persoonlijke levenssfeer is van toepassing op elke verwerking van persoonsgegevens in het kader van deze richtlijn. Deze richtlijn doet met name geen afbreuk aan Verordening (EU) 2016/679 en Richtlijn 2002/58/EG van het Europees Parlement en de Raad en mag derhalve vooral geen invloed hebben op de taken en bevoegdheden van de onafhankelijke toezichthoudende autoriteiten die bevoegd zijn om toe te zien op de naleving van de respectieve Uniewetgeving inzake gegevensbescherming.

---

14 Het verkeerslichtprotocol ("Traffic Light Protocol" – TLP) is een middel voor iemand die informatie deelt om zijn publiek te informeren over eventuele beperkingen bij de verdere verspreiding van deze informatie. Het wordt gebruikt in bijna alle CSIRT-gemeenschappen en in sommige centra voor informatie-uitwisseling en -analyse (Information Analysis and Sharing Centres – ISAC's).

(7) Met de intrekking van Richtlijn (EU) 2016/1148 moet het toepassingsgebied per sector worden uitgebreid tot een groter deel van de economie in het licht van de overwegingen (4) tot en met (6). De sectoren die onder Richtlijn (EU) 2016/1148 vallen, moeten daarom worden uitgebreid om de sectoren en diensten die van vitaal belang zijn voor belangrijke maatschappelijke en economische activiteiten binnen de interne markt, volledig te bestrijken. De regels mogen niet verschillen naargelang het gaat om aanbieders van essentiële diensten of digitaledienstverleners. Dat onderscheid is achterhaald gebleken, aangezien het niet het werkelijke belang van de sectoren of diensten voor de maatschappelijke en economische activiteiten in de interne markt weerspiegelt.

(8) Overeenkomstig Richtlijn (EU) 2016/1148 waren de lidstaten verantwoordelijk voor het bepalen welke entiteiten voldoen aan de criteria om als aanbieders van essentiële diensten te worden aangemerkt ("identificatieproces"). Om de grote verschillen tussen de lidstaten in dat opzicht weg te werken en rechtszekerheid te bieden voor de vereisten inzake risicobeheer en de rapportageverplichtingen voor alle betrokken 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 de "size-cap"-regel, waarbij alle middelgrote en grote ondernemingen, zoals gedefinieerd in Aanbeveling 2003/361/EG van de Commissie[15], die actief zijn in de sectoren of het soort diensten verrichten die onder deze richtlijn vallen, binnen de werkingssfeer van de richtlijn vallen.
[...]

[15] 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).

(8a) Om een duidelijk overzicht te krijgen van de entiteiten die onder het toepassingsgebied van deze richtlijn vallen, moeten de lidstaten nationale mechanismen voor zelfmelding kunnen instellen op grond waarvan onder deze richtlijn vallende entiteiten, ten minste hun naam, adres en contactgegevens, de sector waarin zij actief zijn of het soort dienst dat zij verlenen, en, indien van toepassing, een lijst van de lidstaten waar zij onder deze richtlijn vallende diensten verlenen, moeten opgeven aan de autoriteiten die uit hoofde van deze richtlijn bevoegd autoriteiten of de instanties die daartoe door de lidstaten zijn aangewezen. Waar reeds registers op nationaal niveau bestaan, kunnen de lidstaten beslissen welk passend mechanisme te gebruiken voor de identificatie van entiteiten die binnen het toepassingsgebied van deze richtlijn vallen.

(9) [...] **Kleine of** micro-entiteiten [...] die voldoen aan bepaalde criteria die wijzen op een sleutelrol voor de economieën of samenlevingen van de lidstaten of voor bepaalde sectoren of soorten diensten, moeten echter ook onder deze richtlijn vallen. De lidstaten [...] moeten ervoor verantwoordelijk zijn dat aan de Commissie [...] **ten minste relevante informatie wordt verstrekt over het aantal aangemerkte entiteiten, de sector waartoe zij behoren of het soort dienst dat zij verlenen, en de specifieke criteria op basis waarvan zij zijn geïdentificeerd. De lidstaten kunnen ook besluiten om, indien dit in overeenstemming is met de nationale veiligheidsvoorschriften, de namen van deze entiteiten bij de Commissie te melden.**

(9a) Overheidsinstanties die activiteiten verrichten op het gebied van nationale veiligheid, defensie, openbare veiligheid, rechtshandhaving, alsook de rechterlijke macht, parlementen en centrale banken, vallen niet binnen het toepassingsgebied van deze richtlijn. Voor de toepassing van deze richtlijn worden entiteiten met regelgevende bevoegdheid niet geacht activiteiten op het gebied van rechtshandhaving te verrichten en zijn zij derhalve niet op deze gronden uitgesloten van het toepassingsgebied van deze richtlijn. Daarnaast vallen overheidsinstanties van de centrale overheid die overeenkomstig een internationale overeenkomst samen met een derde land zijn opgericht, niet binnen het toepassingsgebied van deze richtlijn.

(9aa) De lidstaten moeten kunnen vaststellen dat entiteiten die vóór de inwerkingtreding van deze richtlijn als aanbieders van essentiële diensten in overeenstemming met Richtlijn (EU) 2016/1148 zijn aangemerkt, als essentiële entiteiten moeten worden beschouwd.

(9aaa) Deze richtlijn is niet van toepassing op diplomatieke en consulaire missies van de lidstaten in het buitenland en op de ICT-infrastructuur die deze missies gebruiken, voor zover deze infrastructuur zich in het buitenland bevindt of voor gebruikers in het buitenland wordt gebruikt.

(10) De Commissie kan, in samenwerking met de Samenwerkingsgroep, richtsnoeren opstellen voor de toepassing van de criteria die van toepassing zijn op micro- en kleine ondernemingen.

(11) [...] **Entiteiten die binnen het toepassingsgebied van deze richtlijn vallen, moeten in twee categorieën worden ingedeeld: essentiële en belangrijke entiteiten, die rekening houden met de mate van kriticiteit van de sector of van het soort diensten dat zij verlenen, en met de omvang ervan. In dit verband moet, indien van toepassing, ook terdege rekening worden gehouden met relevante sectorale risicobeoordelingen of richtsnoeren van bevoegde autoriteiten.** Zowel essentiële als belangrijke entiteiten moeten voldoen aan de vereisten inzake risicobeheer en de rapportageverplichtingen. De toezichts- en sanctieregelingen tussen deze twee categorieën entiteiten moeten worden gedifferentieerd om te zorgen voor een billijk evenwicht tussen **risicogebaseerde** eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds.

(12) **Deze richtlijn stelt de minimumvereisten vast voor maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen voor alle sectoren die binnen het toepassingsgebied ervan vallen. Om versnippering van de cyberbeveiligingsbepalingen van rechtshandelingen van de Unie te voorkomen, moet de Commissie, wanneer aanvullende sectorspecifieke bepalingen met betrekking tot** maatregelen voor het beheer van cyberbeveiligingsrisico's en rapportageverplichtingen **noodzakelijk worden geacht om een hoog niveau van cyberbeveiliging te waarborgen, beoordelen of dergelijke bepalingen kunnen worden opgenomen in een uitvoeringshandeling in het kader van de bevoegdheidsdelegatiewaarin deze richtlijn voorziet. Indien dergelijke handelingen niet geschikt zijn voor dat doel, kan** sectorspecifieke wetgeving bijdragen tot het waarborgen van **een** hoog niveau [...] van cyberbeveiliging, waarbij ten volle rekening wordt gehouden met de specifieke kenmerken en complexiteit van [...] **de betrokken** sectoren. **De redenen waarom een uitvoeringshandeling in het kader van de bevoegdheidsdelegatie waarin deze richtlijn voorziet niet passend was, moeten worden toegelicht in de sectorspecifieke wetgeving. Tegelijkertijd moet in dergelijke sectorspecifieke bepalingen van rechtshandelingen van de Unie terdege rekening worden gehouden met de behoefte aan een alomvattend en geharmoniseerd kader voor cyberbeveiliging.** [...] Dit [...] laat de bestaande uitvoeringsbevoegdheden die [...] **aan** de Commissie zijn verleend in een aantal sectoren, waaronder vervoer en energie, onverlet.

(12a) Wanneer een sectorspecifieke rechtshandeling van de Unie **bepalingen bevat** die [...] vereis**en** dat essentiële of belangrijke entiteiten **maatregelen nemen die ten minste van gelijke werking zijn als de in deze richtlijn vastgestelde verplichtingen** inzake risicobeheer [...] op het gebied van cyberbeveiliging **en verplichtingen** om **significante** incidenten of significante cyberbedreigingen te melden [...], moeten die sectorspecifieke bepalingen**, onder meer inzake toezicht en handhaving,** van toepassing zijn. **Bij het bepalen van de gelijke werking van verplichtingen in de sectorspecifieke bepalingen van een rechtshandeling van de Unie moeten de volgende aspecten in aanmerking worden genomen: i) de maatregelen voor het beheer van cyberbeveiligingsrisico's moeten bestaan uit passende en evenredige technische en organisatorische maatregelen om de risico's te beheersen voor de beveiliging van netwerk- en informatiesystemen die de betrokken entiteiten bij hun dienstverlening gebruiken, en moeten ten minste alle in deze richtlijn vastgestelde elementen omvatten; ii) de verplichting om significante incidenten en cyberbedreigingen te melden moet ten minste gelijkwaardig zijn aan de verplichtingen van deze richtlijn met betrekking tot de inhoud, de vorm en de termijnen van de kennisgevingen; iii) de wijze waarop entiteiten en de betrokken autoriteiten van sectorspecifieke rechtshandelingen van de Unie rapporteren, moet ten minste gelijkwaardig zijn aan de vereisten van deze richtlijn wat betreft inhoud, formaat en termijnen, en moet rekening houden met de rol van de CSIRT's; iv) de vereisten voor grensoverschrijdende samenwerking voor de betrokken autoriteiten moeten ten minste gelijkwaardig zijn aan die van deze richtlijn. Indien de sectorspecifieke bepalingen van een rechtshandeling van de Unie niet geldt voor alle entiteiten in een specifieke sector die binnen het toepassingsgebied van deze richtlijn valt, moeten de desbetreffende bepalingen van deze richtlijn van toepassing blijven op entiteiten die niet onder die sectorspecifieke bepalingen vallen.**

(12aa) De Commissie **moet de toepassing van het vereiste van gelijke werking met betrekking tot sectorspecifieke bepalingen van rechtshandelingen van de Unie periodiek evalueren,** waarbij [...]. **De Commissie moet de Samenwerkingsgroep raadplegen bij de voorbereiding van de periodieke evaluatie**.

(12aaa) In toekomstige sectorspecifieke rechtshandelingen van de Unie moet terdege rekening worden gehouden met de definities in artikel 4 van deze richtlijn en met het in hoofdstuk VI van deze richtlijn vastgestelde toezichts- en handhavingskader.

(12ab) Wanneer krachtens sectorspecifieke bepalingen van rechtshandelingen van de Unie essentiële of belangrijke entiteiten maatregelen moeten vaststellen die ten minste van gelijke werking zijn als de in deze richtlijn vastgestelde rapportageverplichtingen, moeten overlappingen inzake die verplichting worden vermeden en moet worden gezorgd voor samenhang en doeltreffendheid bij de behandeling van meldingen van cyberbedreigingen of -incidenten. Daartoe kunnen die sectorspecifieke bepalingen de lidstaten in staat stellen een gemeenschappelijk, automatisch en rechtstreeks meldingsechanisme in te stellen voor het melden van significante incidenten en cyberbedreigingen aan zowel de autoriteiten waarvan de taken zijn vastgelegd in de respectieve sectorspecifieke bepalingen als de bevoegde autoriteiten, met inbegrip van het centrale contactpunt en, in voorkomend geval, CSIRT's, die verantwoordelijk zijn voor de cyberbeveiligingstaken waarin deze richtlijn voorziet, of dat ervoor zorgt dat systematisch en onmiddellijk informatie wordt gedeeld en samengewerkt wordt tussen de betrokken autoriteiten en CSIRT's bij de behandeling van dergelijke kennisgevingen. Ter vereenvoudiging van de rapportage en de uitvoering van het gemeenschappelijke, automatische en directe meldingsmechanisme kunnen de lidstaten, in overeenstemming met sectorspecifieke wetgeving, gebruikmaken van het centrale toegangspunt dat zij overeenkomstig artikel 11, lid 5a, van deze richtlijn instellen. Met het oog op harmonisatie moeten de rapportageverplichtingen die zijn vastgesteld in sectorspecifieke rechtshandelingen van de Unie, worden afgestemd op die van deze richtlijn. De lidstaten kunnen bepalen dat de krachtens deze richtlijn bevoegde autoriteiten of de nationale CSIRT's de adressaten van de melding zijn, in overeenstemming met sectorspecifieke wetgeving.

(13) Verordening XXXX/XXXX van het Europees Parlement en de Raad moet worden beschouwd als een sectorspecifieke rechtshandeling van de Unie met betrekking tot deze richtlijn voor wat betreft de entiteiten in de financiële sector. De bepalingen van Verordening XXXX/XXXX betreffende maatregelen voor het risicobeheer op het gebied van informatie- en communicatietechnologie (ICT), het beheer van ICT-gerelateerde incidenten en met name de rapportage van incidenten, alsmede betreffende digitale operationele veerkrachttests, regelingen voor het delen van informatie en risico's van derden op het gebied van ICT, moeten van toepassing zijn in plaats van de bepalingen die **in** [...] deze richtlijn zijn vastgesteld. De lidstaten mogen de bepalingen van deze richtlijn betreffende risicobeheer [...] op het gebied van cyberbeveiliging en de rapportageverplichtingen, en toezicht en handhaving dan ook niet toepassen op [...] financiële entiteiten die onder Verordening XXXX/XXXX vallen. Tegelijkertijd is het van belang een sterke relatie en de uitwisseling van informatie met de financiële sector in het kader van deze richtlijn in stand te houden. Daartoe biedt Verordening XXXX/XXXX [...] de Europese toezichthoudende autoriteiten (ETA's) voor de financiële sector en de nationale bevoegde autoriteiten op grond van Verordening XXXX/XXXX[...], de mogelijkheid deel te nemen aan **de** [...] **werkzaamheden** [...] van de Samenwerkingsgroep en informatie uit te wisselen en samen te werken met de op grond van deze richtlijn aangewezen centrale contactpunten**,** [...] **evenals** met de nationale CSIRT's. De bevoegde autoriteiten uit hoofde van Verordening XXXX/XXXX moeten de details van grote ICT-gerelateerde incidenten **en significante cyberbedreigingen** ook doorgeven aan de in het kader van deze richtlijn aangewezen centrale contactpunten, **de bevoegde autoriteiten** of **de nationale CSIRT's**. **Dit kan door het automatisch en rechtstreeks doorsturen van incidentenmeldingen of via een gemeenschappelijk rapporteringsplatform.** Bovendien moeten de lidstaten de financiële sector blijven opnemen in hun cyberbeveiligingsstrategieën en **kunnen** [...] de nationale CSIRT's de financiële sector bij hun activiteiten betrekken.

(13a) Om lacunes in en overlappingen van de in punt 2a), van bijlage I bedoelde cyberbeveiligingsverplichtingen voor entiteiten in de luchtvaartsector te vermijden, moeten de krachtens de Verordeningen (EG) nr. 300/2008[16] en (EU) 2018/1139[17] van het Europees Parlement en de Raad aangewezen nationale autoriteiten en de bevoegde autoriteiten uit hoofde van deze richtlijn samenwerken bij de uitvoering van risicobeheersmaatregelen op het gebied van cyberbeveiliging en het toezicht op die maatregelen op nationaal niveau. Wanneer een entiteit de risicobeheersmaatregelen op het gebied van cyberbeveiliging uit hoofde van deze richtlijn [...]naleeft, kunnen de krachtens Verordeningen (EG) nr. 300/2008 en (EU) 2018/1139 aangewezen nationale autoriteiten ervan uitgaan dat die entiteit ook de in die verordeningen vastgestelde vereisten en de desbetreffende op grond daarvan vastgestelde gedelegeerde en uitvoeringshandelingen naleeft.

---

16 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).

17 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).

(14) Gezien de onderlinge verbanden tussen cyberbeveiliging en de fysieke beveiliging van entiteiten moet een coherente aanpak worden gewaarborgd tussen Richtlijn (EU) XXX/XXX van het Europees Parlement en de Raad en deze richtlijn. Daartoe moeten de lidstaten ervoor zorgen dat kritieke entiteiten **[**en gelijkwaardige entiteiten**]** uit hoofde van Richtlijn (EU) XXX/XXX [...] **als** essentiële entiteiten uit hoofde van deze richtlijn worden beschouwd. De lidstaten moeten er ook voor zorgen dat hun strategieën op het gebied van cyberbeveiliging voorzien in een beleidskader voor een betere coördinatie tussen de bevoegde autoriteit in het kader van deze richtlijn en die in het kader van Richtlijn (EU) XXX/XXX in de context van de uitwisseling van informatie over incidenten en cyberbedreigingen en de uitoefening van toezichthoudende taken. De in het kader van beide richtlijnen **bevoegde** [...]autoriteiten moeten samenwerken en informatie uitwisselen, met name met betrekking tot de identificatie van kritieke entiteiten, cyberbedreigingen, cyberbeveiligingsrisico's, incidenten, **evenals niet-cybergerelateerde risico's, bedreigingen en incidenten** die kritieke entiteiten **[**of **entiteiten die gelijkwaardig zijn aan kritieke entiteiten]** treffen, [...] **met inbegrip van** door kritieke entiteiten genomen maatregelen op het gebied van cyberbeveiliging en **fysieke** maatregelen, **en de resultaten van toezichtactiviteiten met betrekking tot die entiteiten. Om de toezichtactiviteiten tussen de krachtens beide richtlijnen aangewezen bevoegde autoriteiten te stroomlijnen en de administratieve lasten voor de betrokken entiteiten tot een minimum te beperken, moeten de bevoegde autoriteiten ernaar streven de modellen voor het melden van incidenten en de toezichtsprocessen te harmoniseren.** [...] **In voorkomend geval** kunnen de uit hoofde van Richtlijn (EU) XXX/XXX [...] bevoegde autoriteiten de uit hoofde van deze richtlijn [...] bevoegde autoriteiten **verzoeken** hun toezichts- en handhavingsbevoegdheden [...] uit te oefenen **met betrekking tot** een essentiële entiteit die als kritiek is aangemerkt. [...]

(14a) Entiteiten die tot de digitale-infrastructuursector behoren, zijn in wezen gebaseerd op netwerk- en informatiesystemen en daarom moeten de hun bij deze richtlijn opgelegde verplichtingen op een brede manier betrekking hebben op de fysieke beveiliging van dergelijke systemen als onderdeel van hun verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging. Aangezien deze aangelegenheden onder deze richtlijn vallen, zijn de verplichtingen van de hoofdstukken III tot en met VI van Richtlijn (EU) XXX/XXX [CER] niet van toepassing op dergelijke entiteiten.

(15) Het behoud van een betrouwbaar, veerkrachtig en veilig domeinnaamsysteem (DNS) is een sleutelfactor voor het behoud van de integriteit van het internet en is essentieel voor de continue en stabiele werking ervan, waarvan de digitale economie en de maatschappij afhankelijk zijn. Daarom moet deze richtlijn van toepassing zijn op aanbieders van DNS-diensten in de DNS**-leverings- en** -omzettingsketen **die belangrijk zijn voor de interne markt**, met inbegrip van [...] **registers** voor topleveldomeinnamen [...], **de entiteiten die domeinnaamregistratiediensten verlenen, exploitanten van** gezaghebbende naamservers voor domeinnamen en **exploitanten van** recursieve resolvers. **De term "DNS-dienstverlener" mag niet worden gebruikt voor DNS-diensten die worden geëxploiteerd voor eigen doeleinden van de betrokken entiteit en haar gelieerde entiteiten. De uit deze richtlijn voortvloeiende cyberbeveiligingsverplichtingen voor deze categorie aanbieders zijn strikt beperkt tot maatregelen voor risicobeheer op het gebied van cyberbeveiliging en melding, en laten derhalve de governance van het mondiale DNS door de multistakeholdergemeenschap onverlet.**

(16) Cloudcomputerdiensten moeten betrekking hebben op diensten die toegang op aanvraag en brede toegang op afstand mogelijk maken tot een schaalbare en elastische pool van gedeelde en gedistribueerde computerbronnen. Deze computerbronnen omvatten middelen zoals netwerken, servers of andere infrastructuur, besturingssystemen, software, opslag, toepassingen en diensten. **De dienstenmodellen van cloudcomputing omvatten onder meer het aanbieden van infrastructuur, platformen, software en netwerken (Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) en Network-as-a-Service (NaaS)).** De invoeringsmodellen van cloud-computing moeten private, gemeenschaps-, publieke en hybride cloud omvatten. De genoemde dienst- en invoeringsmodellen hebben dezelfde betekenis als de in de ISO/IEC 17788:2014-norm gedefinieerde benamingen van dienst- en invoeringsmodellen. Het vermogen van de cloudcomputergebruiker om eenzijdig zelfvoorzienend te zijn, zoals servertijd of netwerkopslag, zonder enige menselijke interactie door de cloudcomputer-dienstverlener, zou kunnen worden omschreven als beheer op verzoek. Met het begrip "brede toegang op afstand" wordt bedoeld: de cloudcapaciteiten worden via het netwerk aangeboden en zijn toegankelijk via mechanismen die het gebruik van heterogene thin- of thick-client-platforms bevorderen (waaronder mobiele telefoons, tablets, laptops, werkstations).

Met "schaalbaar" wordt bedoeld: computercapaciteit die, ongeacht de geografische locatie van de capaciteit, op flexibele wijze door aanbieders van cloudcomputerdiensten wordt toegewezen teneinde schommelingen in de vraag te kunnen opvangen. Met "elastische groep" wordt bedoeld: 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. Met "gedeeld" wordt bedoeld: 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. Met "gedistribueerd" wordt bedoeld: de computercapaciteit die zich op verschillende netwerkcomputers of -toestellen bevindt en die onderling communiceert en coördineert door middel van het doorgeven van berichten.

(17) Gezien de opkomst van innovatieve technologieën en nieuwe bedrijfsmodellen wordt verwacht dat er nieuwe invoerings- en servicemodellen voor cloudcomputing op de markt zullen verschijnen als antwoord op de veranderende behoeften van klanten. In die context kunnen cloudcomputerdiensten in een sterk gedistribueerde vorm worden verleend, nog dichter bij de plaats waar de gegevens worden gegenereerd of verzameld, waardoor de overstap van het traditionele model naar een sterk gedistribueerd model ("edge computing") wordt gemaakt.

(18) Diensten die worden aangeboden door aanbieders van datacentradiensten kunnen niet altijd worden verleend in een vorm van een cloudcomputerdienst. Datacentra maken dan ook niet altijd deel uit van de cloudcomputerinfrastructuur. Om alle risico's voor de beveiliging van netwerk- en informatiesystemen te beheren, moet deze richtlijn ook van toepassing zijn op aanbieders van dergelijke datacentrumdiensten die geen cloudcomputerdiensten zijn. Voor de toepassing van deze richtlijn wordt onder "datacentrumdienst" verstaan: 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 informatie-technologie en netwerkapparatuur die diensten op het gebied van gegevensopslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole. De term "datacentrumdienst" is niet van toepassing op interne bedrijfsdatacentra die eigendom zijn van en geëxploiteerd worden voor eigen doeleinden van de betreffende entiteit.

(19) Verleners van postdiensten in de zin van Richtlijn 97/67/EG van het Europees Parlement en de Raad[18], [...] **waaronder** verleners [...] van [...] koerierdiensten, moeten onder deze richtlijn vallen indien zij ten minste een van de stappen in de postbestelketen en met name ophaling, sortering of distributie, met inbegrip van ophaaldiensten, verzorgen. Vervoers-diensten die niet in samenhang met een van deze stappen worden ondernomen, moeten buiten het toepassingsgebied van de postdiensten vallen.

---

[18] 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).

(20) Deze toenemende onderlinge afhankelijkheid is het resultaat van een steeds meer grens-overschrijdend en onderling afhankelijk dienstverleningsnetwerk dat gebruik maakt van belangrijke infrastructuren in de hele Unie in de sectoren energie, vervoer, digitale infrastructuur, drinkwater en afvalwater, gezondheid, bepaalde aspecten van het openbaar bestuur en de ruimtevaart, voor zover het gaat om de verlening van bepaalde diensten die afhankelijk zijn van grondgebonden infrastructuren die eigendom zijn van, beheerd en geëxploiteerd worden door de lidstaten of door private partijen, en die dus geen betrekking hebben op infrastructuren die eigendom zijn van, beheerd of geëxploiteerd worden door of namens de Unie als onderdeel van haar ruimtevaartprogramma's. Deze onderlinge afhankelijkheid houdt in dat elke verstoring, zelfs als deze aanvankelijk beperkt blijft tot één entiteit of één sector, een bredere kettingreactie kan teweegbrengen, met mogelijkerwijs verstrekkende en langdurige negatieve gevolgen voor de verlening van diensten op de hele interne markt. De COVID-19-pandemie heeft de kwetsbaarheid van onze steeds meer onderling afhankelijke samenlevingen voor de risico's van lage waarschijnlijkheid aangetoond.

(**20a**) **Om een hoog niveau van cyberbeveiliging te bereiken en te handhaven, moeten de bij deze richtlijn vereiste nationale cyberbeveiligingsstrategieën samenhangende kaders bieden voor governance op het gebied van cyberbeveiliging. De strategieën kunnen bestaan uit een of meer documenten van wetgevende of niet-wetgevende aard.**

(21) 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 meer dan één nationale bevoegde autoriteit kunnen aanwijzen die verantwoordelijk is voor het vervullen van de taken in verband met de beveiliging van de netwerk- en informatiesystemen van essentiële en belangrijke entiteiten in het kader van deze richtlijn. De lidstaten moeten deze rol kunnen toewijzen aan een bestaande autoriteit.

(22) Om de grensoverschrijdende samenwerking en communicatie tussen de autoriteiten te vergemakkelijken en een doeltreffende uitvoering van deze richtlijn mogelijk te maken, moet elke lidstaat één nationaal 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.

(23) De bevoegde autoriteiten of de CSIRT's moeten de meldingen van incidenten op een effectieve en efficiënte manier van de entiteiten ontvangen, **mede teneinde, in voorkomend geval, een tijdige respons op incidenten te vergemakkelijken en de meldende entiteit van antwoord te voorzien**. De centrale contactpunten moeten worden belast met het doorsturen van meldingen van incidenten naar de centrale contactpunten van andere betrokken lidstaten. [...]

(23a) In de sectorspecifieke rechtshandelingen van de Unie die maatregelen voor het beheer van cyberbeveiligingsrisico's of rapportageverplichtingen vereisen van minstens gelijke werking als de bij deze richtlijn vastgestelde maatregelen en verplichtingen, kan worden vastgelegd dat hun aangewezen bevoegde autoriteiten hun toezichts- en handhavingsbevoegdheden met betrekking tot die maatregelen of verplichtingen uitoefenen met de hulp van de overeenkomstig deze richtlijn aangewezen bevoegde autoriteiten. De bevoegde autoriteiten in kwestie kunnen hiervoor samenwerkingsregelingen treffen. In deze samenwerkingsregelingen kunnen onder meer de procedures voor de coördinatie van toezichtsactiviteiten worden omschreven, waaronder 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 bevoegde autoriteiten, met inbegrip van verzoeken van overeenkomstig deze richtlijn aangewezen bevoegde autoriteiten om toegang tot cybergerelateerde informatie.

(24) De lidstaten moeten, zowel wat de technische als de organisatorische mogelijkheden betreft, adequaat worden uitgerust om incidenten en risico's van het netwerk- en het informatiesysteem te voorkomen, op te sporen, erop te reageren en te beperken. De lidstaten moeten er daarom voor zorgen dat zij beschikken over goed functionerende CSIRT's, ook bekend als computercrisisresponsteams ("computer emergency response teams" — "CERT's"), die voldoen aan de essentiële 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. Om de vertrouwensrelatie tussen de entiteiten en de CSIRT's te versterken, [...] **kunnen** de lidstaten, in gevallen waarin een CSIRT deel uitmaakt van de bevoegde autoriteit, een functionele scheiding overwegen tussen de operationele taken van de CSIRT's, met name met betrekking tot het delen van informatie en de ondersteuning van de entiteiten, en de toezichtsactiviteiten van de bevoegde autoriteiten.

(25) Wat de persoonsgegevens betreft, moeten de CSIRT's overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad[19] namens en op verzoek van een entiteit in het kader van deze richtlijn een proactieve scan kunnen uitvoeren van de netwerk- en informatiesystemen die voor de verlening van hun diensten worden gebruikt. **Indien van toepassing** moeten de lidstaten ernaar streven dat alle sectorale CSIRT's over gelijke technische capaciteiten beschikken. De lidstaten kunnen het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) om bijstand vragen bij de ontwikkeling van nationale CSIRT's.

(26) Gezien het belang van internationale samenwerking op het gebied van cyberbeveiliging moeten de CSIRT's naast hun samenwerking in het bij deze richtlijn opgerichte CSIRT-netwerk ook kunnen deelnemen aan internationale samenwerkingsnetwerken. **Daarom kunnen CSIRT's en bevoegde autoriteiten informatie, met inbegrip van persoonsgegevens, uitwisselen met CSIRT's van derde landen of hun autoriteiten, met het oog op de uitvoering van hun taken uit hoofde van Verordening (EU) 2016/679. Bij ontstentenis van een adequaatheidsbesluit overeenkomstig artikel 45 van Verordening (EU) 2016/679 of van passende waarborgen uit hoofde van artikel 46 van die verordening, kan de uitwisseling van persoonsgegevens die noodzakelijk wordt geacht voor de beperking van significante cyberbedreigingen of de respons op een aan de gang zijnd significant incident, worden beschouwd als nodig op grond van een gewichtige reden van algemeen belang in de zin van artikel 49, lid 1, punt d), van Verordening (EU) 2016/679.**

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

(27) Overeenkomstig de bijlage bij Aanbeveling (EU) 2017/1548 van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises ("Blauwdruk")[20], moet onder een grootschalig incident een incident worden verstaan met significante gevolgen voor ten minste twee lidstaten of die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen. Afhankelijk van hun oorzaak en gevolgen kunnen grootschalige incidenten escaleren en veranderen in volwaardige crises die de goede werking van de interne markt niet mogelijk maken. Gezien het brede toepassingsgebied en in de meeste gevallen het grensoverschrijdende karakter van dergelijke incidenten, moeten de lidstaten en de betrokken instellingen, organen en agentschappen van de Unie op technisch, operationeel en politiek niveau samenwerken om de respons in de hele Unie naar behoren te coördineren.

(28) Aangezien de exploitatie van kwetsbaarheden in netwerk- en informatiesystemen aanzienlijke verstoringen en schade kan veroorzaken, is het snel identificeren en verhelpen van deze kwetsbaarheden een belangrijke factor in het verminderen van het cyberbeveiligingsrisico. Entiteiten die dergelijke systemen ontwikkelen **of beheren**, moeten daarom passende procedures vaststellen om kwetsbaarheden aan te pakken wanneer deze worden ontdekt. Aangezien kwetsbaarheden vaak door derden (rapporterende entiteiten) worden ontdekt en gemeld (bekendgemaakt), moet de fabrikant of aanbieder van ICT-producten of -diensten ook de nodige procedures invoeren om kwetsbaarheidsinformatie van derden te ontvangen. In dit verband bieden de internationale normen ISO/IEC 30111 en ISO/IEC **29147** richtsnoeren voor respectievelijk de respons op kwetsbaarheden en het bekendmaken van kwetsbaarheden. Wat de bekendmaking van kwetsbaarheden betreft, is met name de coördinatie tussen de rapporterende entiteiten en de fabrikanten of aanbieders van ICT-producten of -diensten van belang. De gecoördineerde bekendmaking van kwetsbaarheden duidt een gestructureerd proces aan waarbij kwetsbaarheden aan organisaties worden gemeld op een manier die de organisatie 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 de coördinatie tussen de rapporterende entiteit en de organisatie omvatten wat betreft het tijdstip van het herstel en de bekendmaking van de kwetsbaarheden.

---

20 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).

(29) De lidstaten moeten daarom maatregelen nemen en een ter zake dienend nationaal beleid vaststellen om een gecoördineerde bekendmaking van kwetsbaarheden te faciliteren. **Als onderdeel van hun nationale beleid moeten de lidstaten ernaar streven de problemen waar onderzoekers van kwetsbaarheden mee worden geconfronteerd, waaronder hun mogelijke blootstelling aan strafrechtelijke aansprakelijkheid, zoveel mogelijk weg te nemen, overeenkomstig hun nationale rechtsorde.** [...] De lidstaten moeten een CSIRT aanwijzen die de rol van "coördinator" op zich neemt en die, indien nodig, optreedt als tussenpersoon tussen de rapporterende entiteiten en de fabrikanten of aanbieders van ICT-producten of -diensten. De taken van de CSIRT-coördinator moeten met name bestaan uit het identificeren van en contact opnemen met de betrokken entiteiten, het ondersteunen van de rapporterende entiteiten, het onderhandelen over tijdschema's voor de bekendmaking en het beheren van kwetsbaarheden die van invloed zijn op meerdere organisaties (**gecoördineerde** bekendmaking van kwetsbaarheden door meerdere partijen). Wanneer **de gemelde kwetsbaarheid grote gevolgen kan hebben voor entiteiten** [...] in meer dan één lidstaat [...], moeten de aangewezen CSIRT's [...]**, waar nodig,** binnen het CSIRT-netwerk samenwerken.

(30) Toegang tot correcte en tijdige informatie over kwetsbaarheden die van invloed zijn op ICT-producten en -diensten draagt bij aan een verbeterd risicobeheer inzake cyberbeveiliging. In dat opzicht zijn bronnen van openbaar beschikbare informatie over kwetsbaarheden een belangrijk instrument voor entiteiten en hun gebruikers, maar ook voor nationale bevoegde autoriteiten en CSIRT's. Daarom moet het Enisa een kwetsbaarheidsregister instellen waarin essentiële en belangrijke entiteiten en hun leveranciers, alsmede entiteiten die niet onder het toepassingsgebied van deze richtlijn vallen **of aangewezen CSIRT's**, op vrijwillige basis kwetsbaarheden kunnen bekendmaken en de kwetsbaarheidsinformatie kunnen verstrekken die gebruikers in staat stelt passende beperkende maatregelen te nemen.

(31) Hoewel er soortgelijke kwetsbaarheidsregisters of -databases bestaan, worden deze gehost en onderhouden door entiteiten die niet in de Unie zijn gevestigd. Een Europees kwetsbaarheidsregister dat door het Enisa wordt bijgehouden, zou zorgen voor meer transparantie met betrekking tot het bekendmakingsproces voordat de kwetsbaarheid officieel bekend wordt gemaakt, en voor meer veerkracht in geval van verstoringen of onderbrekingen van de verlening van soortgelijke diensten. Om dubbel werk te voorkomen en zoveel mogelijk complementariteit na te streven, moet het Enisa de mogelijkheid onderzoeken om gestructureerde samenwerkingsovereenkomsten te sluiten met soortgelijke registers in jurisdicties van derde landen. **Het Enisa moet met name nauwe samenwerking met de aanbieders van het register van gemeenschappelijke kwetsbaarheden en risico's ("Common Vulnerabilities and Exposures" – "CVE") overwegen, waaronder de mogelijkheid om een CVE-registratieautoriteit ("CVE Numbering Authority") te worden.**

(32) **De Samenwerkingsgroep moet de strategische samenwerking en de informatie-uitwisseling tussen de lidstaten blijven ondersteunen en faciliteren, en het onderling vertrouwen tussen de lidstaten blijven vergroten.** De Samenwerkingsgroep moet om de twee jaar een werkprogramma opstellen, met inbegrip van de acties die door de groep moeten worden ondernomen om zijn doelstellingen en taken uit te voeren. Om mogelijke verstoringen van de werkzaamheden van de groep te voorkomen, moet het tijdschema van het eerste programma dat in het kader van deze richtlijn is vastgesteld, worden afgestemd op het tijdschema van het laatste programma dat in het kader van Richtlijn (EU) 2016/1148 is vastgesteld.

(33) 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 die moeten worden aangepakt door een betere uitvoering van de bestaande regels.

(34) 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. Hij moet regelmatig gezamenlijke bijeenkomsten organiseren met relevante private belanghebbenden uit de hele Unie om de activiteiten van de groep te bespreken en input te verzamelen over nieuwe beleidsuitdagingen. Om de samenwerking op het niveau van de Unie te versterken, moet de groep overwegen organen en agentschappen van de Unie die betrokken zijn bij het cyberbeveiligingsbeleid, zoals het Europees Centrum voor de bestrijding van cybercriminaliteit (EC3), het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA) en het Agentschap van de Europese Unie voor het ruimtevaartprogramma (EUSPA), uit te nodigen om deel te nemen aan de werkzaamheden van de groep.

(35) De bevoegde autoriteiten en de CSIRT's moeten de bevoegdheid krijgen om deel te nemen aan uitwisselingsprogramma's voor ambtenaren uit andere lidstaten om de samenwerking te verbeteren. De bevoegde autoriteiten moeten de nodige 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.

(35a) 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 zich bezighouden met cyberbeveiligingsbeleid, zoals Europol, uit te nodigen om deel te nemen aan zijn werkzaamheden.

(36) [...]

(36a) Om de doeltreffende uitvoering van de bepalingen van deze richtlijn, zoals de bepalingen met betrekking tot het beheer van kwetsbaarheden, risicobeheer op het gebied van cyberbeveiliging, rapportagemaatregelen en regelingen voor het delen van informatie, te faciliteren, mogen de lidstaten samenwerken met derde landen en activiteiten ondernemen die daartoe geschikt worden geacht, met inbegrip van het uitwisselen van informatie over bedreigingen, incidenten, kwetsbaarheden, instrumenten en methoden, tactieken, technieken en procedures, paraatheid en oefeningen op het gebied van cybercrisisbeheer, opleidingen, vertrouwensopbouw en regelingen voor het gestructureerd delen van informatie. Deze samenwerkings-overeenkomsten moeten in overeenstemming zijn met het recht van de Unie inzake gegevensbescherming.

(37) De lidstaten moeten bijdragen aan de totstandbrenging van het in Aanbeveling (EU) 2017/1584 beschreven EU-kader voor crisisrespons op het gebied van cyberbeveiliging 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 die de modaliteiten van die samenwerking bepalen**, en moeten dubbel werk voorkomen**. In de procedureregels van het EU-CyCLONe moet nader worden gespecificeerd hoe het netwerk moet functioneren, met inbegrip van, maar niet beperkt tot rollen, samenwerkingswijzen, interacties met andere relevante actoren en modellen voor het delen van informatie, alsmede communicatiemiddelen. Voor crisisbeheer op het **politieke** niveau van de Unie moeten de betrokken partijen zich baseren op de regelingen voor geïntegreerde politieke crisisrespons ("Integrated Political Crisis Response" — IPCR). De Commissie moet hiervoor gebruikmaken van het ARGUS-proces voor sectoroverschrijdende crisiscoördinatie op hoog niveau. Als de crisis een belangrijke externe of gemeenschappelijke veiligheids- en defensiedimensie (GVDB) met zich meebrengt, moet het crisisresponsmechanisme van de Europese Dienst voor extern optreden (EDEO) worden geactiveerd.

(37a) EU-CyCLONe moet bij grootschalige cyberincidenten en -crises fungeren als intermediair netwerk tussen het technische en politieke niveau. Het moet de samenwerking op operationeel niveau verbeteren door voort te bouwen op de bevindingen van het CSIRT-netwerk, gebruik te maken van zijn eigen vermogens om een effectbeoordeling op te stellen van grootschalige incidenten en crises, en de besluitvorming op politiek niveau te ondersteunen. De instellingen, organen en agentschappen van de EU moeten een bevoegde autoriteit die verantwoordelijk is voor het beheer van grootschalige veiligheidsincidenten en -crisis, aanwijzen om lid te worden van EU-CyCLONe.

(38) [...]

(39) [...]

(39a) De verantwoordelijkheid voor het waarborgen van de veiligheid van netwerk- en informatiesystemen ligt voor een groot deel bij essentiële en belangrijke entiteiten. Er moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordeling en de uitvoering van risicogerichte beveiligingsmaatregelen behelst.

(40) Risicobeheersmaatregelen moeten **rekening houden met de mate waarin de entiteit afhankelijk is van netwerk- en informatiesystemen en** maatregelen omvatten om eventuele risico's van incidenten te identificeren, om incidenten te voorkomen, op te sporen en te behandelen en om de gevolgen ervan te beperken. De beveiliging van netwerk- en informatiesystemen moet de beveiliging van opgeslagen, verzonden en verwerkte gegevens omvatten.

(40a) Aangezien bedreigingen voor de beveiliging van netwerk- en informatiesystemen uit verschillende hoeken kunnen komen, wordt in deze richtlijn een "alle risico's"-benadering gevolgd die betrekking heeft op de bescherming van netwerk- en informatiesystemen en hun fysieke omgeving tegen elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens, of van diensten die door of via netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen, zoals diefstal, brand, overstromingen en telecommunicatie- en stroomstoringen, of ongeoorloofde fysieke toegang tot en beschadiging en verstoring van de informatie- en informatieverwerkingsfaciliteiten van de entiteit. Bij de risicobeheersmaatregelen moet derhalve ook aandacht worden besteed aan de fysieke en omgevingsbeveiliging, door maatregelen te nemen om de netwerk- en informatiesystemen van de entiteit te beschermen tegen systeemstoringen, menselijke fouten, kwaadwillige acties en natuurverschijnselen, in overeenstemming met Europese of internationaal erkende normen, zoals die in de ISO 27000-reeks. In dit verband moeten entiteiten, als onderdeel van hun risicobeheersmaatregelen, ook aandacht besteden aan beveiligingsaspecten ten aanzien van personeel en een passend toegangsbeleid voeren. Deze maatregelen moeten in overeenstemming zijn met Richtlijn XXXX [CER-richtlijn].

(40b) Bij ontstentenis van passende overeenkomstig Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligingscertificeringsregelingen, kunnen de lidstaten eisen dat entiteiten gecertificeerde ICT-producten, -diensten en-processen gebruiken of een certificaat behalen onder beschikbare nationale cyberbeveiligingsregelingen, zodat zij voldoen aan de eisen inzake het beheer van cyberbeveiligingsrisico's in deze richtlijn.

(41) Om te voorkomen dat aan essentiële en belangrijke entiteiten onevenredige financiële en administratieve lasten worden opgelegd, moeten de eisen inzake het beheer van cyberbeveiligingsrisico's in verhouding staan tot het risico **voor** [...] het betrokken netwerk- en informatiesysteem [...], rekening houdend met de stand van de techniek van dergelijke maatregelen **en de uitvoeringskosten**. **Er moet tevens terdege rekening worden gehouden met de omvang van de entiteit, alsook met de waarschijnlijkheid dat een incident zich voordoet en de ernst van het incident.**

(41a) Om de regelgevingslast te verlichten, moeten de vereisten voor de uitvoering van risicobeheersmaatregelen op het gebied van cyberbeveiliging voor middelgrote, kleine en micro-entiteiten in beginsel minder streng zijn, tenzij strengere vereisten gerechtvaardigd zijn op grond van kriticiteitscriteria of nationale risicobeoordelingen, met name ten aanzien van entiteiten die voldoen aan de kriticiteitsgerelateerde criteria in deze richtlijn.

(42) Essentiële en belangrijke entiteiten moeten de beveiliging van de netwerk- en informatiesystemen die zij bij hun activiteiten gebruiken, waarborgen. Dit zijn voornamelijk private netwerk- en informatiesystemen die door hun interne IT-medewerkers worden beheerd of waarvan de beveiliging is uitbesteed. De vereisten inzake risicobeheer en rapportage voor cyberbeveiliging uit hoofde van deze richtlijn moeten van toepassing zijn op de betrokken essentiële en belangrijke entiteiten, ongeacht of zij het onderhoud van hun netwerk- en informatiesystemen intern uitvoeren of uitbesteden.

(42aa) Gezien hun grensoverschrijdende aard moeten DNS-dienstverleners, registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, en aanbieders van cloudcomputingdiensten, van datacentrumdiensten, van netwerken voor de levering van inhoud, van beheerde diensten en van beheerde beveiligingsdiensten worden onderworpen aan een hogere mate van harmonisatie op Unieniveau. Daarom moet de uitvoering van cyberbeveiligingsmaatregelen worden bewerkstelligd door middel van een uitvoeringshandeling.

(43) Het aanpakken van risico's op het gebied van cyberbeveiliging die voortvloeien uit de toeleveringsketen van een entiteit en uit haar relatie met haar leveranciers is bijzonder belangrijk gezien de prevalentie van incidenten waarbij entiteiten het slachtoffer zijn geworden van cyberaanvallen en waarbij kwaadwillende actoren 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. De entiteiten moeten daarom de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners beoordelen en er rekening mee houden, met inbegrip van hun veilige ontwikkelingsprocedures.

(44) Onder de dienstverleners spelen aanbieders van beheerde beveiligingsdiensten ("managed security services providers" — MSSP's) op het gebied van bijvoorbeeld incidentrespons, penetratietesten, beveiligingsaudits en consultancy een bijzonder belangrijke rol in het bijstaan van entiteiten bij hun inspanningen om incidenten op te sporen en erop te reageren. Deze MSSP's zijn echter ook zelf het doelwit geweest van cyberaanvallen en vormen door hun nauwe integratie in de activiteiten van de exploitanten een bijzonder cyberbeveiligingsrisico. De entiteiten moeten daarom meer zorgvuldigheid betrachten bij de selectie van een MSSP.

(44a) Ook nationale bevoegde autoriteiten kunnen, in het kader van hun toezichthoudende taken, gebruikmaken van cyberbeveiligingsdiensten zoals beveiligingsaudits en penetratietesten of incidentrespons. Om entiteiten en nationale bevoegde autoriteiten te helpen bij het selecteren van gekwalificeerde en betrouwbare aanbieders van cyberbeveiligingsdiensten, moet de Commissie, met behulp van de Samenwerkingsgroep en het Enisa, overwegen om overeenkomstig artikel 48 van Verordening (EU) 2019/881 Europese cyberbeveiligingscertificeringsregelingen aan te vragen.

(45) Entiteiten moeten ook aandacht besteden aan de risico's op het gebied van cyberbeveiliging die voortvloeien uit hun interacties en relaties met andere belanghebbenden binnen een breder ecosysteem. De 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 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 de entiteiten, gezien het belang en de waarde van gegevens voor de activiteiten van de entiteiten, bij het gebruik van gegevenstransformatie en gegevensanalysediensten van derden, alle passende cyberbeveiligingsmaatregelen nemen.

(46) Om de belangrijkste risico's van de toeleveringsketen verder aan te pakken en entiteiten die actief zijn in sectoren die onder deze richtlijn vallen, te helpen om de risico's van de toeleveringsketen en de leveranciers op het gebied van cyberbeveiliging op passende wijze te beheren, moet de Samenwerkingsgroep waarbij de relevante nationale autoriteiten betrokken zijn, in samenwerking met de Commissie en het Enisa, gecoördineerde sectorale risicobeoordelingen van de toeleveringsketen uitvoeren, zoals reeds is gedaan voor 5G-netwerken naar aanleiding van Aanbeveling (EU) 2019/534 inzake cyberbeveiliging van 5G-netwerken[21], met als doel per sector vast te stellen welke de kritieke ICT-diensten, -systemen of -producten, de relevante bedreigingen en kwetsbaarheden zijn.

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

(47) Bij de beoordeling van de risico's voor de toeleveringsketen 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 beveiliging van 5G-netwerken in de hele EU en in het EU-instrumentarium voor 5G-cyberbeveiliging dat door de Samenwerkingsgroep is overeengekomen. Om te bepalen welke toeleveringsketens aan een gecoördineerde risicobeoordeling 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, -systemen of -producten; ii) de relevantie van specifieke kritieke ICT-diensten, -systemen of -producten voor het uitvoeren van kritieke of gevoelige functies, met inbegrip van de verwerking van persoonsgegevens; iii) de beschikbaarheid van alternatieve ICT-diensten, -systemen of -producten; iv) de veerkracht van de gehele toeleveringsketen van ICT-diensten, -systemen of -producten tegen verstorende gebeurtenissen en v) voor opkomende ICT-diensten, -systemen of -producten, hun potentiële toekomstige betekenis voor de activiteiten van de entiteiten.

(48) Om de wettelijke verplichtingen die aan aanbieders van openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten worden opgelegd, te stroomlijnen en aanbieders van vertrouwensdiensten in verband met de beveiliging van hun netwerk- en informatiesystemen in staat te stellen gebruik te maken van het bij deze richtlijn vastgestelde rechtskader (met inbegrip van de aanwijzing van het CSIRT dat verantwoordelijk is voor de behandeling van risico's en incidenten, de deelname van de bevoegde autoriteiten en organen aan de werkzaamheden van de Samenwerkingsgroep en het **netwerk van CSIRT's**), moeten zij binnen het toepassingsgebied van deze richtlijn worden gebracht. De overeenkomstige bepalingen van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad[22] en Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad[23] met betrekking tot het opleggen van [...] beveiligings- en meldingsverplichting**en** aan d**a**t soort entiteiten moeten derhalve worden ingetrokken.

---

22 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).

23 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).

(48a) De in deze richtlijn vastgelegde beveiligingsverplichtingen zijn bedoeld als aanvulling op de eisen voor verleners van vertrouwensdiensten in Verordening (EU) nr. 910/2014 (eIDAS-verordening). Verleners van vertrouwensdiensten moet worden verzocht alle mogelijke passende en evenredige maatregelen te nemen om de risico's voor hun diensten te beheersen, onder meer met betrekking tot klanten en afhankelijke derden, en krachtens deze richtlijn melding te maken van beveiligingsincidenten. De verplichtingen inzake beveiliging en rapportage moeten ook betrekking hebben op de fysieke bescherming van de geleverde dienst. Artikel 24 van Verordening (EU) nr. 910/2014 blijft van toepassing.

(48 bis bis) De lidstaten kunnen de rol van bevoegde autoriteit voor vertrouwensdiensten toebedelen aan de toezichthoudende organen uit hoofde van de eIDAS-verordening, zodat de huidige praktijken worden voortgezet en er wordt voortgebouwd op de kennis en ervaring die is opgedaan bij de toepassing van die verordening. Indien die rol aan een ander orgaan wordt toegewezen, moeten de nationale bevoegde autoriteiten in het kader van deze richtlijn nauw en tijdig samenwerken en de nodige informatie uitwisselen om ervoor te zorgen dat er doeltreffend toezicht wordt gehouden op verleners van vertrouwensdiensten en dat deze zich houden aan de vereisten van deze richtlijn en Verordening [XXXX/XXXX].

In voorkomend geval moet de nationale bevoegde autoriteit van deze richtlijn het toezichthoudend orgaan van de eIDAS-verordening onmiddellijk informeren over alle gemelde significante cyberbedreigingen of -incidenten met gevolgen voor vertrouwensdiensten en over alle gevallen waarin een verlener van vertrouwensdiensten de vereisten van deze richtlijn niet naleeft. Voor de rapportage kunnen de lidstaten, indien van toepassing, een beroep doen op het centrale contactpunt dat is opgezet om incidenten automatisch te kunnen melden aan zowel het toezichthoudend orgaan uit hoofde van de eIDAS-verordening als de bevoegde autoriteit uit hoofde van deze richtlijn. De regels inzake de rapportageverplichtingen moeten Verordening (EU) 2016/679 en Richtlijn 2002/58/EG van het Europees Parlement en de Raad[24] onverlet laten.

---

[24] 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).

(49) Indien nodig en om onnodige verstoringen te voorkomen, **moeten de lidstaten bij het nemen van maatregelen voor de omzetting van deze richtlijn, rekening houden 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, en zo voortbouwen op de kennis en vaardigheden inzake maatregelen voor het beheer van beveiligingsrisico's en incidentmeldingen die reeds zijn opgedaan in het kader van Richtlijn (EU) 2018/1972. Het Enisa kan ook richtsnoeren inzake beveiligings- en rapportage-eisen opstellen voor aanbieders van openbare elektronischecommunicatienetwerken of openbare elektronische-communicatiediensten, om de harmonisatie en transitie te vergemakkelijken en de verstoringen tot een minimum te beperken. De lidstaten kunnen de rol van bevoegde autoriteit voor elektronische communicatie toebedelen aan de nationale regelgevende instanties, zodat de huidige praktijken worden voortgezet en er wordt voortgebouwd op de kennis en ervaring die is opgedaan in het kader van Richtlijn (EU) 2018/1972.**

(50) Gezien het toenemende belang van nummeronafhankelijke interpersoonlijke communicatiediensten moet ervoor worden gezorgd dat ook voor dergelijke diensten passende beveiligingseisen gelden, gelet op hun specifieke aard en economisch belang. Aanbieders van dergelijke diensten moeten dus ook zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op het risico. Aangezien aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten normaal gesproken geen daadwerkelijke controle uitoefenen op de transmissie van signalen over netwerken, kan de mate van risico voor dergelijke diensten in sommige opzichten als lager worden beschouwd dan voor traditionele elektronische-communicatiediensten. Hetzelfde geldt voor interpersoonlijke communicatiediensten die gebruikmaken van nummers en die geen daadwerkelijke controle uitoefenen op de signaaloverdracht.

(51) 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 diensten die via het internet worden verleend. Om te zorgen voor een soepele verlening van diensten die door essentiële en belangrijke entiteiten worden verleend, is het van belang dat openbare elektronische-communicatienetwerken, zoals internetbackbones of onderzeese communicatiekabels, over passende cyberbeveiligingsmaatregelen beschikken en incidenten in verband daarmee melden.

(52) [...] **Indien van toepassing** moeten de entiteiten de ontvangers van hun diensten op de hoogte brengen van bijzondere [...] maatregelen die zij kunnen nemen om het [...] risico **dat voortvloeit uit een significante cyberbedreiging** voor henzelf te beperken. **In voorkomend geval en met name wanneer de significante cyberbedreiging kan leiden tot een concreet incident, moeten de entiteiten de ontvangers van hun diensten en de bevoegde autoriteiten of CSIRT's ook informeren over de bedreiging zelf.** De verplichting om de ontvangers van dergelijke bedreigingen te informeren mag entiteiten niet ontslaan van de verplichting om op eigen kosten passende en onmiddellijke maatregelen te nemen om eventuele cyberbedreigingen te voorkomen of te verhelpen en het normale beveiligingsniveau van de dienst te herstellen. De verstrekking van dergelijke informatie over [...] **cyberbedreigingen** aan de ontvangers moet gratis zijn.

(53) De aanbieders van openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten moeten met name de ontvangers van de dienst op de hoogte brengen van bijzondere en significante cyberbedreigingen en van de maatregelen die zij kunnen nemen om de beveiliging van hun communicatie te beschermen, bijvoorbeeld door gebruik te maken van specifieke soorten software of versleuteltechnologieën.

(54) Om de veiligheid van elektronische-communicatienetwerken en -diensten te waarborgen, moet het gebruik van versleuteling, en met name eind-tot-eindcodering, worden bevorderd en, waar nodig, verplicht worden gesteld voor aanbieders van dergelijke diensten en netwerken, overeenkomstig de beginselen van beveiliging en privacy, standaard en door het ontwerp, voor de doeleinden van artikel 18. Het gebruik van eind-tot-eindversleuteling moet aansluiten op de bevoegdheden van de lidstaten om de bescherming van hun wezenlijke veiligheidsbelangen en de openbare veiligheid te waarborgen en om het onderzoek, de opsporing en de vervolging van strafbare feiten in overeenstemming met het recht van de Unie mogelijk te maken. Oplossingen voor legale toegang tot informatie in eind-tot-eind versleutelde communicatie moeten de effectiviteit van de versleuteling voor de bescherming van de privacy en de beveiliging van de communicatie behouden en tegelijkertijd een effectief antwoord op misdaad bieden.

(55) Deze richtlijn voorziet in een aanpak in twee fasen van de melding van incidenten om het juiste evenwicht te vinden tussen enerzijds een snelle melding die de potentiële verspreiding van incidenten helpt te beperken en entiteiten in staat stelt steun te zoeken, en anderzijds een grondige melding die waardevolle lessen trekt uit individuele incidenten en mettertijd de veerkracht van individuele bedrijven en hele sectoren ten aanzien van cyberbedreigingen verbetert. Wanneer entiteiten zich bewust worden van een incident, moeten zij binnen 24 uur een eerste melding doen, gevolgd door een eindverslag uiterlijk een maand later. De eerste melding hoeft enkel de informatie te bevatten die strikt noodzakelijk is om de bevoegde autoriteiten op de hoogte te brengen van het incident en de entiteit in staat te stellen om, indien nodig, bijstand te vragen. In die melding moet, indien van toepassing, worden aangegeven of het incident vermoedelijk door een onwettige of kwaadwillige handeling is veroorzaakt. De lidstaten moeten ervoor zorgen dat de eis om deze eerste melding in te dienen de middelen van de rapporterende entiteit niet afleidt van activiteiten die verband houden met de incidentenbehandeling en die als prioritair moeten worden aangemerkt. Om verder te voorkomen dat rapportageverplichtingen inzake incidenten middelen onttrekken aan de incidentrespons of de inspanningen van de entiteiten op dat gebied anderszins in gevaar brengen, moeten de lidstaten ook bepalen dat de betrokken entiteit in naar behoren gemotiveerde gevallen en in overleg met de bevoegde autoriteiten of het CSIRT kan afwijken van de termijnen van 24 uur voor de eerste melding en één maand voor het eindverslag.

(55a) Een proactieve aanpak van cyberbedreigingen is een onmisbaar onderdeel van het beheer van cyberbeveiligingsrisico's en moet ervoor zorgen dat bevoegde autoriteiten daadwerkelijk kunnen voorkomen dat cyberbedreigingen leiden tot concrete incidenten die aanzienlijke materiële of immateriële schade kunnen veroorzaken. Daartoe is het van cruciaal belang dat significante cyberbedreigingen worden gemeld.

(56) Essentiële en belangrijke entiteiten bevinden 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 lasten en kunnen ook leiden tot onzekerheden met betrekking tot het formaat en de procedures van dergelijke meldingen. Met het oog hierop en om de melding van beveiligingsincidenten te vereenvoudigen, [...] **kunnen** de lidstaten een centraal contactpunt instellen voor alle meldingen die op grond van deze richtlijn en ook op grond van andere EU-wetgeving, zoals Verordening (EU) 2016/679 en Richtlijn 2002/58/EG, vereist zijn. Het Enisa moet, in samenwerking met de Samenwerkingsgroep, gemeenschappelijke meldingsmodellen ontwikkelen door middel van richtsnoeren die de door het recht van de Unie verlangde rapportage-informatie vereenvoudigen en stroomlijnen en de lasten voor bedrijven verminderen.

(57) Wanneer het vermoeden bestaat dat een incident verband houdt met ernstige criminele activiteiten op grond van het recht van de Unie of het nationale recht, moeten de lidstaten essentiële en belangrijke entiteiten aanmoedigen om, op basis van de toepasselijke regels voor strafrechtelijke procedures in overeenstemming met het recht van de Unie, incidenten met een vermoedelijk ernstig crimineel karakter aan de betrokken rechtshandhavings-instanties 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 EC3 en het Enisa.

(58) Persoonsgegevens worden in veel gevallen in gevaar gebracht als gevolg van incidenten. In dit verband moeten de bevoegde autoriteiten samenwerken en informatie uitwisselen over alle relevante zaken met de gegevensbeschermingsautoriteiten en de toezichthoudende autoriteiten overeenkomstig Richtlijn 2002/58/EG.

(59) Het onderhouden van nauwkeurige en volledige databases van domeinnamen en registratiegegevens (de zogenaamde "WHOIS-gegevens") en het verlenen van rechtmatige toegang tot dergelijke gegevens is essentieel om de beveiliging, stabiliteit en veerkracht van het DNS te waarborgen, wat op zijn beurt bijdraagt tot een hoog gemeenschappelijk niveau van cyberbeveiliging binnen de Unie. Wanneer de verwerking persoonsgegevens omvat, moet die verwerking in overeenstemming zijn met het recht van de Unie inzake gegevensbescherming.

(60) De beschikbaarheid en tijdige toegankelijkheid van deze gegevens voor overheidsinstanties, met inbegrip van de autoriteiten die krachtens het recht van de Unie of het interne recht bevoegd zijn voor het voorkomen, onderzoeken of vervolgen van strafbare feiten, CERT's, CSIRT's, en met betrekking tot de gegevens van hun cliënten voor aanbieders van elektronische-communicatienetwerken en -diensten en aanbieders van cyberbeveiligingstechnologieën en -diensten die namens die cliënten optreden, is van essentieel belang om misbruik van domeinnamensystemen te voorkomen en te bestrijden, met name om cyberbeveiligingsincidenten te voorkomen, op te sporen en erop te reageren. Deze toegang moet in overeenstemming zijn met de EU-wetgeving inzake gegevensbescherming voor zover deze betrekking heeft op persoonsgegevens.

(61) Om de beschikbaarheid van nauwkeurige en volledige domeinnaamregistratiegegevens te waarborgen, moeten registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen (de zogenaamde registratoren) de integriteit en beschikbaarheid van domeinnaamregistratiegegevens verzamelen en waarborgen. **Met betrekking tot de registratiegegevens moeten de entiteiten in het bijzonder de naam en het e-mailadres van de registrant verifiëren.** [...] Registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, moeten beleid en procedures vaststellen om nauwkeurige en volledige registratiegegevens te verzamelen en bij te houden en om onjuiste registratiegegevens te voorkomen en te corrigeren in overeenstemming met de gegevensbeschermingsregels van de Unie.

(62) Registers voor topleveldomeinnamen en de entiteiten die voor hen domeinnaamregistratiediensten verlenen, moeten gegevens voor de registratie van domeinnamen die buiten het toepassingsgebied van de gegevensbeschermingsregels van de Unie vallen, zoals gegevens die betrekking hebben op rechtspersonen, openbaar maken[25]. Registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, moeten ook legale toegang tot specifieke domeinnaamregistratiegegevens over natuurlijke personen mogelijk maken voor legitieme toegangvragende partijen, in overeenstemming met de wetgeving van de Unie inzake gegevensbescherming. De lidstaten moeten ervoor zorgen dat registers voor topleveldomeinnamen en de entiteiten die voor hen domeinnaamregistratiediensten verlenen, onverwijld reageren op verzoeken [...] om openbaarmaking van gegevens over domeinnaamregistratie **van legitieme toegangvragende partijen, zoals autoriteiten die uit hoofde van het Unierecht of het nationale recht bevoegd zijn voor de nationale veiligheid en het strafrechtsysteem, of CSIRT's**. Registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor hen verlenen, moeten beleid en procedures vaststellen voor de publicatie en bekendmaking van registratiegegevens, met inbegrip van overeenkomsten inzake het dienstverleningsniveau voor de behandeling van verzoeken om toegang van legitieme toegangvragende partijen. De toegangsprocedure kan ook 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. **De lidstaten moeten ervoor zorgen dat alle vormen van toegang tot domeinregistratiegegevens (zowel persoonsgegevens als niet-persoonsgebonden gegevens) gratis zijn.** Met het oog op de bevordering van geharmoniseerde praktijken in de gehele interne markt kan de Commissie richtsnoeren voor dergelijke procedures vaststellen, zonder afbreuk te doen aan de bevoegdheden van het Europees Comité voor gegevensbescherming **en in lijn met en ter aanvulling van de internationale normen die de multistakeholdergemeenschap heeft ontwikkeld**.

---

25 [...] **Verordening** (EU) 2016/679 [...] **van het Europees Parlement en de Raad**, overweging 14: "Deze verordening heeft geen betrekking op de verwerking van gegevens over rechtspersonen en met name als rechtspersonen gevestigde ondernemingen, zoals de naam en de rechtsvorm van de rechtspersoon en de contactgegevens van de rechtspersoon.".

(63) Essentiële en belangrijke entiteiten in het kader van deze richtlijn dienen onder de jurisdictie te vallen van de lidstaat waar zij hun diensten verlenen. **De in de punten 1 tot en met 7 en 10 van bijlage I bedoelde entiteiten en de in punt 8 van bijlage I en de punten 1 tot en met 5 van bijlage II bij deze richtlijn bedoelde verleners van vertrouwensdiensten en internetknooppunten moeten onder de jurisdictie vallen van de lidstaat waar zij zijn gevestigd.** Indien de entiteit diensten verricht **of een vestiging heeft** in meer dan één lidstaat, moet zij onder de afzonderlijke en gelijktijdige jurisdictie van elk van deze lidstaten vallen. De bevoegde autoriteiten van deze lidstaten moeten samenwerken, elkaar wederzijds bijstand verlenen en, in voorkomend geval, gezamenlijke toezichtsacties uitvoeren. **Indien een lidstaat besluit zijn jurisdictie uit te oefenen, moet hij voorkomen dat hetzelfde gedrag meer dan één keer wordt bestraft wegens schending van de verplichtingen in deze richtlijn.**

(64) Om rekening te houden met het grensoverschrijdende karakter van de diensten en activiteiten van DNS-dienstverleners, registers voor topleveldomeinnamen, **entiteiten die registratiediensten voor topleveldomeinnamen verlenen,** aanbieders van netwerken voor de levering van inhoud, aanbieders van cloudcomputerdiensten, aanbieders van data-centrumdiensten en digitale aanbieders, zou slechts één lidstaat jurisdictie mogen hebben over deze entiteiten. De jurisdictie moet worden toegekend aan de lidstaat waar de respectieve 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 niet bepalend.

Of aan dit criterium wordt voldaan, mag niet afhangen van de vraag of het netwerk- en informatiesysteem 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 belangrijkste vestiging moet de plaats zijn waar de besluiten met betrekking tot de risicobeheers-maatregelen op het gebied van cyberbeveiliging in de Unie **hoofdzakelijk** worden genomen. Dit zal doorgaans overeenkomen met de plaats van de centrale administratie van de bedrijven in de Unie. Indien **niet kan worden vastgesteld op welke plaats deze besluiten hoofdzakelijk worden genomen of** dergelijke besluiten niet in de Unie worden genomen, moet de hoofdvestiging worden geacht zich te bevinden in de lidstaten waar de entiteit een vestiging heeft met het hoogste aantal werknemers in de Unie. 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.

(64a) Indien een aanbieder van openbare elektronischecommunicatienetwerken of openbare elektronische-communicatiediensten een recursieve DNS-dienst enkel verricht als onderdeel van de internettoegangsdienst, wordt de entiteit geacht onder de jurisdictie te vallen van alle lidstaten waar zij diensten verricht.

(64 bis bis) Om een duidelijk overzicht te krijgen van DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten voor toplevel-domeinnamen verlenen, aanbieders van netwerken voor de levering van inhoud, van cloudcomputerdiensten en van datacentradiensten en digitale aanbieders die in de hele Unie diensten verlenen die binnen het toepassingsgebied van deze richtlijn vallen, moet het Enisa een register aanleggen en bijhouden voor deze entiteiten, op basis van meldingen van de lidstaten, indien van toepassing via hun nationale mechanismen voor zelfmelding. Om ervoor te zorgen dat de informatie die in dit register moet worden opgenomen nauwkeurig en volledig is, moeten de lidstaten de gegevens die in hun nationale registers staan over deze entiteiten indienen bij het Enisa. Het Enisa en de lidstaten moeten maatregelen nemen om de interoperabiliteit van deze registers te bevorderen, en tegelijkertijd de bescherming van vertrouwelijke of gerubriceerde gegevens waarborgen.

(65) Wanneer een DNS-dienstverlener, register voor topleveldomeinnamen, aanbieder van een netwerk voor de levering van inhoud, aanbieder van cloudcomputerdiensten, aanbieder van datacentrumdiensten en digitale aanbieder die niet in de Unie is gevestigd, diensten binnen de Unie aanbiedt, moet hij een vertegenwoordiger aanwijzen. Om te bepalen of een dergelijke entiteit diensten binnen de Unie aanbiedt, moet worden nagegaan of het duidelijk is dat de entiteit voornemens is diensten aan te bieden aan personen in een of meer lidstaten. Het loutere feit dat er in de Unie toegang is tot de website van de entiteit of van een tussenpersoon of tot een e-mailadres en andere contactgegevens, of dat een taal wordt gebruikt die gangbaar is in het derde land waar de entiteit is gevestigd, is als zodanig onvoldoende 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 andere taal te bestellen, of de vermelding van klanten of gebruikers die zich in de Unie bevinden, kunnen echter duidelijk maken dat de entiteit voornemens 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 contact met de vertegenwoordiger kunnen opnemen. De vertegenwoordiger moet uitdrukkelijk bij schriftelijke opdracht van de entiteit worden aangewezen om namens de entiteit op te treden met betrekking tot haar verplichtingen uit hoofde van deze richtlijn, met inbegrip van de melding van incidenten.

(66) Wanneer er krachtens de bepalingen van deze richtlijn informatie wordt uitgewisseld, gerapporteerd of anderszins gedeeld die volgens het nationale of het EU-recht als gerubriceerd wordt beschouwd, moeten de overeenkomstige specifieke regels voor de behandeling van gerubriceerde informatie worden toegepast.

(67) Nu cyberbedreigingen complexer en geavanceerder worden, staan of vallen goede opsporings- en preventiemaatregelen voor een groot deel met het regelmatig delen van informatie over bedreigingen en kwetsbaarheden tussen entiteiten. Het delen van informatie draagt bij aan een grotere bewustwording van cyberbedreigingen, wat op zijn beurt het vermogen van de entiteiten om te voorkomen dat bedreigingen tot echte incidenten leiden, vergroot en de entiteiten in staat stelt om de effecten van incidenten beter te beheersen en efficiënter te herstellen. Bij gebrek aan richtsnoeren op het niveau van de Unie lijken verschillende factoren een dergelijk delen van inlichtingen te hebben afgeremd, met name de onzekerheid over de verenigbaarheid met de mededingings- en aansprakelijkheidsregels.

(68) Entiteiten moeten worden aangemoedigd om hun individuele kennis en praktische ervaring op strategisch, tactisch en operationeel niveau collectief te benutten om hun capaciteiten te vergroten om cyberbedreigingen adequaat te beoordelen, te monitoren, zich ertegen te verdedigen en ze te bestrijden. Het is dus noodzakelijk om op het niveau van de Unie ruimte te scheppen voor mechanismen waarmee vrijwillig informatie kan worden gedeeld. Daarom moeten de lidstaten ook relevante entiteiten die niet onder het toepassingsgebied van deze richtlijn vallen, actief ondersteunen en aanmoedigen om deel te nemen aan dergelijke mechanismen voor informatie-deling. Deze mechanismen moeten worden uitgevoerd met volledige inachtneming van de mededingingsregels van de Unie en de regels van het recht van de Unie inzake gegevensbescherming.

(69) [...]**V**oor zover strikt noodzakelijk en evenredig met het oog op netwerk- en informatiebeveiliging, **zou de verwerking van persoonsgegevens** door **essentiële en belangrijke** entiteiten [...] en aanbieders van beveiligingstechnologieën en -diensten **als noodzakelijk kunnen worden beschouwd om te kunnen voldoen aan een wettelijke verplichting of** [...] zou deze een rechtmatig belang van de betrokken verwerkingsverantwoordelijke kunnen vormen**[...]**, als bedoeld in Verordening (EU) 2016/679. Dit **zou** maatregelen **kunnen** [...] omvatten met betrekking tot de preventie, opsporing en analyse van incidenten en de reactie erop, maatregelen om het bewustzijn met betrekking tot specifieke cyberbedreigingen te vergroten, uitwisseling van informatie in het kader van herstel van de kwetsbaarheid en gecoördineerde bekendmaking, alsmede de vrijwillige uitwisseling van informatie over deze incidenten, [...] cyberbedreigingen en kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen. Dergelijke maatregelen kunnen de verwerking van [...] **verschillende** soorten persoonsgegevens vereisen, **bijvoorbeeld**: IP-adressen, uniforme resources locators (URL's), domeinnamen en e-mailadressen. **De verwerking van persoonsgegevens door bevoegde autoriteiten, SPOC's en CSIRT's moet in het nationale recht worden vastgelegd en als noodzakelijk worden beschouwd voor het vervullen van een wettelijke verplichting, voor het vervullen van een taak van algemeen belang of bij de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend, als bedoeld in artikel 6, lid 1, punten c) of e) van Verordening (EU) 2016/679.**

(69a) In de wetgeving van de lidstaten kunnen regels worden vastgelegd op grond waarvan bevoegde autoriteiten, SPOC's en CSIRT's, voor zover dit strikt noodzakelijk en evenredig is voor het waarborgen van de veiligheid van de netwerk- en informatiesystemen van essentiële en belangrijke entiteiten, bijzondere categorieën persoonsgegevens kunnen 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 belangen van natuurlijke personen, met inbegrip van technische beperkingen voor het hergebruik van dergelijke gegevens en het gebruik van ultramoderne beveiligings- en privacybeschermende maatregelen, zoals pseudonimisering of versleuteling wanneer anonimisering aanzienlijke gevolgen kan hebben voor het nagestreefde doel.

(70) Ter versterking van de toezichtsbevoegdheden en -maatregelen die bijdragen tot een doeltreffende naleving, moet deze richtlijn voorzien in een minimumlijst van toezichts-maatregelen en -middelen waarmee de bevoegde autoriteiten toezicht **kunnen** [...] houden op essentiële en belangrijke entiteiten. Bovendien moet deze richtlijn een onderscheid maken tussen de toezichtsregeling voor essentiële en voor belangrijke entiteiten, teneinde te zorgen voor een billijk evenwicht tussen de verplichtingen voor zowel de entiteiten als de bevoegde autoriteiten. Zo moeten essentiële entiteiten aan een volwaardig toezichtsstelsel (*vooraf* en *achteraf*) worden onderworpen, terwijl belangrijke entiteiten aan een licht toezichtsstelsel, uitsluitend achteraf, moeten worden onderworpen. Voor deze laatste categorie betekent dit dat belangrijke entiteiten **niet mogen worden verplicht** [...] systematisch de naleving van de vereisten inzake risicobeheer voor cyberbeveiliging **te** documenteren, terwijl de bevoegde autoriteiten een reactieve benadering *achteraf* van het toezicht moeten toepassen en dus geen algemene verplichting hebben om toezicht te houden op die entiteiten. **Voor belangrijke entiteiten kan het toezicht *achteraf* plaatsvinden wanneer bewijzen, aanwijzingen of informatie onder de aandacht van bevoegde autoriteiten zijn gebracht en die door deze autoriteiten worden geacht te wijzen op een mogelijke niet-nakoming van de in deze richtlijn vastgelegde verplichtingen. Dergelijke bewijzen, aanwijzingen of informatie kunnen bijvoorbeeld van het type zijn dat door andere autoriteiten, entiteiten, burgers, media of andere bronnen aan bevoegde autoriteiten wordt verstrekt, kunnen openbaar beschikbare informatie zijn, of kunnen voortkomen uit andere activiteiten die bevoegde autoriteiten bij de uitvoering van hun taken verrichten.**

(70bis) 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 toezichts-maatregelen en -middelen die per risicocategorie worden aanbevolen, zoals het gebruik, de frequentie of het type van inspecties ter plaatse of gerichte beveiligings-audits 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 geëvalueerd en herzien, onder meer met betrekking tot aspecten als de middelentoewijzing en de behoeften.

(70bisa) Met betrekking tot overheidsinstanties moeten de toezichtsbevoegdheden conform de nationale kaders en nationale rechtsorde worden uitgeoefend. De lidstaten moeten een besluit kunnen nemen over het opleggen van passende, evenredige en doeltreffende toezichts- en handhavingsmaatregelen ten aanzien van deze entiteiten.

(70bisaa) Om aan te tonen dat bepaalde risicobeheersmaatregelen op het gebied van cyberbeveiliging worden nageleefd, zouden de lidstaten essentiële en belangrijke entiteiten kunnen verplichten gebruik te maken van gekwalificeerde vertrouwens-diensten of aangemelde stelsels voor elektronische identificatie volgens Verordening (EU) nr. 910/2014.

(71) Om de handhaving doeltreffend te maken, moet er een minimumlijst van administratieve sancties voor inbreuken op de bij deze richtlijn vastgestelde verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging worden vastgesteld, waarbij een duidelijk en samenhangend kader voor dergelijke sancties in de hele Unie moet worden opgezet. Er moet terdege rekening worden gehouden met de aard, de ernst en de duur van de inbreuk, de daadwerkelijk veroorzaakte schade of geleden verliezen of de potentiële schade of verliezen die hadden kunnen worden veroorzaakt, het opzettelijke of nalatige karakter van de inbreuk, de maatregelen die zijn genomen om de geleden schade en/of verliezen te voorkomen of te beperken, de mate van verantwoordelijkheid of eventuele relevante eerdere inbreuken, de mate van samenwerking met de bevoegde instantie en elke andere verzwarende of verzachtende omstandigheid. Het opleggen van sancties, met inbegrip van administratieve boeten, moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het recht van de Unie en het Handvest van de grondrechten van de Europese Unie, met inbegrip van een doeltreffende rechtsbescherming en een eerlijke rechtsgang.

(71bis) De bepalingen over de aansprakelijkheid van natuurlijke personen die binnen een entiteit bepaalde verantwoordelijkheden dragen wegens het niet nakomen van hun plicht om te zorgen voor naleving van de in deze richtlijn vastgelegde verplichtingen, houden voor de lidstaten geen verplichting in om te zorgen voor strafrechtelijke vervolging of civielrechtelijke aansprakelijkheidsstelling voor schade die door een dergelijke schending aan derden wordt toegebracht.

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

(73) Wanneer aan een onderneming administratieve geldboeten worden opgelegd, moet een onderneming voor die doeleinden worden opgevat als een onderneming in de zin van de artikelen 101 en 102 VWEU. Wanneer administratieve boeten worden opgelegd aan personen die geen onderneming zijn, moet de toezichthoudende 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 boeten moeten worden onderworpen. Het opleggen van een administratieve boete 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.

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

(75) Wanneer deze richtlijn niet voorziet in de harmonisatie van administratieve sancties of, indien nodig, in andere gevallen, bijvoorbeeld bij ernstige inbreuken op de in deze richtlijn vastgelegde verplichtingen, moeten de lidstaten een systeem toepassen dat voorziet in doeltreffende, evenredige en afschrikkende sancties. De aard van deze strafrechtelijke of bestuursrechtelijke sancties moet door de wetgeving van de lidstaten worden bepaald.

(76) Om de doeltreffendheid en het afschrikkingseffect van de sancties die van toepassing zijn op inbreuken op de uit hoofde van deze richtlijn vastgestelde verplichtingen verder te versterken, moeten de bevoegde instanties de bevoegdheid krijgen om sancties toe te passen die bestaan uit de opschorting van een certificering of vergunning voor een deel of het geheel van de door een essentiële entiteit verleende diensten en het opleggen van een tijdelijk verbod op de uitoefening van bestuursfuncties door een natuurlijke persoon. Gezien de ernst en het effect ervan op de activiteiten van de entiteiten en uiteindelijk op hun consumenten, mogen dergelijke sancties alleen worden toegepast in verhouding tot de ernst van de inbreuk en rekening houdend met de specifieke omstandigheden van elk geval, met inbegrip van het opzettelijke of nalatige karakter van de inbreuk, de maatregelen die zijn genomen om de geleden schade en/of verliezen te voorkomen of te beperken. Dergelijke sancties mogen alleen worden toegepast als ultiem middel, met andere woorden alleen nadat de andere relevante handhavingsacties waarin deze richtlijn voorziet, zijn uitgeput, en alleen totdat de entiteiten waarop zij van toepassing zijn, de nodige maatregelen nemen om de tekortkomingen te verhelpen of te voldoen aan de vereisten van de bevoegde autoriteit waarvoor dergelijke sancties zijn opgelegd. Het opleggen van dergelijke sancties moet worden onderworpen aan passende procedurele waarborgen overeenkomstig de algemene beginselen van het recht van de Unie en het Handvest van de grondrechten van de Europese Unie, met inbegrip van een doeltreffende rechtsbescherming, een eerlijke rechtsgang, het vermoeden van onschuld en de rechten van de verdediging.

(76bis) Met het oog op een doeltreffend toezicht en doeltreffende handhaving, met name in gevallen met een grensoverschrijdende dimensie, moeten de lidstaten die een verzoek om wederzijdse bijstand hebben ontvangen passende toezichts- en handhavings-maatregelen nemen, voor zover die het verzoek betreffen, met betrekking tot de entiteit die de diensten verleent of die over het netwerk- en informatiesysteem op hun grond-gebied beschikt.

(77) 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 in verband met persoonsgegevens.

(78) 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 organisaties. Om deze redenen moeten de beheersorganen van de entiteiten die onder het toepassingsgebied van deze richtlijn vallen, de maatregelen inzake cyberbeveiligingsrisico's goedkeuren en toezicht houden op de uitvoering ervan.

(79) Er moet een [...]**systeem voor inter**collegiaal [...] **leren** worden ingevoerd **om het wederzijds vertrouwen te helpen versterken en te leren van goede praktijken en ervaringen**, en waarmee deskundigen die door de lidstaten zijn aangewezen aan [...] **intercollegiale uitwisseling** over de uitvoering van het cyberbeveiligingsbeleid kunnen doen[...]. **Bij de invoering van het systeem voor intercollegiaal leren moet er in het bijzonder op worden gelet dat dit systeem de betrokken autoriteiten van de lidstaten niet onnodig of onevenredig belast. De Commissie moet alle mogelijkheden onderzoeken om te garanderen dat de kosten die kunnen voortvloeien uit de organisatie van opdrachten betreffende intercollegiaal leren financieel worden gedekt. Voorts moet het systeem voor intercollegiaal leren rekening houden met de resultaten van soortgelijke mechanismen – zoals het systeem voor collegiale toetsing van het CSIRT-netwerk –, waarde toevoegen en dubbel werk voorkomen. De invoering van het systeem voor intercollegiaal leren dient de nationale of Uniewetgeving inzake de bescherming van vertrouwelijke en gerubriceerde informatie onverlet te laten. Vóór het begin van de intercollegiale leerrondes kunnen de lidstaten een zelfbeoordeling van de relevante aspecten uitvoeren. Op verzoek van de Samenwerkingsgroep kan het Enis waar nodig richtsnoeren verstrekken over de zelfbeoordeling en de desbetreffende modellen. De lidstaten kunnen besluiten hun respectieve verslagen openbaar te maken.**

(80) [...]

(81) Om eenvormige voorwaarden te waarborgen voor de uitvoering van de relevante bepalingen van deze richtlijn betreffende de procedurele regelingen die nodig zijn voor het functioneren van de Samenwerkingsgroep, de technische elementen met betrekking tot de risicobeheersmaatregelen of het soort informatie, het formaat en de procedure voor de melding van incidenten**, de categorieën entiteiten die nodig zijn om bepaalde gecertificeerde ICT-producten, -diensten en -processen te gebruiken**, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad[26].

(82) De Commissie moet deze richtlijn op gezette tijden herzien, in overleg met de betrokken partijen, met name om vast te stellen of er wijzigingen nodig zijn in het licht van veranderingen in de maatschappelijke, politieke, technologische of marktomstandigheden.

---

[26] 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).

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

(84) Deze richtlijn eerbiedigt de grondrechten en neemt de beginselen in acht die zijn erkend in het Handvest van de grondrechten van de Europese Unie, met name het recht op eerbiediging van het privéleven en van de communicatie, de bescherming van persoonsgegevens, de vrijheid van ondernemerschap, het recht op eigendom, het recht op een doeltreffende voorziening in rechte en het recht om te worden gehoord. Deze richtlijn moet worden uitgevoerd overeenkomstig deze rechten en beginselen,

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

HOOFDSTUK I

Algemene bepalingen

Artikel 1

Onderwerp

1. Bij deze richtlijn worden maatregelen vastgesteld om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie te waarborgen, **teneinde de werking van de interne markt te verbeteren**.

2. Met het oog hierop worden in deze richtlijn:

   a) verplichtingen voor de lidstaten vastgesteld om nationale strategieën voor cyberbeveiliging vast te stellen en om nationale bevoegde autoriteiten, centrale contactpunten en computer security incident response teams (CSIRT's) aan te wijzen;

   b) verplichtingen vastgesteld inzake risicobeheer en rapportage op het gebied van cyberbeveiliging voor entiteiten van een type [...] dat in de bijlage**n I en II** wordt vermeld[...];

   c) **regels en** verplichtingen vastgesteld met betrekking tot het delen van informatie op het gebied van cyberbeveiliging.

Artikel 2

Toepassingsgebied

1. Deze richtlijn is van toepassing op publieke en private entiteiten van de [...] types die in de bijlagen **I en II** [...] worden **vermeld** [...] **en onder of boven de drempels voor middelgrote ondernemingen** [...] in de zin van Aanbeveling 2003/361/EG van de Commissie[27] **vallen**. **Artikel 3, lid 4, en artikel 6, lid 2, tweede en derde alinea, van de bijlage bij die aanbeveling zijn niet van toepassing voor de toepassing van deze richtlijn.**

2. [...]**O**ngeacht de [...] omvang **van de in lid 1 bedoelde entiteiten** is deze richtlijn ook van toepassing **wanneer:** […]

   a) de diensten worden verleend door een van de volgende entiteiten:

      i) **aanbieders van** de in punt 8 van bijlage I bedoelde openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten;

      ii) **de in punt XX van bijlage I bedoelde gekwalificeerde verleners van vertrouwensdiensten;**

      iii) **de in punt XX van bijlage I bedoelde niet-gekwalificeerde verleners van vertrouwensdiensten;**

      iv) de in punt 8 van bijlage I bedoelde registers voor topleveldomeinnamen [...];

   b) […]

[27] 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).

c) de entiteit **in een lidstaat** de enige aanbieder is van een dienst [...] **die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten**;

d) een mogelijke verstoring van de dienstverlening door de entiteit **ernstige** [...] gevolgen kan hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid;

e) een mogelijke verstoring van de dienstverlening door de entiteit **ernstige** [...] systeemrisico's met zich mee kan brengen, met name voor de sectoren waar een dergelijke verstoring een grensoverschrijdende impact kan hebben;

f) [...];

g) de entiteit wordt aangemerkt als een kritieke entiteit overeenkomstig Richtlijn (EU) XXXX/XXXX van het Europees Parlement en de Raad[28] [Richtlijn inzake de veerkracht van kritieke entiteiten], **[**of als een entiteit die gelijkwaardig is aan een kritieke entiteit overeenkomstig artikel 7 van die richtlijn**]**.

2a. **Ongeacht hun omvang is deze richtlijn ook van toepassing op overheidsinstanties van centrale overheden die overeenkomstig het nationale recht als zodanig in een lidstaat zijn erkend en waarnaar wordt verwezen in punt 9 van bijlage I. De lidstaten kunnen bepalen dat deze richtlijn ook van toepassing is op overheidsinstanties op regionaal en lokaal niveau.**

28 *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

3. […]

Deze richtlijn doet geen afbreuk aan de verantwoordelijkheden van de lidstaten om de nationale veiligheid te waarborgen of aan hun bevoegdheid om andere essentiële staatsfuncties te vrijwaren, waaronder het waarborgen van de territoriale integriteit van de staat en het handhaven van de openbare orde.

3a. 1) Deze richtlijn is niet van toepassing op:

a) entiteiten die buiten het toepassingsgebied van het Unierecht vallen en in elk geval alle entiteiten die hoofdzakelijk activiteiten verrichten op het gebied van defensie, nationale veiligheid, openbare veiligheid of rechtshandhaving, ongeacht welke entiteit die activiteiten uitoefent en ongeacht of het gaat om een publieke of private entiteit, onverminderd punt 2);

b) entiteiten die activiteiten uitvoeren op het gebied van de rechterlijke macht, parlementen of centrale banken.[...]

2) Wanneer overheidsinstanties activiteiten op deze gebieden enkel verrichten in het kader van hun algemene activiteiten, worden zij volledig uitgesloten van het toepassingsgebied van deze richtlijn.

3aa. Deze richtlijn is niet van toepassing op:

i) activiteiten van entiteiten die buiten het toepassingsgebied van het Unierecht vallen en in elk geval alle activiteiten met betrekking tot nationale veiligheid of defensie, ongeacht welke entiteit die activiteiten uitoefent en ongeacht of het gaat om een publieke of private entiteit;

ii) activiteiten van entiteiten binnen de rechterlijke macht, parlementen, centrale banken en op het gebied van de openbare veiligheid, met inbegrip van overheids-instanties die rechtshandhavingsactiviteiten uitoefenen met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of het uitvoeren van straffen.

3aaa. De in deze richtlijn vastgelegde verplichtingen houden niet in dat informatie wordt verstrekt waarvan de bekendmaking strijdig is met de wezenlijke belangen van de lidstaten inzake nationale veiligheid, openbare veiligheid of defensie.

3aaaa. Deze richtlijn geldt onverminderd het Unierecht inzake de bescherming van persoonsgegevens, met name de Verordening (EU) 2016/679 en Richtlijn 2002/58/EG.

3b. Deze richtlijn is niet van toepassing op entiteiten die zijn vrijgesteld van Verordening (EU) XXXX/XXXX van het Europees Parlement en de Raad [de DORA-verordening], overeenkomstig artikel 2, lid 4, van de DORA-verordening.

4. Deze richtlijn geldt onverminderd [...][29] [...] de Richtlijnen 2011/93/EU[30] en 2013/40/EU[31] van het Europees Parlement en de Raad.

5. Onverminderd artikel 346 VWEU worden gegevens die krachtens de voorschriften van de Unie en de lidstaten vertrouwelijk zijn, zoals de voorschriften inzake het zakengeheim, alleen met de Commissie en andere betrokken autoriteiten **overeenkomstig deze richtlijn** uitgewisseld wanneer deze uitwisseling noodzakelijk is voor de toepassing van deze richtlijn. De uitgewisselde informatie blijft beperkt tot de informatie die relevant is en in verhouding 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 essentiële of belangrijke entiteiten beschermd.

---

29 [...]

30 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).

31 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).

Artikel 2 bis

Essentiële en belangrijke entiteiten

1. Van de entiteiten waarop deze richtlijn van toepassing is, worden de volgende als essentieel beschouwd:

i) entiteiten als bedoeld in de punten 1 tot en met 8a en 10 van bijlage I bij deze richtlijn die boven de drempels voor middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie vallen;

ii) de in artikel 2, lid 2, punten a) en i) bedoelde middelgrote entiteiten;

iii) entiteiten als bedoeld in artikel 2, lid 2, punten a), ii) en iv), van deze richtlijn, ongeacht de omvang;

iv) entiteiten als bedoeld in artikel 2, lid 2, punt g), en artikel 2, lid 2a), van deze richtlijn, ongeacht de omvang;

v) indien opgericht door de lidstaten, entiteiten die vóór de inwerkingtreding van deze richtlijn door de lidstaten als aanbieders van essentiële diensten zijn aangemerkt overeenkomstig Richtlijn (EU) 2016/1148 of het nationale recht;

vi) entiteiten als bedoeld in bijlage II die boven de drempels voor middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie vallen, en die door de lidstaten op basis van de in artikel 2, lid 2, punten c) tot en met e) bedoelde criteria als essentieel zijn aangemerkt;

vii) middelgrote entiteiten in de zin van Aanbeveling 2003/361/EG van de Commissie, die door de lidstaten op basis van de in artikel 2, lid 2, punten c) tot en met e) bedoelde criteria als essentieel zijn aangemerkt;

viii) micro- of kleine entiteiten in de zin van Aanbeveling 2003/361/EG van de Commissie als bedoeld in lid 2, punt a), i), of die zijn vastgesteld overeenkomstig lid 2, punten c) tot en met e), van dit artikel en die door de lidstaten op basis van nationale risicobeoordelingen als essentieel zijn aangemerkt.

2. Van de entiteiten waarop deze richtlijn van toepassing is, worden de volgende als belangrijk beschouwd:

i) entiteiten als bedoeld in bijlage I bij deze richtlijn die kunnen worden aangemerkt als middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG van de Commissie en entiteiten als bedoeld in bijlage II en die onder of boven de drempels voor middelgrote ondernemingen in de zin van Aanbeveling 2003/361/EG[32] van de Commissie vallen;

ii) entiteiten als bedoeld in artikel 2, lid 2, punt iii), van deze richtlijn, ongeacht de omvang;

iii) kleine en micro-entiteiten als bedoeld in artikel 2, lid 2, punt a), i);

iv) kleine en micro-entiteiten die door de lidstaten op grond van artikel 2, lid 2, punten c) tot en met e), als belangrijke entiteiten zijn aangemerkt.

---

32 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).

Artikel 2a

Meldingsmechanismen

1. **De lidstaten kunnen een nationaal mechanisme voor zelfmelding instellen op grond waarvan alle onder deze richtlijn vallende entiteiten ten minste hun naam, adres, contactgegevens, de sector waarin zij actief zijn of het soort dienst dat zij verlenen en, indien van toepassing, de lijst van lidstaten waar zij onder deze richtlijn vallende diensten verlenen, moeten opgeven aan de uit hoofde van deze richtlijn bevoegde autoriteiten of bij de daartoe door de lidstaten aangewezen instanties.**

2. De lidstaten verstrekken de Commissie **[...] met betrekking tot de entiteiten die zij overeenkomstig artikel 2, lid 2, punten b) tot en met e), hebben aangemerkt, ten minste relevante informatie over het aantal aangemerkte entiteiten, de sector waartoe zij behoren of het soort dienst dat zij verlenen, overeenkomstig de bijlagen, en de specifieke bepaling(en) van artikel 2, lid 2, op basis waarvan zij uiterlijk [12 maanden na de termijn voor omzetting van deze richtlijn] zijn aangemerkt.** De lidstaten herzien [...] **deze informatie[...]** regelmatig, en vervolgens ten minste om de twee jaar, en werken deze zo nodig bij.

Artikel 2b

Sectorspecifieke handelingen van de Unie

1. Indien [...] bepalingen van sectorspecifieke handelingen **van het Unierecht** [...] voorschrijven dat essentiële of belangrijke entiteiten [...] ofwel risicobeheersmaatregelen op het gebied van cyberbeveiliging moeten nemen, ofwel **significante** incidenten of [...] cyberbedreigingen moeten melden, en indien deze eisen ten minste van gelijke werking zijn als de in deze richtlijn vastgestelde verplichtingen, zijn de relevante bepalingen van deze richtlijn, **met inbegrip van de bepaling inzake toezicht en handhaving als bedoeld in hoofdstuk VI**, niet van toepassing **op dergelijke entiteiten**. **Indien de sectorspecifieke bepalingen van een rechtshandeling van de Unie niet alle entiteiten bestrijken in een specifieke sector die binnen het toepassingsgebied van deze richtlijn valt, moeten de desbetreffende bepalingen van deze richtlijn van toepassing blijven op entiteiten die niet onder die sectorspecifieke bepalingen vallen.**

2. De in lid 1 van dit artikel bedoelde eisen worden geacht van gelijke werking te zijn als de in deze richtlijn vastgestelde verplichtingen indien de respectieve sectorspecifieke handeling van de Unie voorziet in onmiddellijke toegang, waar mogelijk automatisch en rechtstreeks, tot de meldingen van incidenten door de uit hoofde van deze richtlijn bevoegde autoriteiten of door de aangewezen CSIRT's, en indien

a) de risicobeheersmaatregelen op het gebied van cyberbeveiliging minstens van gelijke werking zijn als die welke zijn vastgesteld in artikel 18, leden 1 en 2, van deze Richtlijn; of

b) de eisen inzake de melding van significante incidenten minstens van gelijke werking zijn als die van artikel 20, leden 1 tot en met 6.

3. De Commissie maakt periodiek een evaluatie van de toepassing van de in de leden 1 en 2 van dit artikel bedoelde vereisten inzake gelijke werking met betrekking tot sector-specifieke bepalingen van rechtshandelingen van de Unie. De Commissie raadpleegt de Samenwerkingsgroep en het Enisa bij de voorbereiding van de periodieke evaluatie.

Artikel 3

Minimumharmonisatie

Onverminderd hun andere verplichtingen uit hoofde van het recht van de Unie kunnen de lidstaten **[...] op de gebieden die onder deze richtlijn vallen** bepalingen vaststellen of handhaven die een hoger niveau van cyberbeveiliging waarborgen.

Artikel 4

Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

1) "netwerk- en informatiesysteem":

   a) een elektronisch communicatienetwerk in de zin van artikel 2, lid 1, van Richtlijn (EU) 2018/1972;

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

   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 vertrouwen weerstand te bieden aan **elke gebeurtenis [...]** die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen of verzonden of verwerkte gegevens of **van** de daarmee verband houdende diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar **kan** brengen;

2a) "elektronischecommunicatiediensten": een elektronisch[...] communicatienetwerk in de zin van artikel 2, lid 4, van Richtlijn (EU) 2018/1972;

3) "cyberbeveiliging": cyberbeveiliging in de zin van artikel 2, lid 1, van Verordening (EU) 2019/881 van het Europees Parlement en de Raad[33];

4) "nationale strategie voor **cyberbeveiliging**" [...]: een samenhangend kader van een lidstaat **voor governance**, met strategische doelstellingen en prioriteiten **op het gebied van** [...] **cyberbeveiliging** [...] in die lidstaat;

5) "incident": elke 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;

5a) "grootschalig cyberbeveiligingsincident": een incident met significante gevolgen voor ten minste twee lidstaten of die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen;

---

33 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).

6) "incidentenbehandeling": alle acties en procedures die gericht zijn op het opsporen, analyseren en indammen van en de respons op een incident;

6a) "risico": de mogelijkheid van verlies of verstoring als gevolg van een incident; dit wordt uitgedrukt als een combinatie van de omvang van een dergelijk verlies of verstoring en de waarschijnlijkheid dat een dergelijk incident zich voordoet;

7) "cyberbedreiging": een cyberbedreiging in de zin van artikel 2, lid 8, van Verordening (EU) 2019/881;

7a) "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 haar gebruikers doordat zij aanzienlijke materiële of immateriële schade veroorzaakt;

8) "kwetsbaarheid": een zwakheid, vatbaarheid of gebrek van een **ICT-**activum of een systeem [...] dat door een cyberbedreiging kan worden uitgebuit;

8a) "bijna-ongeluk": een gebeurtenis die mogelijkerwijs schade had kunnen toebrengen aan de netwerk- en informatiesystemen van een entiteit of haar gebruikers, maar die met succes is voorkomen;

9) "vertegenwoordiger": elke in de Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens i) een DNS-dienstverlener, een register voor topleveldomeinnamen, een aanbieder van cloudcomputerdiensten, een aanbieder van datacentrumdiensten, een aanbieder van een netwerk voor de voor de levering van inhoud als bedoeld in punt 8 van bijlage I of ii) entiteiten als bedoeld in punt [...] 6 van bijlage II die niet in de Unie zijn gevestigd en die door een nationale bevoegde autoriteit of een CSIRT kunnen worden aangesproken in plaats van de entiteit met betrekking tot de verplichtingen van die entiteit uit hoofde van deze richtlijn;

10) "norm": een norm in de zin van artikel 2, lid 1, van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad[34];

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

12) "internetuitwisselingspunt (IXP)": een netwerkfaciliteit die de interconnectie van meer dan twee onafhankelijke netwerken (autonome systemen) mogelijk maakt, in de eerste plaats om de uitwisseling van internetverkeer te vergemakkelijken; een IXP biedt alleen interconnectie voor autonome systemen; een IXP vereist niet dat het internetverkeer dat tussen een paar deelnemende autonome systemen verloopt, via een derde autonoom systeem verloopt, noch dat het dat verkeer wijzigt of anderszins verstoort;

13) "domeinnaamsysteem (DNS)": een hiërarchisch gedistribueerd naamgevingssysteem dat de eindgebruikers in staat stelt diensten en bronnen op het internet te bereiken;

14) "DNS-dienstverlener": een entiteit die recursieve of gezaghebbende diensten op het gebied van domeinnaamomzetting **voor** [...] **gebruik door derden** verleent, **met uitzondering van root-naamservers** [...];

---

34 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).

15) "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, **behalve in situaties waarin een register topleveldomeinnamen enkel voor eigen gebruik aanwendt**;

15a) "entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen": registers voor topleveldomeinnamen, registratoren voor topleveldomeinnamen en agenten van registratoren zoals wederverkopers en aanbieders van proxydiensten;

16) "digitale dienst": een dienst in de zin van artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad[35];

16a) "vertrouwensdiensten": vertrouwensdiensten in de zin van artikel 3, lid 16, van Verordening (EU) nr. 910/2014;

[35] 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).

16b) "gekwalificeerde verleners van vertrouwensdiensten": een gekwalificeerde verlener van vertrouwensdiensten in de zin van artikel 3, lid 20, van Verordening (EU) nr. 910/2014;

17) "elektronische marktplaats": een digitale dienst in de zin van artikel 2, punt n), van Richtlijn 2005/29/EG van het Europees Parlement en de Raad[36];

18) "onlinezoekmachine": een digitale dienst in de zin van artikel 2, lid 5, van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad;[37]

19) "cloudcomputerdienst": een digitale dienst die administratie op aanvraag en brede toegang op afstand tot een schaalbare en elastische pool van gedeelde [...] computerbronnen mogelijk maakt, **ook wanneer deze over verschillende locaties verspreid zitten**;

20) "datacentrumdienst": een dienst die structuren, of groepen van structuren, omvat die bestemd zijn voor de gecentraliseerde accommodatie, de interconnectie en de exploitatie van informatietechnologie en netwerkapparatuur die diensten op het gebied van gegevens-opslag, -verwerking en -transport aanbiedt, samen met alle faciliteiten en infrastructuren voor energiedistributie en omgevingscontrole;

---

36 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 handels-praktijken") (PB L 149 van 11.6.2005, blz.22).

37 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 online-tussenhandelsdiensten (PB L 186 van 11.7.2019, blz. 57).

21) "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;

22) "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, en met name via chats, posts, video's en aanbevelingen)[...];

23) "overheidsinstantie": een entiteit die **overeenkomstig het nationale recht als zodanig in een lidstaat is erkend**, [...] 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 bij wet namens een andere entiteit met rechtspersoonlijkheid optreden**;

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

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

24) "entiteit": elke 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;

25) "essentiële entiteit": elke entiteit van een type [...] **dat in bijlage I wordt bedoeld en overeenkomstig artikel 2 bis, lid 1, als "essentieel" wordt aangeduid**;

26) "belangrijke entiteit": elke entiteit van het type [...] **dat in de bijlagen I en II wordt bedoeld en overeenkomstig artikel 2 bis, lid 2, als "belangrijk" wordt aangeduid**.

26a) "ICT-product": een ICT-product in de zin van artikel 2, lid 12, van Verordening (EU) 2019/881;

26aa) "ICT-dienst": een ICT-dienst in de zin van artikel 2, lid 13, van Richtlijn (EU) 2019/881;

26ab) "ICT-proces": een ICT-proces in de zin van artikel 2, lid 14, van Verordening (EU) 2019/881;

26ac) "aanbieder van beheerde diensten": een entiteit die diensten verleent, zoals netwerk-, applicatie-, infrastructuur- en beveiligingsdiensten, via doorlopend en regelmatig beheer, ondersteuning en actieve administratie in de gebouwen van klanten, in het datacentrum (hosting) van hun MSP of in een datacentrum van derden;

26ad) "aanbieder van beheerde beveiligingsdiensten": elke entiteit die uitbesteed toezicht en beheer van beveiligingsapparatuur en -systemen aanbiedt. Tot de gebruikelijke diensten behoren managed firewall, inbraakdetectie, virtueel private netwerk (VPN), zoeken naar zwakke plekken en virusbestrijding.

Dit omvat ook het gebruik van operationele beveiligingscentra met een hoge beschikbaarheid (van hun eigen faciliteiten of van andere aanbieders van datacentra-diensten) om 24/7 diensten te verlenen die bedoeld zijn om het aantal personeelsleden voor operationele beveiliging dat een onderneming moet aannemen, opleiden en behouden om een adequate veiligheidsmentaliteit te behouden, te verminderen.

HOOFDSTUK II

Gecoördineerde regelgevende kaders op het gebied van cyberbeveiliging

Artikel 5

Nationale cyberbeveiligingsstrategie

1. Elke lidstaat stelt een nationale cyberbeveiligingsstrategie vast waarin de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen worden gedefinieerd om een hoog niveau van cyberbeveiliging te bereiken en te handhaven. De nationale cyberbeveiligingsstrategie omvat met name de volgende zaken:

   a) [...] doelstellingen en prioriteiten van de strategie van de lidstaten inzake cyberbeveiliging;

   b) een governancekader om deze doelstellingen en prioriteiten te verwezenlijken, met inbegrip van het in lid 2 bedoelde beleid en de taken en verantwoordelijkheden van de verschillende autoriteiten en actoren die betrokken zijn bij de uitvoering van de [...] strategie;

   c) [...] richtsnoeren om in die lidstaat relevante activa vast te stellen en cyberbeveiligingsrisico's te **beoordelen** [...];

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

   e) […]

f) een beleidskader voor een betere coördinatie tussen de bevoegde autoriteiten in het kader van deze richtlijn en Richtlijn (EU) XXXX/XXXX van het Europees Parlement en de Raad[38] [richtlijn betreffende de veerkracht van kritieke entiteiten] met het oog op het delen van informatie over **cyberbeveiligingsrisico's,** [...] cyberbedreigingen **en -incidenten, evenals niet-cybergerelateerde risico's, bedreigingen en incidenten** en de uitoefening van toezichthoudende taken, **indien nodig**;

fa) beleidskader voor coördinatie en samenwerking tussen bevoegde autoriteiten uit hoofde van deze richtlijn en bevoegde autoriteiten die zijn aangewezen krachtens sectorspecifieke wetgeving.

2. In het kader van de nationale strategie inzake cyberbeveiliging stellen de lidstaten met name het volgende beleid vast:

a) een beleid dat gericht is op cyberbeveiliging in de toeleveringsketen voor ICT-producten en -diensten die door [...] entiteiten worden gebruikt voor het verlenen van hun diensten;

b) **een beleid** [...] voor het opnemen en specificeren van aan cyberbeveiliging gerelateerde eisen voor ICT-producten en -dienst**en** in overheidsopdrachten**, met inbegrip van cyberbeveiligingscertificaten**;

c) een beleid **inzake het beheer van kwetsbaarheden, dat de bevordering en vergemakkelijking van** [...] **vrijwillige** gecoördineerde bekendmaking van de kwetsbaarheid in de zin van artikel 6, **lid 1**, bevordert en faciliteert;

d) een beleid met betrekking tot het in stand houden van de algemene beschikbaarheid**,** [...] integriteit **en vertrouwelijkheid** van de openbare kern van het open internet;

e) een beleid ter bevordering en ontwikkeling van **onderwijs en opleiding,** vaardigheden, bewustmaking en onderzoeks- en ontwikkelingsinitiatieven op het gebied van cyber-beveiliging;

---

38 *[voeg de volledige titel en de publicatiegegevens van het PB in wanneer deze bekend zijn]*

f) een beleid ter ondersteuning van academische en onderzoeksinstellingen bij de ontwikkeling van instrumenten voor cyberbeveiliging en een veilige netwerk-infrastructuur;

g) een beleid, relevante procedures en passende instrumenten voor het delen van informatie ter ondersteuning van de vrijwillige uitwisseling van informatie op het gebied van cyberbeveiliging tussen bedrijven in overeenstemming met het recht van de Unie;

h) een beleid dat gericht is op de specifieke behoeften van kmo's, met name die welke buiten het toepassingsgebied van deze richtlijn vallen, met betrekking tot begeleiding en ondersteuning bij het verbeteren van hun weerbaarheid tegen cyberbedreigingen [...].

3. De lidstaten stellen de Commissie binnen drie maanden na de goedkeuring ervan in kennis van hun nationale cyberbeveiligingsstrategieën. **Daarbij** mogen de lidstaten **elementen van de strategie die verband houden met** [...] nationale veiligheid, weglaten.

4. De lidstaten beoordelen hun nationale cyberbeveiligingsstrategieën op gezette tijden en ten minste om de [...] **vijf** jaar op basis van kernprestatie-indicatoren en wijzigen deze waar nodig. Het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) helpt de lidstaten op **hun** verzoek bij de ontwikkeling van een nationale strategie en van kernprestatie-indicatoren voor de beoordeling van de strategie.

Artikel 6

Gecoördineerde bekendmaking van de kwetsbaarheid en een Europees kwetsbaarheidsregister

1. Elke lidstaat wijst een van zijn CSIRT's als bedoeld in artikel 9 aan als coördinator met het oog op een gecoördineerde bekendmaking van de kwetsbaarheid. Het aangewezen CSIRT treedt op als een betrouwbare tussenpersoon en faciliteert, waar nodig, de interactie tussen de verslagleggende entiteit**, de eigenaar van de potentiële kwetsbaarheid** en de fabrikant of aanbieder van ICT-producten of -diensten. **Elke natuurlijke of rechtspersoon kan, eventueel anoniem, een kwetsbaarheid als bedoeld in artikel 4, lid 8, melden aan het aangewezen CSIRT. Het aangewezen CSIRT zorgt voor een gedegen afhandeling van de melding en waarborgt de vertrouwelijkheid ten aanzien van de identiteit van de persoon die de kwetsbaarheid meldt.** Wanneer de gemelde kwetsbaarheid [...] **significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat**, werken de aangewezen CSIRT's van alle betrokken lidstaten**, waar nodig,** binnen het CSIRT-netwerk met **andere aangewezen CSIRT's** samen.

2. Enisa ontwikkelt en onderhoudt**, in overleg met de Samenwerkingsgroep,** een Europees kwetsbaarheidsregister. Daartoe stelt het Enisa de passende informatiesystemen, beleids-maatregelen en procedures vast en onderhoudt deze, met name om belangrijke en essentiële entiteiten en hun leveranciers van netwerk- en informatiesystemen in staat te stellen **op vrijwillige basis** de in ICT-producten of ICT-diensten aanwezige, **algemeen bekende** kwetsbaarheden bekend te maken en te registreren, en om alle belanghebbende partijen toegang te verlenen tot de informatie over de in het register opgenomen kwetsbaarheden. Het register bevat met name informatie over de kwetsbaarheid, het betrokken ICT-product of de betrokken ICT-diensten en de ernst van de kwetsbaarheid afgezet tegen de omstandigheden waaronder deze kan worden uitgebuit, de beschikbaarheid van gerelateerde patches en, bij gebrek aan beschikbare patches, richtsnoeren **van nationale bevoegde autoriteiten of CSIRT's** voor gebruikers van kwetsbare producten en diensten over de wijze waarop de risico's die voortvloeien uit bekendgemaakte kwetsbaarheden, kunnen worden beperkt. **Het Enisa zorgt ervoor dat het Europees kwetsbaarheidsregister gebruikmaakt van een veilige en veerkrachtige communicatie- en informatie-infrastructuur.**

Artikel 7

Nationale kaders voor crisisbeheer op het gebied van cyberbeveiliging

1. Elke lidstaat wijst een of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor het beheer van grootschalige cyberbeveiligingsincidenten en -crises. De lidstaten zorgen ervoor dat de bevoegde autoriteiten over voldoende middelen beschikken om de hun toegewezen taken doeltreffend en efficiënt uit te voeren. **De lidstaten zorgen voor samenhang met de bestaande kaders voor algemene crisisbeheersing.**

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

3. Elke lidstaat stelt een nationaal plan voor incidenten en crisisrespons op het gebied van cyberbeveiliging vast waarin doelstellingen en modaliteiten voor het beheer van grootschalige incidenten en crises op het gebied van cyberbeveiliging zijn vastgelegd. In het plan wordt met name het volgende bepaald:

   a) doelstellingen van nationale paraatheidsmaatregelen en -activiteiten;

   b) de taken en verantwoordelijkheden van de nationale bevoegde autoriteiten;

   c) procedures voor het beheer van cyberbeveiligingscrises**, met inbegrip van de integratie ervan in het algemene nationale kader voor crisisbeheersing** en de kanalen voor informatie-uitwisseling;

   d) paraatheidsmaatregelen, met inbegrip van oefeningen en opleidingsactiviteiten op gezette tijden;

   e) de betrokken publieke en private [...] partijen en de betrokken infrastructuur;

   f) 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 het niveau van de Unie en de ondersteuning daarvan te waarborgen.

4. De lidstaten stellen [...] de Commissie **in kennis van** de aanwijzing van hun in lid 1 bedoelde bevoegde autoriteiten en verstrekken binnen drie maanden na die aanwijzing en de vaststelling van hun nationale responsplannen **relevante informatie met betrekking tot de vereisten van lid 3 van dit artikel over** die plannen op het gebied van cyberbeveiligingsincidenten en -crises [...]. De lidstaten kunnen specifieke informatie [...] uitsluiten voor zover dit [...] noodzakelijk is om hun nationale veiligheid, **openbare veiligheid of defensie** te waarborgen.

Artikel 8

Nationale bevoegde autoriteiten en centrale contactpunten

1. Elke lidstaat wijst een of meer bevoegde autoriteiten aan die verantwoordelijk zijn voor cyberbeveiliging en voor de in hoofdstuk VI van deze richtlijn bedoelde toezichthoudende taken. De lidstaten kunnen daartoe een of meer bestaande instanties aanwijzen.

2. De in lid 1 bedoelde bevoegde autoriteiten houden toezicht op de toepassing van deze richtlijn op nationaal niveau.

3. Elke lidstaat wijst een nationaal centraal contactpunt voor cyberbeveiliging aan ("centraal contactpunt"). Wanneer een lidstaat slechts één bevoegde autoriteit aanwijst, is die bevoegde autoriteit ook het centrale contactpunt voor die lidstaat.

4. Elk centraal contactpunt oefent een verbindingsfunctie uit om de grensoverschrijdende samenwerking van de autoriteiten van zijn lidstaat met de relevante autoriteiten in andere lidstaten te waarborgen, alsmede om te zorgen voor sectoroverschrijdende samenwerking met andere nationale bevoegde autoriteiten binnen zijn lidstaat.

5. De lidstaten zien erop toe dat de in lid 1 bedoelde bevoegde autoriteiten en de 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. De lidstaten zorgen voor een doeltreffende, efficiënte en veilige samenwerking tussen de aangewezen vertegenwoordigers in de in artikel 12 bedoelde Samenwerkingsgroep.

6. Elke lidstaat stelt de Commissie onverwijld in kennis van de aanwijzing van de in lid 1 bedoelde bevoegde autoriteit en het in lid 3 bedoelde centrale contactpunt, van hun taken en van elke latere wijziging daarvan. Elke lidstaat maakt de aanwijzing ervan bekend. De Commissie publiceert de lijst van de aangewezen centrale contactpunten.

Artikel 9

Computer security incident response teams (CSIRT's)

1. Elke lidstaat wijst een of meer CSIRT's aan die voldoen aan de vereisten van artikel 10, lid 1, en die ten minste de in de bijlagen I en II bedoelde sectoren, subsectoren of entiteiten bestrijken en verantwoordelijk zijn voor de incidentenbehandeling volgens een welbepaald proces. Een CSIRT kan worden ingesteld bij een bevoegde autoriteit als bedoeld in artikel 8.

2. De lidstaten zorgen ervoor dat elk CSIRT over voldoende middelen beschikt om zijn in artikel 10, lid 2, omschreven taken doeltreffend uit te voeren. **Bij de uitvoering van deze taken kunnen CSIRT's op basis van een risicogebaseerde benadering het verlenen van bepaalde diensten aan entiteiten prioriteren.**

3. De lidstaten zorgen ervoor dat elk CSIRT over een passende, veilige en veerkrachtige communicatie- en informatie-infrastructuur beschikt om informatie uit te wisselen met essentiële en belangrijke entiteiten en andere relevante belanghebbende partijen. Daartoe zorgen de lidstaten ervoor dat de CSIRT's bijdragen aan de invoering van veilige instrumenten voor informatiedeling.

4. De CSIRT's werken samen en wisselen in voorkomend geval relevante informatie uit overeenkomstig artikel 26 met betrouwbare sectorale of sectoroverschrijdende gemeenschappen van essentiële en belangrijke entiteiten.

5. De CSIRT's nemen deel aan overeenkomstig artikel 16 georganiseerd intercollegiaal [...] **leren**.

6. De lidstaten zorgen ervoor dat hun CSIRT's doeltreffend, efficiënte n veilige samenwerken in het in artikel 13 bedoelde netwerk van CSIRT's.

7. De lidstaten stellen de Commissie onverwijld in kennis van de overeenkomstig lid 1 aangewezen CSIRT's, de overeenkomstig artikel 6, lid 1, aangewezen CSIRT-coördinator en hun respectieve taken met betrekking tot de in de bijlagen I en II bedoelde entiteiten.

8. De lidstaten kunnen bij de ontwikkeling van nationale CSIRT's de hulp van het Enisa inroepen.

Artikel 10

Eisen 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 communicatie**kanalen** [...] door zwakke punten (single points of failure) te voorkomen en beschikken over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en zij contact met anderen kunnen opnemen. De communicatiekanalen worden voorts duidelijk gespecificeerd en meegedeeld aan de gebruikersgroep en de samenwerkingspartners;

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

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

d) de CSIRT's krijgen voldoende personeel om een volcontinue beschikbaarheid te garanderen;

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

f) de CSIRT's hebben de mogelijkheid om deel te nemen aan internationale samenwerkingsnetwerken.

2. De CSIRT's hebben tot taak:

a) het monitoren van cyberbedreigingen, kwetsbaarheden en incidenten op nationaal niveau;

b) het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder essentiële en belangrijke entiteiten, evenals aan **bevoegde autoriteiten en** andere belanghebbende partijen over cyberbedreigingen, kwetsbaarheden en incidenten;

c) de respons op incidenten;

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

e) **[...]** zorgen voor het proactief scannen van de netwerk- en informatiesystemen [...] **om kwetsbaarheden met mogelijk significante gevolgen op te sporen, op voorwaarde dat er geen toegang wordt verschaft tot de netwerk- en informatiesystemen of de werking ervan niet negatief wordt beïnvloed, indien de entiteit er geen toestemming voor heeft gegeven;**

f) het deelnemen aan het CSIRT-netwerk en het verlenen van wederzijdse bijstand **overeenkomstig hun capaciteiten en bevoegdheden** aan andere leden van het netwerk op hun verzoek;

fa) indien van toepassing, optreden als coördinator voor het gecoördineerde proces van bekendmaking van kwetsbaarheden overeenkomstig artikel 6, lid 1, dat met name voorziet in het faciliteren van de interactie tussen de rapporterende entiteiten, de eigenaar van de mogelijke kwetsbaarheid en de producent of aanbieder van ICT-producten of -diensten in gevallen waarin dit nodig is, het identificeren van en contact opnemen met de betrokken entiteiten, het ondersteunen van rapporterende entiteiten, het onderhandelen over bekendmakingstermijnen en het beheren van kwetsbaarheden die gevolgen hebben voor meerdere organisaties (gecoördineerde bekendmaking van kwetsbaarheden voor meerdere partijen).

3. De CSIRT's brengen samenwerkingsverbanden tot stand met relevante actoren in de private sector, teneinde de doelstellingen van de richtlijn beter te verwezenlijken.

3a. CSIRT's kunnen samenwerkingsverbanden aangaan met nationale CSIRT's van derde landen. In het kader van deze samenwerking kunnen zij relevante informatie, waaronder persoonsgegevens, uitwisselen overeenkomstig het Unierecht inzake gegevensbescherming.

4. Om de samenwerking te faciliteren, bevorderen de CSIRT's de invoering en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën met betrekking tot de volgende zaken:

a) procedures voor de incidentenbehandeling;

b) crisisbeheer op het gebied van cyberbeveiliging;

c) gecoördineerde bekendmaking van kwetsbaarheden.

Artikel 11

Samenwerking op nationaal niveau

1. Wanneer zij gescheiden zijn, werken de in artikel 8 bedoelde bevoegde autoriteiten, het centrale contactpunt en het 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 ofwel hun bevoegde autoriteiten, ofwel hun CSIRT's meldingen ontvangen over incidenten en significante cyberbedreigingen en bijna-ongelukken die uit hoofde van deze richtlijn worden ingediend. Wanneer een lidstaat besluit dat zijn CSIRT's die meldingen niet ontvangen, krijgen de CSIRT's, voor zover dat nodig is voor de uitvoering van hun taken, toegang tot gegevens over de door de essentiële of belangrijke entiteiten gemelde incidenten, overeenkomstig artikel 20.

3. Elke lidstaat zorgt ervoor dat zijn bevoegde autoriteiten of CSIRT's zijn centrale contactpunt in kennis stellen van meldingen van incidenten, significante cyberbedreigingen en bijna-ongelukken die op grond van deze richtlijn worden ingediend.

4. Voor zover dat nodig is om de in deze richtlijn vastgestelde taken en verplichtingen doeltreffend uit te voeren, zorgen de lidstaten voor passende samenwerking tussen de bevoegde autoriteiten, CSIRT's en centrale contactpunten, evenals rechtshandhavings-instanties, gegevensbeschermingsautoriteiten en de in die lidstaat **bevoegde** autoriteiten die [...] overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten [...]] zijn **aangewezen**, **de bevoegde autoriteiten uit hoofde van Uitvoeringsverordening (EU) 2019/1583 van de Commissie, de nationale regulerende instanties die overeenkomstig Richtlijn (EU) 2018/1972 zijn aangewezen, de nationale autoriteiten die uit hoofde artikel 17 van Verordening (EU) nr. 910/2014 zijn aangewezen,** [...] de nationale financiële autoriteiten die overeenkomstig Verordening (EU) XXXX/XXXX van het Europees Parlement en de Raad [de DORA-verordening] zijn aangewezen, **evenals bevoegde autoriteiten die door andere sectorspecifieke rechts-handelingen van de Unie zijn aangewezen**.

5. De lidstaten zorgen ervoor dat hun **uit hoofde van deze richtlijn** bevoegde autoriteiten **en de uit hoofde van Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] aangewezen bevoegde autoriteiten** regelmatig [...] informatie **uitwisselen** [...] over **de identificatie van kritieke entiteiten,** cyberbeveiligingsrisico's, **cyberbedreigingen en -incidenten, evenals niet-cybergerelateerde risico's, bedreigingen en incidenten** die van invloed zijn op essentiële entiteiten die overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] als kritiek zijn aangemerkt, **[**of als entiteiten die gelijkwaardig zijn aan kritieke entiteiten,**]** alsmede over de maatregelen die [...] zijn genomen naar aanleiding van deze risico's en incidenten. **De lidstaten zorgen er ook voor dat de bevoegde autoriteiten uit hoofde van deze richtlijn** [...] **en de bevoegde autoriteiten die zijn aangewezen uit hoofde van Verordening XXXX/XXXX [DORA-verordening], Richtlijn 2018/1972 en Verordening (EU) nr. 910/2014 regelmatig relevante informatie uitwisselen.**

Met betrekking tot verleners van vertrouwensdiensten, en [...] met name [...] wanneer die toezichthoudende rol uit hoofde van deze richtlijn wordt toegewezen aan een ander orgaan dan de krachtens Verordening (EU) nr. 910/2014 aangewezen toezichthoudende organen, werken de nationale bevoegde autoriteiten in het kader van deze richtlijn nauw en tijdig samen en wisselen zij de nodige informatie uit om ervoor te zorgen dat er doeltreffend toezicht wordt gehouden op verleners van vertrouwensdiensten en dat deze zich houden aan de vereisten van deze richtlijn en Verordening [XXXX/XXXX] **en, in voorkomend geval, informeert de nationale bevoegde autoriteit uit hoofde van deze richtlijn onverwijld het toezichthoudend orgaan van de eIDAS-verordening over alle gemelde significante cyberbedreigingen of -incidenten met gevolgen voor vertrouwensdiensten**.

5a. Teneinde [...] de melding van incidenten te vereenvoudigen, kunnen de lidstaten een centraal contactpunt instellen voor alle meldingen die, in voorkomend geval, op grond van deze richtlijn en ook op grond van Verordening (EU) 2016/679 en Richtlijn 2002/58/EG vereist zijn. De lidstaten kunnen het centrale toegangspunt gebruiken voor kennisgevingen die op grond van andere sectorspecifieke rechtshandelingen van de Unie vereist zijn. Dit centrale toegangspunt doet geen afbreuk aan de toepassing van de bepalingen van Verordening (EU) 2016/679 en Richtlijn 2002/58/EG, met name die welke betrekking hebben op onafhankelijke toezichthoudende autoriteiten.

HOOFDSTUK III

EU-Samenwerking

Artikel 12

Samenwerkingsgroep

1. Om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te faciliteren [...], **en om het vertrouwen te versterken** [...], wordt er een Samenwerkingsgroep opgericht.

2. De Samenwerkingsgroep voert zijn taken uit op basis van de in lid 6 bedoelde tweejaarlijkse werkprogramma's.

3. De Samenwerkingsgroep bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het 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) XXXX/XXXX [DORA-verordening]** aangewezen bevoegde autoriteiten kunnen **overeenkomstig artikel 42, lid 1, van Verordening (EU) XXXX/XXXX [DORA-verordening]** [...] deelnemen aan de activiteiten van de Samenwerkingsgroep.

   Waar nodig kan de Samenwerkingsgroep vertegenwoordigers van belanghebbenden uitnodigen om deel te nemen aan zijn werkzaamheden.

   De Commissie verzorgt het secretariaat.

4. De Samenwerkingsgroep heeft tot taak:

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

   aa) richtsnoeren te verstrekken met betrekking tot de ontwikkeling en uitvoering van beleid inzake gecoördineerde bekendmaking van kwetsbaarheden als bedoeld in artikel 5, lid 2, punt c),en artikel 6, lid 1;

b) beste praktijken en informatie uit te wisselen met betrekking tot de uitvoering van deze richtlijn, onder meer met betrekking tot cyberbedreigingen, incidenten, kwetsbaarheden, bijna-ongelukken, bewustmakingsinitiatieven, opleidingen, oefeningen en vaardigheden, capaciteitsopbouw en normen en technische specificaties;

c) advies uit te wisselen en samenwerken met de Commissie rond nieuwe beleidsinitiatieven op het gebied van cyberbeveiliging;

d) advies uit te wisselen en samenwerken met de Commissie rond ontwerpen van uitvoeringshandelingen [...] van de Commissie die overeenkomstig deze richtlijn worden vastgesteld;

e) beste praktijken en informatie uit te wisselen met de betrokken instellingen, organen en instanties van de Unie;

ea) van gedachten te wisselen over de uitvoering van sectorale wetgeving met cyberbeveiligingsaspecten;

f) de verslagen over het in artikel 16, lid 7, bedoelde intercollegiaal [...] **leren** te bespreken;

g) de resultaten van de in artikel 34 bedoelde **ervaringen** [...] van het gemeenschappelijk toezicht in grensoverschrijdende gevallen te bespreken;

h) strategische richtsnoeren aan het CSIRT-netwerk **en EU–CyCLONe** te verstrekken over specifieke nieuwe kwesties;

ha) van gedachten te wisselen over de beleidsfollow-up van grootschalige cyberincidenten op basis van de lessen die zijn getrokken uit het CSIRT-netwerk en EU-CyCLONe;

i) bij te dragen tot de cyberbeveiligingscapaciteiten in de hele Unie door de uitwisseling van nationale ambtenaren te faciliteren via een programma voor capaciteitsopbouw waarbij personeel van de bevoegde autoriteiten van de lidstaten of van de CSIRT's betrokken is;

j) regelmatige gezamenlijke bijeenkomsten te organiseren met private belanghebbenden uit de hele Unie om de activiteiten van de groep te bespreken en input te verzamelen over nieuwe beleidsuitdagingen;

k) de werkzaamheden in verband met cyberbeveiligingsoefeningen, met inbegrip van het werk van het Enisa, te bespreken**;**

ka) het mechanisme voor intercollegiaal leren overeenkomstig artikel 16 van deze richtlijn vast te stellen.

5. De Samenwerkingsgroep kan het CSIRT-netwerk verzoeken om een technisch verslag over geselecteerde onderwerpen.

6. Uiterlijk ... [24 maanden na de datum van inwerkingtreding van deze richtlijn] en vervolgens om de twee jaar stelt de Samenwerkingsgroep een werkprogramma op met betrekking tot de acties die moeten worden ondernomen om de doelstellingen en taken van de groep uit te voeren. Het tijdschema van het eerste programma dat in het kader van deze richtlijn wordt vastgesteld, wordt afgestemd op het tijdschema van het laatste in het kader van Richtlijn (EU) 2016/1148 vastgestelde programma.

7. De Commissie kan uitvoeringshandelingen vaststellen tot vaststelling van de voor de werking van de Samenwerkingsgroep noodzakelijke procedurele regelingen. Deze uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 37, lid 2, bedoelde onderzoeksprocedure.

8. De Samenwerkingsgroep komt regelmatig en ten minste eenmaal per jaar bijeen met de krachtens Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] opgerichte groep voor de veerkracht van kritieke entiteiten om de strategische samenwerking en de uitwisseling van informatie te bevorderen en te **faciliteren**.

Artikel 13

CSIRT-netwerk

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

2. Het CSIRT-netwerk bestaat uit vertegenwoordigers van de CSIRT's van de lidstaten**, aangewezen overeenkomstig artikel 9,** en van CERT-EU. De Commissie neemt als waarnemer deel aan het CSIRT-netwerk. Het Enisa verzorgt het secretariaat en ondersteunt de samenwerking tussen de CSIRT's actief.

3. Het CSIRT-netwerk heeft tot taak:

   a) informatie over de capaciteiten van CSIRT's uit te wisselen;

   b) relevante informatie uit te wisselen over incidenten, bijna-ongelukken, cyberbedreigingen, risico's en kwetsbaarheden;

ba) informatie uit te wisselen over publicaties en aanbevelingen op het gebied van cyberbeveiliging;

bb) technische oplossingen te delen die de technische afhandeling van incidenten faciliteren;

bc) beste praktijken, instrumenten en processen met betrekking tot de taken van de CSIRT's uit te wisselen;

c) op verzoek van een [...] **lid** van het CSIRT-netwerk dat mogelijkerwijs door een incident wordt getroffen, informatie uit te wisselen en te bespreken met betrekking tot dat incident en de daarmee samenhangende cyberbedreigingen, risico's en kwetsbaarheden;

d) op verzoek van een [...] **lid** van het CSIRT-netwerk, een gecoördineerde respons op een incident dat binnen het rechtsgebied van die lidstaat is vastgesteld, te bespreken en waar mogelijk uit te voeren;

e) steun te verlenen aan de lidstaten bij de aanpak van grensoverschrijdende incidenten in het kader van deze richtlijn;

f) samen te werken met**, beste praktijken uit te wisselen** en bijstand te verlenen aan de in artikel 6 bedoelde aangewezen CSIRT's met betrekking tot het beheer van [...] gecoördineerde bekendmaking van kwetsbaarheden die van invloed zijn op meerdere fabrikanten of aanbieders van ICT-producten, ICT-diensten en ICT-processen die in verschillende lidstaten zijn gevestigd;

g) verdere vormen van operationele samenwerking te bespreken en te identificeren, ook met betrekking tot:

i) categorieën van cyberbedreigingen en -incidenten;

ii) vroegtijdige waarschuwingen;

iii) wederzijdse bijstand;

iv) beginselen en modaliteiten voor de coördinatie in verband met grensoverschrijdende risico's en incidenten;

v) een bijdrage aan het nationale incident- en crisisresponsplan op het gebied van cyberbeveiliging als bedoeld in artikel 7, lid 3, **op verzoek van een lidstaat**;

h) de Samenwerkingsgroep te informeren over zijn activiteiten en over de verdere vormen van operationele samenwerking die op grond van punt g) worden besproken, waarbij zo nodig om richtsnoeren in dat verband wordt verzocht;

i) de balans op te maken van cyberbeveiligingsoefeningen, ook van de door het Enisa georganiseerde oefeningen;

j) op verzoek van een individuele CSIRT, de capaciteiten en de paraatheid van die CSIRT te bespreken;

k) samen te werken en informatie uit te wisselen met regionale en uniale centra voor beveiligingsoperaties ("Security Operations Centres" – SOC's) om het gemeenschappelijk situationeel bewustzijn inzake incidenten en bedreigingen in de hele Unie te verbeteren;

l) de verslagen te bespreken van het in artikel 16, lid 7, bedoelde intercollegiaal [...] **leren**;

m) richtsnoeren uit te vaardigen om de convergentie van de operationele praktijken met betrekking tot de toepassing van de bepalingen van dit artikel inzake operationele samenwerking te faciliteren.

4. Met het oog op de in artikel 35 bedoelde evaluatie en uiterlijk [24 maanden na de datum van inwerkingtreding van deze richtlijn], en vervolgens om de twee jaar, beoordeelt het CSIRT-netwerk de voortgang van de operationele samenwerking en stelt het een verslag op. In het verslag worden met name conclusies getrokken over de resultaten van het in artikel 16 bedoelde intercollegiaal **leren** [...] met betrekking tot de nationale CSIRT's, met inbegrip van conclusies en aanbevelingen, die op grond van dit artikel worden uitgevoerd. Dit verslag wordt ook aan de Samenwerkingsgroep voorgelegd.

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

6. Het CSIRT-netwerk werkt samen met het EU-CyCLONe op basis van overeengekomen procedurele regelingen.

Artikel 14

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

1. Om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises op operationeel niveau te ondersteunen en te zorgen voor een regelmatige uitwisseling van informatie tussen de lidstaten en de instellingen, organen en agentschappen van de Unie, wordt hierbij het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) opgericht.

2. Het EU-CyCLONe bestaat uit de vertegenwoordigers van de overeenkomstig artikel 7 aangewezen autoriteiten voor **cyber**crisisbeheer van de lidstaten[...]. **De Commissie neemt als waarnemer deel aan de activiteiten van het netwerk.** Het Enisa verzorgt het secretariaat van het netwerk en ondersteunt de veilige uitwisseling van informatie **en voorziet in de nodige instrumenten ter ondersteuning van de samenwerking tussen de lidstaten met het oog op een veilige uitwisseling van informatie.**

Waar nodig kan het EU-CyCLONe vertegenwoordigers van belanghebbenden uitnodigen om deel te nemen aan zijn werkzaamheden.

3. Het 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 te ontwikkelen [...] voor grootschalige [...] cyberbeveiligingsincidenten en -crises;

ba) de gevolgen en de impact van relevante grootschalige cyberbeveiligingsincidenten te beoordelen en mogelijke risicobeperkende maatregelen voor te stellen;

c) **het beheer van** grootschalige cyberbeveiligingsincidenten en -crises [...] te coördineren en de besluitvorming op politiek niveau met betrekking tot dergelijke incidenten en crises te ondersteunen;

d) **op verzoek van een lidstaat zijn** in artikel 7, lid **3**[...]) bedoelde nationale respons-plannen op het gebied van cyberbeveiligingsincidenten en **-crises** te bespreken**;**[...]

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

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

6. Het EU-CyCLONe werkt samen met het CSIRT-netwerk op basis van overeengekomen procedurele regelingen.

7. Het EU-CyCLONe dient uiterlijk [24 maanden na de datum van inwerkingtreding van deze richtlijn] bij het Europees Parlement en de Raad een verslag in met een beoordeling van zijn werkzaamheden.

Artikel 14 bis

Internationale samenwerking

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 het EU-CyCLONe mogelijk maken en organiseren, overeenkomstig het recht van de Unie inzake gegevensbescherming.

Artikel 15

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

1. Het Enisa stelt in samenwerking met de Commissie **en de Samenwerkingsgroep** een tweejaarlijks verslag op over de stand van zaken op het gebied van cyberbeveiliging in de Unie. Het [...] verslag [...] omvat **met name**[...]:

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

   a) [...] **een beoordeling van de** ontwikkeling van cyberbeveiligingscapaciteiten in de publieke en private sector**en** in de hele Unie;

   b) […]

   c) **een geaggregeerde beoordeling op basis van kwantitatieve en kwalitatieve indicatoren** van de cyberbeveiliging[...], die voorziet in een [...]**overzicht** van het maturiteitsniveau van de cyberbeveiligingsvermogens**, met inbegrip van sectorspecifieke capaciteiten.**

2. Het verslag bevat specifieke beleidsaanbevelingen voor het verhogen van het cyber-beveiligingsniveau in de Unie en een samenvatting van de bevindingen voor de specifieke periode uit de technische situatieverslagen inzake de EU-cyberbeveiliging van het Agentschap, die overeenkomstig artikel 7, lid 6, van Verordening (EU) 2019/881 door het Enisa zijn opgesteld.

Artikel 16

Intercollegiaal leren

1. **Met het oog op het vergroten van het wederzijds vertrouwen, het bereiken van een hoog gezamenlijk niveau van cyberbeveiliging, evenals het versterken van de cyber-beveiligingscapaciteiten van de lidstaten en van beleidsmaatregelen die nodig zijn voor de doeltreffende uitvoering van deze richtlijn,** [...] stelt de **Samenwerkingsgroep**, [...] **met de steun van de Commissie en** na raadpleging van [...] het Enisa, **en, waar nodig, het CSIRT-netwerk,** uiterlijk **24 [...]** maanden na de inwerkingtreding van deze richtlijn, de methode [...] vast **voor een objectief, niet-discriminerend en eerlijk** systeem [...] voor intercollegiaal [...] **leren in verband met** de [...] **uitvoering van deze richtlijn** door de lidstaten. **Deelname aan het intercollegiaal leren is vrijwillig.** Het **systeem zal uit beoordelingsrondes bestaan** [...] die worden uitgevoerd door deskundigen op het gebied van cyberbeveiliging, [...] afkomstig uit de lidstaten [...], en zal betrekking hebben op [...] een of meer van de volgende zaken:

   i) de [...] uitvoering van de in de artikelen 18 en 20 bedoelde vereisten inzake het risicobeheer en de rapportageverplichtingen op het gebied van cyberbeveiliging;

   ii) de [...] capaciteiten, met inbegrip van de beschikbare [...] middelen, en [...] de uitoefening van de taken van de **in artikel 8 bedoelde** nationale bevoegde autoriteiten **en in artikel 9 bedoelde CSIRT's**;

[…]

i**ii**[...]) de [...] **uitvoering** van de in artikel 34 bedoelde wederzijdse bijstand;

iv) de [...] **uitvoering** van het in artikel 26 [...] bedoelde kader voor de uitwisseling van informatie.

2. **De criteria op basis waarvan de lidstaten deskundigen aanwijzen die in aanmerking komen om deel te nemen aan de rondes intercollegiaal leren, zijn** [...] objectief, niet-discriminerend, eerlijk en transparant [...] **en worden opgenomen in de in lid 1 bedoelde methode**. Het Enisa en de Commissie [...] **kunnen** deskundigen aanwijzen om als waarnemers deel te nemen aan de [...] **rondes intercollegiaal leren**. […]

3. [...] .

3a. Voor de start van de rondes intercollegiaal leren kunnen de lidstaten een zelfbeoordeling uitvoeren van de aspecten die onder die specifieke ronde intercollegiaal leren vallen en deze zelfbeoordeling aan de in lid 2 bedoelde aangewezen deskundigen verstrekken.

4. Het intercollegiaal[...] **leren** [...] **kan** [...] **fysieke** of virtuele bezoeken ter plaatse en uitwisselingen elders omvatten. Met het oog op het beginsel van goede samenwerking verstrekken de lidstaten [...] **die aan het intercollegiaal leren deelnemen** de aangewezen deskundigen de [...] informatie die nodig is voor de beoordeling [...]**, onverminderd de nationale of Uniewetgeving betreffende de bescherming van vertrouwelijke of gerubriceerde informatie of de bescherming van essentiële staatsfuncties, zoals de nationale veiligheid.** Alle informatie die via het intercollegiaal [...] **leren** wordt verkregen, wordt uitsluitend voor dat doel gebruikt. De deskundigen die aan het intercollegiaal [...] **leren** deelnemen, maken geen gevoelige of vertrouwelijke informatie die zij in **dat kader** [...] hebben verkregen, bekend aan derden. **De lidstaat die aan het intercollegiaal leren deelneemt, kan bezwaar maken tegen de aanwijzing van bepaalde deskundigen op basis van naar behoren gemotiveerde redenen die aan de Samenwerkingsgroep worden meegedeeld.**

5. Na **een behandeling in een ronde intercollegiaal leren** [...] worden dezelfde aspecten niet meer behandeld in verdere **rondes** intercollegiaal [...] **leren voor de** [...] **deelnemende** lidstat**en** gedurende de [...] **vier** jaar die volgen op de afsluiting van **die** [...] **ronde** intercollegiaal [...] **leren**, **tenzij de betrokken lidstaat hierom vraagt of ermee instemt op voorstel** [...] van de **Samenwerkingsgroep[...].**

6. […]

7. Deskundigen die deelnemen aan **rondes** intercollegiaal [...] **leren** stellen verslagen op over de bevindingen en conclusies van de [...] **beoordelingen**. **De lidstaten mogen opmerkingen maken over hun respectieve ontwerpverslagen, die bij het verslag worden gevoegd.** Het **eind**verslag wordt ingediend bij [...] de Samenwerkingsgroep[...]. **De lidstaten kunnen beslissen om hun respectieve verslagen openbaar te maken.**

HOOFDSTUK IV

Verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging

AFDELING I

Risicobeheer en rapportage op het gebied van cyberbeveiliging

Artikel 17

Governance

1. De lidstaten zorgen ervoor dat de beheersorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 18, [...] **toezien** op de uitvoering ervan en verantwoordelijk [...] **kunnen worden gesteld** voor de niet-naleving door de entiteiten van de verplichtingen uit hoofde van dit artikel.

   De toepassing van dit lid laat de nationale wetgeving van de lidstaten met betrekking tot de aansprakelijkheidsregels in openbare instanties en de aansprakelijkheid van ambtenaren en gekozen en benoemde overheidsfunctionarissen onverlet.

2. De lidstaten zorgen ervoor dat de leden van het beheersorgaan regelmatig [...] opleidingen **moeten** volgen om voldoende kennis en vaardigheden te verwerven om risico's en beheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de activiteiten van de entiteit te kunnen opsporen en beoordelen.

Artikel 18

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1**a. In deze richtlijn wordt een "alle risico's"-benadering gevolgd die betrekking heeft op de bescherming van netwerk- en informatiesystemen en hun fysieke omgeving tegen elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens, of van diensten die door of via netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen.**

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten bij het verlenen van hun diensten gebruiken, te beheersen. Rekening houdend met de stand van de techniek **en de uitvoerings-kosten** zorgen deze maatregelen voor een beveiligingsniveau van de netwerk- en informatie-systemen dat is afgestemd op het aanwezige risico. **Bij de beoordeling van de evenredigheid van deze maatregelen wordt terdege rekening gehouden met de mate waarin de entiteit is blootgesteld aan risico's, de omvang van de entiteit, de waarschijnlijkheid dat incidenten zich voordoen en de ernst ervan. Gezien het niveau en de aard van het risico voor de samenleving in geval van incidenten die essentiële dan wel belangrijke entiteiten treffen, kunnen aan belangrijke entiteiten minder strenge maatregelen voor het beheer van cyberbeveiligingsrisico's worden opgelegd dan aan essentiële entiteiten.**

2. De in lid 1 bedoelde maatregelen omvatten ten minste het volgende:

a) risicoanalyse en beleid inzake de beveiliging van informatiesystemen;

b) incidentenbehandeling (preventie en opsporing van, [...] respons op **en herstel na** incidenten);

c) bedrijfscontinuïteit 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, zoals leveranciers van diensten op het gebied van gegevensopslag en -verwerking of beheerde beveiligingsdiensten;

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) **beleid inzake** het gebruik van cryptografie en versleuteling;

ga) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en vermogensbeheer.

3. De lidstaten zorgen ervoor dat de entiteiten, wanneer zij de in lid 2, punt d), bedoelde passende maatregelen overwegen, rekening **moeten** 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 de in lid 2, punt d), bedoelde passende maatregelen overwegen, rekening moeten houden met de resultaten van de overeenkomstig artikel 19, lid 1, uitgevoerde gecoördineerde risicobeoordelingen.**

4. De lidstaten zien erop toe dat wanneer een entiteit vaststelt dat haar diensten of taken niet in overeenstemming zijn met de in lid 2 vastgestelde eisen, zij onverwijld alle nodige corrigerende maatregelen neemt om de betrokken dienst in overeenstemming te brengen.

5. De Commissie kan uitvoeringshandelingen vaststellen om de technische en methodologische specificaties, **en, zo nodig, de sectorale kenmerken** van de in lid 2 **van dit artikel** bedoelde elementen vast te stellen. **De Commissie stelt uiterlijk [18 maanden na de inwerking-treding van deze richtlijn] uitvoeringshandelingen vast om de technische en methodologische specificaties vast te stellen voor de in artikel 24, lid 1, bedoelde entiteiten en de in punt 8 van bijlage I bedoelde verleners van vertrouwensdiensten. Die uitvoeringshandelingen worden volgens de in artikel 37, lid 2, bedoelde onderzoeks-procedure vastgesteld.** Bij de voorbereiding van deze **uitvoerings**handelingen [...] **volgt** de Commissie [...] zoveel mogelijk de internationale en Europese normen en de relevante technische specificaties**, en wisselt zij overeenkomstig artikel 12, lid 4, punt d), advies uit met de Samenwerkingsgroep en het Enisa over de ontwerpuitvoeringshandelingen**.

6. […]

Artikel 19

Gecoördineerde risicobeoordelingen van kritieke toeleveringsketens in de EU

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

2. Na overleg met de Samenwerkingsgroep en het Enisa stelt de Commissie vast welke specifieke kritieke ICT-diensten, -systemen of -producten aan de in lid 1 bedoelde gecoördineerde risicobeoordeling kunnen worden onderworpen.

Artikel 20

Rapportageverplichtingen

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten aan de bevoegde autoriteiten of het CSIRT overeenkomstig de leden 3 en 4 onverwijld elk incident melden dat aanzienlijke gevolgen heeft voor de verlening van hun diensten. In voorkomend geval melden deze entiteiten de ontvangers van hun diensten onverwijld **de** incidenten die een nadelige invloed kunnen hebben op de verlening van die dienst. De lidstaten zorgen ervoor dat deze entiteiten onder meer alle informatie rapporteren die de bevoegde autoriteiten of het CSIRT in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen. **Het melden zelf mag de meldende entiteit niet aan een verhoogde aansprakelijkheid onderwerpen.**

2. […]

Indien van toepassing stellen [...] **de essentiële en belangrijke** entiteiten de ontvangers van hun diensten die mogelijkerwijs door een significante cyberbedreiging worden getroffen, onverwijld in kennis van de maatregelen of middelen die deze ontvangers kunnen nemen als antwoord op die bedreiging. In voorkomend geval stellen de entiteiten deze ontvangers ook van de bedreiging zelf in kennis. [...] **Het melden zelf** mag de meldende entiteit niet aan een verhoogde aansprakelijkheid onderwerpen.

3. Een incident wordt als significant beschouwd als:

   a) het incident een [...] **ernstige** operationele verstoring **van de dienst** of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken;

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

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

   a) onverwijld en in ieder geval binnen 24 uur nadat het incident bekend is geworden, **als vroegtijdige waarschuwing** een eerste melding indienen, waarin, indien van toepassing, wordt aangegeven of het incident vermoedelijk door een onwettige of kwaadwillige handeling is veroorzaakt;

   b) op verzoek van een bevoegde autoriteit of een CSIRT, een tussentijds verslag indienen over relevante updates van de situatie;

   c) uiterlijk één maand na de indiening van [...] de in punt a) bedoelde [...] **eerste melding**, een eindverslag indienen waarin ten minste het volgende is opgenomen:

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

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

      iii) toegepaste en lopende beperkende maatregelen.

   De lidstaten bepalen dat de betrokken entiteit in naar behoren gemotiveerde gevallen en in overleg met de bevoegde autoriteiten of het CSIRT kan afwijken van de in de punten a) en c) vastgestelde termijnen. **Afwijken van de in punt c) bedoelde termijn kan met name gerechtvaardigd zijn wanneer het incident nog gaande is.**

5. De nationale bevoegde autoriteiten of het CSIRT verstrekken [...] na ontvangst van de eerste melding als bedoeld in lid 4, punt a), **onverwijld** een antwoord aan de meldende entiteit, met inbegrip van een eerste feedback over het incident en, op verzoek van de entiteit, richtsnoeren voor de uitvoering van mogelijke risicobeperkende maatregelen. Wanneer het CSIRT de in de lid 1 bedoelde melding niet 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 incident van criminele aard is, geven de nationale bevoegde autoriteiten of het CSIRT ook richtsnoeren voor het melden van het incident aan de rechtshandhavings-instanties.

6. In voorkomend geval, en met name wanneer het in lid 1 bedoelde incident betrekking heeft op twee of meer lidstaten, stelt de bevoegde autoriteit**,** [...] het CSIRT **of het centrale contact-punt** de andere getroffen lidstaten en het Enisa in kennis van het incident. **Hierbij wordt op zijn minst informatie verstrekt over de in lid 4 van dit artikel bedoelde elementen.** Daarbij beschermen de bevoegde autoriteiten, de CSIRT's en de centrale contactpunten, in overeenstemming met het recht van de Unie of de nationale wetgeving die in overeenstem-ming is met het recht van de Unie, de beveiligings- en commerciële belangen van de entiteit, alsmede de vertrouwelijkheid van de verstrekte informatie.

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

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

9. Het centrale contactpunt dient [...] **om de zes maanden** bij het Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over incidenten, significante cyberbedreigingen en bijna-ongelukken die overeenkomstig [...] lid 1 [...] en overeenkomstig artikel 27 zijn gemeld. Om bij te dragen tot het verstrekken van vergelijkbare informatie kan het Enisa technische richtsnoeren geven over de parameters van de informatie in het samenvattend verslag. **Het Enisa stelt de Samenwerkingsgroep en het netwerk van CSIRT's om de zes maanden in kennis van zijn bevindingen over de ontvangen meldingen.**

10. De bevoegde autoriteiten verstrekken de overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] aangewezen bevoegde autoriteiten informatie over incidenten en cyberbedreigingen die overeenkomstig de leden 1 en 2 zijn gemeld door essentiële entiteiten die overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] zijn geïdentificeerd als kritieke entiteiten, **[**of als entiteiten die gelijkwaardig zijn aan kritieke entiteiten**]**.

11. De Commissie kan uitvoeringshandelingen vaststellen waarin het soort informatie, het formaat en de procedure van een overeenkomstig de leden 1 en 2 ingediende melding nader worden gespecificeerd. De Commissie kan ook uitvoeringshandelingen vaststellen om de gevallen waarin een incident als significant wordt beschouwd als bedoeld in lid 3, nader te specificeren. Die uitvoeringshandelingen worden volgens de in artikel 37, lid 2, bedoelde onderzoeksprocedure vastgesteld.

Artikel 21

Gebruik van Europese cyberbeveiligingscertificeringsregelingen

1. Om aan te tonen dat aan bepaalde eisen van artikel 18 wordt voldaan, kunnen de lidstaten eisen dat [...] entiteiten [...] **gebruikmaken van specifieke** ICT-producten, [...]-diensten en [...]-processen **die zijn gecertificeerd** in het kader van specifieke Europese cyberbeveiligings-certificeringsregelingen die op grond van artikel 49 van Verordening (EU) 2019/881 zijn vastgesteld. De **ICT-**producten, **-**diensten en **-**processen die aan certificering onderworpen zijn, kunnen door een essentiële of belangrijke entiteit worden ontwikkeld of bij derden worden ingekocht.

2. De Commissie [...] kan uitvoeringshandelingen vaststellen waarin wordt bepaald welke categorieën van essentiële **of belangrijke** entiteiten verplicht zijn om **gebruik te maken van gecertificeerde ICT-producten, -diensten en -processen of** een certificaat te verkrijgen, en uit hoofde van welke specifieke**, op grond van artikel 49 van Verordening (EU) 2019/881 vastgestelde** Europese cyberbeveiligingscertificeringsregelingen [...]. **Die uitvoerings-handelingen** worden volgens **de in artikel 37, lid 2, bedoelde onderzoeksprocedure vastgesteld**. **Bij de voorbereiding van deze uitvoeringshandelingen handelt de Commissie overeenkomstig artikel 56 van Verordening (EU) 2019/881 als volgt:**

   i) zij houdt rekening met de gevolgen die de maatregelen hebben voor de fabrikanten of aanbieders van zulke ICT-producten, -diensten of -processen en voor de gebruikers in termen van de kosten van die maatregelen, de maatschappelijke of economische voordelen die voortvloeien uit de verwachte betere beveiliging van de beoogde ICT-producten, -diensten of -processen, en de beschikbaarheid van alternatieven op de markt;

   ii) zij voert een open, transparant en inclusief overleg met alle betrokken belang-hebbenden en lidstaten;

iii) zij houdt rekening met eventuele uitvoeringstermijnen, overgangs-maatregelen en overgangstermijnen, in het bijzonder betreffende de mogelijke gevolgen van de maatregelen voor de fabrikanten of aanbieders van ICT- producten, -diensten en -processen of voor de gebruikers daarvan, met name kleine en middelgrote ondernemingen;

iv) zij houdt rekening met het bestaan en de uitvoering van de desbetreffende wetgeving van de lidstaten.

3. De Commissie kan het Enisa verzoeken een potentiële regeling op te stellen **of een bestaande Europese cyberbeveiligingscertificeringsregeling te herzien** overeenkomstig artikel 48, lid 2, van Verordening (EU) 2019/881 in gevallen waarin geen passende Europese cyber-beveiligingscertificeringsregeling voor de toepassing van lid 2 **van dit artikel** beschikbaar is.

Artikel 22

Normalisatie

1. Om de convergente uitvoering van artikel 18, 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 of internationaal aanvaarde normen en specificaties die relevant zijn voor de beveiliging van netwerk- en informatiesystemen.

2. Het Enisa stelt in samenwerking met de lidstaten 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 de nationale normen van de lidstaten, die het mogelijk maken deze gebieden te bestrijken.

Artikel 23

Databases van domeinnamen en registratiegegevens

1. Om bij te dragen aan de beveiliging, stabiliteit en veerkracht van het DNS zorgen de lidstaten ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, met de nodige zorgvuldigheid nauwkeurige en volledige domeinnaamregistratiegegevens verzamelen en bijhouden in een speciale databasefaciliteit [...] **overeenkomstig** de EU-wetgeving inzake gegevensbescherming voor wat betreft gegevens die persoonsgegevens zijn.

2. De lidstaten zorgen ervoor dat de in lid 1 bedoelde databases met gegevens over de registratie van domeinnamen relevante informatie bevatten om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen beheren, te identificeren en te contacteren**, waaronder ten minste de volgende gegevens:**

   a) domeinnaam;

   b) datum van registratie;

   c) gegevens van de registrant, met inbegrip van:

      i) voor natuurlijke personen - voornaam, achternaam en e-mailadres;

      ii) voor rechtspersonen - naam en e-mailadres.

3. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de instanties die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, over beleidslijnen en procedures beschikken om ervoor te zorgen dat de databases juiste en volledige informatie bevatten. De lidstaten zorgen ervoor dat deze beleidslijnen en procedures openbaar worden gemaakt.

4. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, onverwijld na de registratie van een domeinnaam, domeinregistratiegegevens die geen persoonsgegevens zijn, bekendmaken.

5. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, op rechtmatige en naar behoren gemotiveerde verzoeken van legitieme toegangvragende partijen toegang verlenen tot specifieke domeinnaamregistratiegegevens, met inachtneming van de gegevensbeschermingswetgeving van de Unie. De lidstaten zorgen ervoor dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten voor topleveldomeinnamen verlenen, alle verzoeken om toegang onverwijld **en in ieder geval binnen 72 uur** beantwoorden. De lidstaten zorgen ervoor dat het beleid en de procedures voor de bekendmaking van dergelijke gegevens openbaar worden gemaakt.

AFDELING II

Jurisdictie en registratie

Artikel 24

Jurisdictie en territorialiteit

1a. Entiteiten die onder deze richtlijn vallen, worden geacht onder de jurisdictie te vallen van de lidstaat waar zij hun diensten verlenen. De in de punten 1 tot en met 7 en 10 van bijlage I bedoelde entiteiten en de in punt 8 van bijlage I en de punten 1 tot en met 5 van bijlage II bij deze richtlijn bedoelde verleners van vertrouwensdiensten en internet-knooppunten worden geacht onder de jurisdictie te vallen van de lidstaat waar zij zijn gevestigd.

1. DNS-dienstverleners, registers voor topleveldomeinnamen **en entiteiten die registratie-diensten voor topleveldomeinnamen verlenen**, aanbieders van cloudcomputerdiensten, [...] van datacentradiensten, [...] van netwerken voor de levering van inhoud, **van beheerde diensten en van beheerde beveiligingsdiensten** als bedoeld in punt 8 **en punt 8 bis** van bijlage I, alsmede digitale aanbieders als bedoeld in punt 6 van bijlage II, worden geacht onder de jurisdictie te vallen van de lidstaat waar zij hun hoofdvestiging in de Unie hebben.

2. Voor de toepassing van deze richtlijn worden de in lid 1 bedoelde entiteiten geacht hun hoofdvestiging in de Unie te hebben in de lidstaat waar de besluiten met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's **hoofdzakelijk** worden genomen. Indien **niet kan worden vastgesteld op welke plaats deze besluiten hoofdzakelijk worden genomen of** dergelijke besluiten in geen enkele vestiging in de Unie worden genomen, wordt de hoofdvestiging geacht zich te bevinden in de lidstaat waar de entiteiten de vestiging met het grootste aantal werknemers in de Unie hebben. **Wanneer de diensten door een groep van ondernemingen worden verleend, wordt de hoofdvestiging van de groep van ondernemingen beschouwd als de hoofdvestiging.**

3. Indien een in lid 1 bedoelde entiteit 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 aangewezen vertegenwoordiger binnen de Unie uit hoofde van dit artikel kan elke lidstaat waar de entiteit diensten verricht, gerechtelijke stappen ondernemen tegen de entiteit wegens niet-nakoming van de verplichtingen uit hoofde van deze richtlijn.

4. De aanwijzing van een vertegenwoordiger door een entiteit als bedoeld in lid 1 laat rechtsvorderingen die tegen de entiteit zelf kunnen worden ingesteld, onverlet.

4a. Lidstaten die een verzoek om wederzijdse bijstand hebben ontvangen met betrekking tot de in lid 1 bedoelde entiteiten, kunnen, binnen de grenzen van het verzoek, passende toezichts- en handhavingsmaatregelen nemen ten aanzien van de betrokken entiteit die op hun grondgebied diensten verleent of waarvan het netwerk- en informatiesysteem zich op hun grondgebied bevindt.

Artikel 25

Register voor bepaalde digitale-infrastructuurentiteiten en digitale aanbieders

1. [...] **De lidstaten zorgen ervoor dat** de in artikel 24, lid 1, bedoelde [...] entiteiten **waarvan de hoofdvestiging zich op hun grondgebied bevindt of waarvan, indien zij niet gevestigd zijn in de Unie, de aangewezen vertegenwoordiger in de Unie op hun grondgebied is gevestigd,** [...] uiterlijk [twaalf maanden na de inwerkingtreding van de richtlijn] de volgende informatie **moeten** indienen bij [...] **de bevoegde autoriteiten**:

a) de naam van de entiteit;

aa) de soort entiteit volgens de bijlagen I en II bij deze richtlijn;

b) het adres van haar hoofdvestiging en haar andere wettelijke vestigingen in de Unie of, indien deze niet in de Unie zijn gevestigd, van haar overeenkomstig artikel 24, lid 3, aangewezen vertegenwoordiger;

c) actuele contactgegevens, inclusief e-mailadressen en telefoonnummers van de entiteiten **en hun vertegenwoordigers;**

d) de lidstaten waar de entiteit de dienst verleent.

In voorkomend geval wordt deze informatie ingediend via het in artikel 2 bis bedoelde nationale mechanisme voor zelfmelding.

2. **De lidstaten zorgen ervoor dat de** in lid 1 bedoelde entiteiten **ook** [...] onverwijld, en in ieder geval binnen drie maanden na de datum waarop de wijziging van kracht is geworden, [...] melding maken van eventuele wijzigingen in de gegevens die zij op grond van lid 1 hebben ingediend.

3. [...] **De centrale contactpunten van de lidstaten sturen de in de leden 1 en 2 bedoelde informatie** door naar [...] **het Enisa**. […]

3a. Op basis van de overeenkomstig lid 3 van dit artikel ontvangen informatie stelt het Enisa voor de in lid 1 bedoelde entiteiten een register op en onderhoudt dat. Op verzoek van de lidstaten geeft het Enisa betrokken bevoegde autoriteiten toegang tot het register, waarbij in voorkomend geval de nodige waarborgen worden geboden om de vertrouwelijkheid van de informatie te beschermen.

4. […]

HOOFDSTUK V

Het delen van informatie

Artikel 26

Regelingen voor het delen van informatie op het gebied van cyberbeveiliging

1. [...] De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten **op vrijwillige basis** onderling relevante informatie over cyberbeveiliging kunnen uitwisselen, met inbegrip van informatie over cyberbedreigingen, **bijna-ongelukken,** kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen. Het delen van deze informatie:

   a) heeft tot doel incidenten te voorkomen, op te sporen, te bestrijden of te beperken;

b) verhoogt het niveau van de cyberbeveiliging, met name door de bewustwording met betrekking tot cyberbedreigingen te vergroten, het vermogen dergelijke bedreigingen om zich te verspreiden, te beperken of te belemmeren, een reeks verdedigings-capaciteiten te ondersteunen, het herstel en bekendmaking van kwetsbaarheden, technieken voor het opsporen van bedreigingen, beperkingsstrategieën of respons- en herstelfasen.

2. De lidstaten zorgen ervoor dat de informatie-uitwisseling plaatsvindt binnen [...] gemeenschappen van essentiële en belangrijke entiteiten. Deze uitwisseling wordt uitgevoerd door middel van regelingen voor het delen van informatie met betrekking tot de potentieel gevoelige aard van de gedeelde informatie [...].

3. De lidstaten **kunnen** regels vaststellen waarin de procedure, de operationele elementen (met inbegrip van het gebruik van specifieke ICT-platforms), de inhoud en de voorwaarden van de in lid 2 bedoelde regelingen voor het delen van informatie worden gespecificeerd. In deze regels **kunnen** ook de details van de betrokkenheid van de overheid bij dergelijke regelingen worden vastgelegd, alsmede de operationele elementen, met inbegrip van het gebruik van specifieke IT-platforms. De lidstaten bieden steun aan voor de toepassing van dergelijke regelingen overeenkomstig hun in artikel 5, lid 2, punt g), bedoelde beleid.

4. Essentiële en belangrijke entiteiten stellen de bevoegde autoriteiten in kennis van hun deelname aan de in lid 2 bedoelde regelingen voor het delen van informatie wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

5. [...] Het Enisa ondersteunt de invoering van de in lid 2 bedoelde regelingen voor het delen van informatie op het gebied van cyberbeveiliging door beste praktijken en richtsnoeren aan te reiken.

Artikel 27

Vrijwillige melding van relevante informatie

1. Onverminderd artikel 20 zorgen de lidstaten ervoor dat essentiële en belangrijke entiteiten de bevoegde autoriteiten of de CSIRT's op vrijwillige basis alle relevante incidenten, cyberbedreigingen of bijna-ongelukken kunnen melden.

2. Onverminderd artikel 3, zorgen de lidstaten ervoor dat entiteiten die buiten het toepassingsgebied van deze richtlijn vallen, op vrijwillige basis meldingen kunnen doen van significante incidenten, cyberbedreigingen of bijna-ongelukken. Bij de verwerking van de meldingen handelen de lidstaten volgens de procedure van artikel 20. De lidstaten kunnen voorrang geven aan de verwerking van verplichte meldingen boven vrijwillige meldingen. **Onverminderd het onderzoek naar en de opsporing en de vervolging van strafbare feiten,** mogen vrijwillige meldingen voor de meldende entiteit niet leiden tot het opleggen van bijkomende verplichtingen waaraan zij niet onderworpen zou zijn geweest indien zij de melding niet had ingediend.

3. Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting voor de betrokken lidstaat vormt.

HOOFDSTUK VI

Toezicht en handhaving

Artikel 28

Algemene aspecten van het toezicht en de handhaving

1. De lidstaten zorgen ervoor dat de bevoegde autoriteiten effectief toezicht houden op de naleving van deze richtlijn, en met name de verplichtingen van de artikelen 18**,** [...] 20 **en 23**, en nemen daartoe de nodige maatregelen. **De lidstaten kunnen bevoegde autoriteiten toestaan prioriteit te verlenen aan het toezicht, waarbij een risicogebaseerde benadering wordt gevolgd.**

2. Bij de aanpak van incidenten [...] werken de bevoegde autoriteiten nauw samen met de gegevensbeschermingsautoriteiten, **overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] aangewezen bevoegde autoriteiten, overeenkomstig Verordening (EU) nr. 910/2014 aangewezen toezichthoudende organen en andere overeenkomstig sectorspecifieke rechtshandelingen van de Unie aangewezen bevoegde autoriteiten**.

3. Onverminderd de nationale wettelijke en institutionele kaders zorgen de lidstaten ervoor dat met betrekking tot het toezicht op de naleving van deze richtlijn door overheidsinstanties en de handhaving van mogelijke sancties voor niet-naleving, de bevoegde autoriteiten over de juiste bevoegdheden beschikken om bij de uitvoering van deze taken operationeel onafhankelijk te zijn van de instanties waarop zij toezicht houden. De lidstaten kunnen besluiten passende, evenredige en doeltreffende toezichts- en handhavingsmaatregelen te nemen ten aanzien van deze instanties, in overeenstemming met de nationale kaders en rechtsorde.

Artikel 29

Toezicht en handhaving voor 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 belangrijke entiteiten **een risicogebaseerde benadering volgen en** de bevoegdheid hebben om deze entiteiten **ten minste** te onderwerpen aan:

   a) inspecties ter plaatse en toezicht elders, met inbegrip van steekproefsgewijze controles;

   b) regelmatige **beveiligings**audits;

   c) gerichte beveiligingsaudits op basis van risicobeoordelingen of beschikbare risicogerelateerde informatie;

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

   e) verzoeken om informatie die nodig is om de door de entiteit genomen cyberbeveiligingsmaatregelen te beoordelen, met inbegrip van gedocumenteerd cyberbeveiligingsbeleid [...];

   f) verzoeken om toegang tot gegevens, documenten of 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.

2a. Bij de uitvoering van hun in lid 2 van dit artikel bedoelde toezichthoudende taken kunnen de bevoegde autoriteiten toezichtsmethoden vaststellen die het mogelijk maken de prioriteit van dergelijke taken volgens een risicogebaseerde benadering te bepalen.

3. Bij de uitoefening van hun bevoegdheden uit hoofde van lid 2, punt e) tot en met g), 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 essentiële entiteiten, **ten minste** de bevoegdheid hebben om:

a) waarschuwingen te geven over de niet-naleving van de in deze richtlijn vastgestelde verplichtingen door de entiteiten;

b) bindende instructies te geven of een bevel uit te vaardigen waarin deze entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuken op de in deze richtlijn vastgestelde verplichtingen te verhelpen;

c) deze entiteiten te gelasten een einde te maken aan gedragingen die niet in overeenstemming zijn met de in deze richtlijn vastgestelde verplichtingen en af te zien van herhaling van die gedragingen;

d) deze entiteiten te gelasten hun risicobeheersmaatregelen en/of rapportageverplichtingen op een gespecificeerde wijze en binnen een gespecificeerde termijn in overeenstemming te brengen met de in de artikelen 18 en 20 vastgestelde verplichtingen;

e) deze entiteiten te gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberbedreiging worden beïnvloed, in kennis te stellen van **de aard van de bedreiging, evenals van** alle mogelijke beschermings- of herstelmaatregelen die door deze natuurlijke of rechtsperso(o)n(en) kunnen worden genomen als antwoord op die bedreiging;

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

g) […]

h) deze entiteiten te gelasten aspecten van niet-naleving van de in deze richtlijn vastgestelde verplichtingen op een bepaalde manier bekend te maken**, wanneer een dergelijke bekendmaking niet leidt tot een schadelijke blootstelling van de betrokken entiteit**;

i) […]

j) een administratieve geldboete op te leggen of de oplegging ervan door de bevoegde organen of rechtbanken overeenkomstig de nationale wetgeving te verzoeken overeenkomstig artikel 31 bovenop of in plaats van de in punten a) tot en met i) van dit lid bedoelde maatregelen, afhankelijk van de omstandigheden van elk afzonderlijk geval.

5. Indien de op grond van lid 4, punt a) tot en met d) en punt f), genomen handhavings-maatregelen ondoeltreffend blijken te zijn, zorgen de lidstaten ervoor dat de bevoegde autoriteiten de bevoegdheid hebben om een termijn vast te stellen waarbinnen de essentiële entiteit wordt verzocht de nodige 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 op te schorten of een certificerings- of vergunnings-instantie **of rechtbank overeenkomstig de nationale wetgeving** te verzoeken deze op te schorten met betrekking tot een deel of alle diensten of activiteiten die door een essentiële entiteit worden verleend;

b) een tijdelijk verbod op te leggen of de oplegging ervan door de bevoegde organen of rechtbanken overeenkomstig de nationale wetgeving te verzoeken, aan personen met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in die essentiële entiteit en aan andere natuurlijke personen die voor de inbreuk verantwoordelijk worden gehouden, om leidinggevende functies in die entiteit uit te oefenen.

Deze sancties worden alleen toegepast totdat de entiteit de nodige maatregelen neemt om de tekortkomingen te verhelpen of voldoet aan de vereisten van de bevoegde autoriteit waarvoor dergelijke sancties zijn opgelegd.

De sancties in dit lid zijn niet van toepassing op overheidsinstanties die onder deze richtlijn vallen.

6. De lidstaten zorgen ervoor dat elke natuurlijke persoon die verantwoordelijk is voor of optreedt als 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 toezicht uit te oefenen op deze entiteit, de bevoegdheid heeft om ervoor te zorgen dat deze entiteit de in deze richtlijn vastgestelde verplichtingen nakomt. De lidstaten zorgen ervoor dat deze natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om de in deze richtlijn vastgestelde verplichtingen na te komen. **Wat overheidsinstanties betreft, laat deze bepaling de wetgeving van de lidstaten inzake de aansprakelijkheid van ambtenaren en gekozen en benoemde overheids-functionarissen onverlet.**

7. Bij het nemen van handhavingsmaatregelen of het opleggen van sancties overeenkomstig de leden 4 en 5 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. Tot de inbreuken die als ernstig moeten worden beschouwd, behoren: herhaalde inbreuken, het niet melden of verhelpen van incidenten met een significant verstorend effect, het niet verhelpen van tekortkomingen naar aanleiding van bindende instructies van de bevoegde autoriteiten, het belemmeren van audits of toezichtsactiviteiten waartoe de bevoegde autoriteit opdracht heeft gegeven naar aanleiding van de vaststelling van een inbreuk, het verstrekken van valse of zeer onnauwkeurige informatie met betrekking tot de in de artikelen 18 en 20 vastgestelde eisen inzake risicobeheer of rapportage-verplichtingen;

b) de duur van de inbreuk, met inbegrip van het element van herhaalde inbreuken;

c) de daadwerkelijk veroorzaakte schade of geleden verliezen of de potentiële schade of verliezen die hadden kunnen worden veroorzaakt, voor zover deze kunnen worden vastgesteld. Bij de beoordeling van dit aspect wordt onder meer rekening gehouden met feitelijke of potentiële financiële of economische verliezen, effecten op andere diensten, aantal getroffen of mogelijk getroffen gebruikers;

d) het opzettelijke of nalatige karakter van de inbreuk;

e) maatregelen die door de entiteit worden genomen om de schade en/of verliezen te voorkomen of te beperken;

f) de naleving van goedgekeurde gedragscodes of goedgekeurde certificerings-mechanismen;

g) het niveau van samenwerking van de verantwoordelijke natuurlijke of rechtspersonen met de bevoegde autoriteiten.

8. De bevoegde autoriteiten geven een gedetailleerde motivering van hun handhavingsbesluiten. Alvorens dergelijke besluiten te nemen, stellen de bevoegde autoriteiten de betrokken entiteiten in kennis van hun voorlopige bevindingen en geven zij deze entiteiten een redelijke termijn om opmerkingen te maken**, tenzij er sprake is van een onmiddellijk gevaar**.

9. De lidstaten zorgen ervoor dat hun **uit hoofde van deze richtlijn** bevoegde autoriteiten [...] de betrokken bevoegde autoriteiten van **diezelfde** lidstaat [...] die zijn aangewezen overeenkomstig Richtlijn (EU) XXXX/XXXX [richtlijn inzake de veerkracht van kritieke entiteiten] in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële entiteit die op grond van Richtlijn (EU) XXXX/XXXX [richtlijn inzake de veerkracht van kritieke entiteiten] als kritieke entiteit **[**of als met een kritieke entiteit gelijkgestelde entiteit**]** wordt aangemerkt, voldoet aan de verplichtingen uit hoofde van deze richtlijn. **Waar nodig** [...] **kunnen** de bevoegde autoriteiten uit hoofde van Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten] [...] de **uit hoofde van deze richtlijn** bevoegde autoriteiten **verzoeken** hun toezichts- en handhavingsbevoegdheden uit te oefenen ten aanzien van een **onder deze richtlijn vallende** essentiële entiteit die **ook** als kritiek **[**of gelijkwaardig**]** is aangemerkt **op grond van Richtlijn (EU) XXXX/XXXX [richtlijn betreffende de veerkracht van kritieke entiteiten]**.

10. De lidstaten zorgen ervoor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten het toezichtforum overeenkomstig artikel 29, lid 1, van Verordening (EU) XXXX/XXXX [DORA-verordening] in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een essentiële entiteit die op grond van artikel 28 van Verordening (EU) XXXX/XXXX [DORA-verordening] is aangewezen als een cruciale derde aanbieder van ICT-diensten voldoet aan de verplichtingen uit hoofde van deze richtlijn.

10a. De lidstaten zorgen ervoor dat hun uit hoofde van deze richtlijn bevoegde autoriteiten de betrokken bevoegde autoriteiten die zijn aangewezen overeenkomstig Verordening (EU) nr. 910/2014 in kennis stellen wanneer zij hun toezichts- en handhavingsbevoegdheden uitoefenen om ervoor te zorgen dat een entiteit die op grond van Verordening (EU) nr. 910/2014 is aangewezen als verlener van vertrouwensdiensten voldoet aan de verplichtingen uit hoofde van deze richtlijn.

Artikel 30

Toezicht en handhaving voor belangrijke entiteiten

1. Wanneer het bewijs, de aanwijzing **of de informatie** wordt geleverd dat een belangrijke entiteit de in deze richtlijn, en met name in de artikelen 18 en 20, vastgestelde verplichtingen **vermoedelijk** niet nakomt, zorgen de lidstaten ervoor dat de bevoegde autoriteiten zo nodig maatregelen nemen door middel van toezichtsmaatregelen achteraf.

2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten bij de uitoefening van hun toezicht houdende taken met betrekking tot belangrijke entiteiten **een risicogebaseerde aanpak hanteren en** de bevoegdheid hebben om deze entiteiten **ten minste** te onderwerpen aan:

a) inspecties ter plaatse en toezicht elders achteraf;

b) gerichte beveiligingsaudits op basis van risicobeoordelingen of beschikbare risico-gerelateerde informatie;

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

d) verzoeken om alle informatie die nodig is om achteraf de cyberbeveiligingsmaatregelen te beoordelen[...];

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

ea) 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.

2a. Bij de uitvoering van hun in lid 2 van dit artikel bedoelde toezichthoudende taken kunnen de bevoegde autoriteiten toezichtsmethoden vaststellen die het mogelijk maken de prioriteit van dergelijke taken volgens een risicogebaseerde benadering te bepalen.

3. Bij de uitoefening van hun bevoegdheden uit hoofde van lid 2, punten d) **tot en met ea)**, 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 de niet-naleving van de in deze richtlijn vastgestelde verplichtingen door de entiteiten;

b) bindende instructies te geven of een bevel uit te vaardigen waarin deze entiteiten worden verplicht de vastgestelde tekortkomingen of de inbreuk op de in deze richtlijn vastgestelde verplichtingen te verhelpen;

c) deze entiteiten te gelasten een einde te maken aan gedragingen die niet in overeenstemming zijn met de in deze richtlijn vastgestelde verplichtingen en af te zien van herhaling van die gedragingen;

d) deze entiteiten te gelasten hun risicobeheersmaatregelen en/of rapportageverplichtingen op een gespecificeerde wijze en binnen een gespecificeerde termijn in overeenstemming te brengen met de in de artikelen 18 en 20 vastgestelde verplichtingen;

e) deze entiteiten te gelasten de natuurlijke of rechtspersonen aan wie zij diensten verlenen of voor wie zij activiteiten uitvoeren die mogelijkerwijs door een significante cyberbedreiging worden beïnvloed, in kennis te stellen van **de aard van de bedreiging, evenals van** alle mogelijke beschermings- of herstelmaatregelen die door deze natuurlijke of rechtsperso(o)n(en) kunnen worden genomen als antwoord op die bedreiging;

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

g) deze entiteiten te gelasten aspecten van niet-naleving van de in deze richtlijn vastgestelde verplichtingen op een bepaalde manier bekend te maken**, wanneer een dergelijke bekendmaking niet leidt tot een schadelijke blootstelling van de betrokken entiteit**;

h) […]

i) een administratieve geldboete op te leggen of de oplegging ervan door de bevoegde organen of rechtbanken overeenkomstig de nationale wetgeving te verzoeken overeenkomstig artikel 31 bovenop of in plaats van de in punten a) tot en met h) van dit lid bedoelde maatregelen, afhankelijk van de omstandigheden van elk afzonderlijk geval.

5. Artikel 29, leden 6 tot en met 8, is ook van toepassing op de toezichts- en handhavingsmaatregelen waarin dit artikel voorziet voor [...] [...] belangrijke entiteiten.

Artikel 31

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

1. De lidstaten zorgen ervoor dat het opleggen van administratieve boeten aan essentiële en belangrijke entiteiten uit hoofde van dit artikel in verband met inbreuken op de verplichtingen uit hoofde van deze richtlijn in elk afzonderlijk geval doeltreffend, evenredig en afschrikkend is.

2. Administratieve boeten worden, afhankelijk van de omstandigheden van elk afzonderlijk geval, opgelegd naast of in plaats van de in artikel 29, lid 4, punten a) tot en met i), artikel 29, lid 5, en artikel 30, lid 4, punten a) tot en met h), 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 rekening gehouden met de in artikel 29, lid 7, genoemde elementen.

4. De lidstaten zorgen ervoor dat overtredingen **door de essentiële entiteiten** van de verplichtingen van artikel 18 of artikel 20 overeenkomstig de leden 2 en 3 van dit artikel worden bestraft met administratieve boeten van ten minste [...] **4** 000 000 EUR of**, in het geval van een rechtspersoon,** [...] 2 % van de totale wereldwijde jaaromzet van de onderneming waartoe de essentiële [...] entiteit in het voorgaande boekjaar behoorde, indien dit bedrag hoger is.

4a. De lidstaten zorgen ervoor dat overtredingen door de belangrijke entiteiten van de verplichtingen van artikel 18 of artikel 20 overeenkomstig de leden 2 en 3 van dit artikel worden bestraft met administratieve boeten van ten minste 2 000 000 EUR of, in het geval van een rechtspersoon, 1 % van de totale wereldwijde jaaromzet van de onderneming waartoe de belangrijke entiteit in het voorgaande boekjaar behoorde, indien dit bedrag hoger is.

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

6. Onverminderd de bevoegdheden van de bevoegde autoriteiten uit hoofde van de artikelen 29 en 30 kan elke lidstaat bepalen of en in welke mate administratieve boeten kunnen worden opgelegd aan de in artikel 4, lid 23, bedoelde overheidsinstanties met inachtneming van de verplichtingen uit hoofde van deze richtlijn.

6a. Wanneer het rechtsstelsel van de lidstaat niet voorziet in administratieve geldboeten, zorgen de lidstaten ervoor dat dit artikel aldus kan worden toegepast dat geldboete wordt geïnitieerd door de bevoegde autoriteit en opgelegd door bevoegde nationale gerechten, waarbij wordt gewaarborgd dat deze rechtsmiddelen doeltreffend zijn en van gelijke werking zijn als de door bevoegde autoriteiten opgelegde administratieve geldboeten. De boeten zijn in elk geval doeltreffend, evenredig en afschrikkend. Die lidstaten delen de Commissie uiterlijk op [...] de wetgevingsbepalingen mee die zij op grond van dit lid vaststellen, alsmede onverwijld alle latere wijzigingen daarvan en alle daarop van invloed zijnde wijzigingswetgeving.

Artikel 32

Inbreuken die een inbreuk op de persoonsgegevens inhouden

1. Wanneer **bij het toezicht of de handhaving** de bevoegde autoriteiten [...] zich ervan **bewust zijn geworden** dat de inbreuk door een essentiële of belangrijke entiteit op de in de artikelen 18 en 20 **van deze richtlijn** vastgestelde verplichtingen een inbreuk in verband met persoonsgegevens, zoals gedefinieerd in artikel 4, lid 12, van Verordening (EU) 2016/679, met zich **kan** meebreng**en**[...], die overeenkomstig artikel 33 van die verordening moet worden gemeld, stellen zij de overeenkomstig de artikelen 55 en 56 van die verordening bevoegde toezichthoudende autoriteiten daarvan **onverwijld** [...] in kennis.

2. Indien de overeenkomstig de artikelen 55 en 56 van Verordening (EU) 2016/679 bevoegde toezichthoudende autoriteiten besluiten hun bevoegdheden overeenkomstig artikel 58, **lid 2,** punt i), van die verordening uit te oefenen en een administratieve boete op te leggen, leggen de **in artikel 8 van deze richtlijn bedoelde** bevoegde autoriteiten voor [...] **een** inbreuk geen administratieve boete op **op basis van** [...] artikel 31 van deze richtlijn. De bevoegde autoriteiten kunnen echter de handhavingsacties toepassen of de sanctiebevoegdheden uitoefenen waarin artikel 29, lid 4, punten a) tot en met i), artikel 29, lid 5, en artikel 30, lid 4, punten a) tot en met h), 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, kan de bevoegde autoriteit de in dezelfde lidstaat gevestigde toezichthoudende autoriteit daarvan in kennis stellen.

Artikel 33

Sancties

1. 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 nodige maatregelen om ervoor te zorgen dat deze worden uitgevoerd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn.

2. De lidstaten stellen de Commissie uiterlijk [twee] jaar na de inwerkingtreding van deze richtlijn in kennis van deze regels en maatregelen en stellen haar onverwijld in kennis van eventuele latere wijzigingen daarvan.

Artikel 34

Wederzijdse bijstand

1. Wanneer een essentiële of belangrijke entiteit diensten verricht in meer dan één lidstaat, of [...] **diensten verleent** in **één of meer** lidstat**en**, maar haar netwerk- en informatiesystemen zich in één of meer andere lidstaten bevinden, werken de bevoegde autoriteit**en** van de **betrokken** lidstat**en** [...] 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 handhavings-maatregelen[...];

b) een bevoegde autoriteit een andere bevoegde autoriteit kan verzoeken de [...] toezichts- of handhavingsmaatregelen te nemen;

c) een bevoegde autoriteit, na ontvangst van een met redenen omkleed verzoek van een andere bevoegde autoriteit, de andere bevoegde autoriteit bijstand verleent **die in verhouding staat tot de middelen waarover zij zelf beschikt**, zodat de [...] toezichts- of handhavingsacties op een effectieve, efficiënte en consistente wijze kunnen worden uitgevoerd. Deze 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 tot wie een verzoek om bijstand is gericht, mag dat verzoek niet weigeren, tenzij na een uitwisseling met de andere betrokken autoriteiten[...] wordt vastgesteld dat [...] de autoriteit niet bevoegd is om de gevraagde bijstand te verlenen **of niet over de nodige middelen beschikt** of dat de gevraagde bijstand niet in verhouding staat tot de toezichthoudende taken van de bevoegde autoriteit die [...] worden uitgevoerd **of dat het verzoek betrekking heeft op informatie of activiteiten inhoudt die in strijd zijn met de nationale veiligheid of de openbare veiligheid of defensie van die lidstaat**.

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

HOOFDSTUK VII

Overgangs- en slotbepalingen

Artikel 35

Evaluatie

De Commissie evalueert op gezette tijden de werking van deze richtlijn en brengt verslag uit aan het Europees Parlement en de Raad. In het verslag wordt met name de relevantie van de in de bijlagen I en II bedoelde sectoren, subsectoren, omvang en type van entiteiten voor het functioneren van de economie en de samenleving met betrekking tot cyberbeveiliging beoordeeld. Bij de uitvoering van **de evaluatie**, [...] houdt de Commissie rekening met de verslagen van [...] het CSIRT-netwerk over de opgedane ervaring op [...] operationeel niveau. Het eerste verslag wordt uiterlijk... [54 maanden na de datum van inwerkingtreding van deze richtlijn ingediend].

Artikel 36

[…]

[…]

[…]

Artikel 37

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.

Artikel 38

Omzetting

1. De lidstaten dienen **uiterlijk**... [[...]**24** maanden na de datum van inwerkingtreding van deze richtlijn**]** [...] de nodige wettelijke en bestuursrechtelijke bepalingen vast te stellen en bekend te maken om aan deze richtlijn te voldoen. Zij stellen de Commissie daarvan onmiddellijk in kennis. Zij passen die bepalingen toe vanaf … [één dag na in het eerste sublid genoemde datum].

2. Wanneer de lidstaten die 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 39

Wijziging van Verordening (EU) nr. 910/2014

In Verordening (EU) nr. 910/2014 wordt artikel 19 [...] ingetrokken **met ingang van... [uiterste datum voor omzetting van deze richtlijn].**

Artikel 40

Wijziging van Richtlijn (EU) 2018/1972

In Richtlijn (EU) 2018/1972 worden artikel 40 en artikel 41 [...] geschrapt**met ingang van... [uiterste datum voor omzetting van deze richtlijn].**

Artikel 41

Intrekking

Richtlijn (EU) 2016/1148 wordt ingetrokken met ingang van... [uiterste datum voor omzetting van deze richtlijn].

Verwijzingen naar Richtlijn (EU) 2016/1148 gelden als verwijzingen naar deze richtlijn, volgens de concordantietabel in de bijlage II[...].

Artikel 42

Inwerkingtreding

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

Artikel 43

Adressaten

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Brussel,

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

BIJLAGE I

SECTOREN, SUBSECTOREN EN SOORTEN ENTITEITEN

Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	— Elektriciteitsbedrijven als bedoeld in artikel 2, punt 57, van Richtlijn (EU) 2019/944 die de functie verrichten van "levering" als gedefinieerd in artikel 2, punt 12, van die richtlijn([39])
		— Distributiesysteembeheerders als bedoeld in artikel 2, punt 29, van Richtlijn (EU) 2019/944
		— Transmissiesysteembeheerders als bedoeld in artikel 2, punt 35, van Richtlijn (EU) 2019/944
		— Producenten als bedoeld in artikel 2, punt 38, van Richtlijn (EU) 2019/944
		— Benoemde elektriciteitsmarktbeheerders als bedoeld in artikel 2, punt 8, van Verordening (EU) 2019/943([40])
		— Marktdeelnemers op de elektriciteitsmarkt als bedoeld in artikel 2, punt 25, van Verordening (EU) 2019/943 die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken als bedoeld in artikel 2, punten 18, 20 en 59, van Richtlijn (EU) 2019/944

[39] 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).

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

	b) Stadsverwarming en -koeling	— Stadsverwarming of stadskoeling als bedoeld in artikel 2, punt 19, van Richtlijn (EU) 2018/2001([41]) ter bevordering van het gebruik van energie uit hernieuwbare bronnen
	c) Aardolie	— Exploitanten van oliepijpleidingen
		— Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport
		— Centrale entiteiten voor de voorraadvorming van aardolie als bedoeld in artikel 2, punt f), van Richtlijn 2009/119/EG van de Raad([42])
	d) Aardgas	— Aardgasbedrijven als bedoeld in artikel 2, punt 8, van Richtlijn 2009/73/EG([43])
		— Distributiesysteembeheerders als bedoeld in artikel 2, punt 6, van Richtlijn 2009/73/EG
		— Transmissiesysteembeheerders als bedoeld in artikel 2, punt 4, van Richtlijn 2009/73/EG
		— Opslagsysteembeheerders als bedoeld in artikel 2, punt 10, van Richtlijn 2009/73/EG

41 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).

42 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).

43 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).

		— LNG-systeembeheerders als bedoeld in artikel 2, punt 12, van Richtlijn 2009/73/EG
		— Aardgasbedrijven als bedoeld 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 transport van waterstof
2. Vervoer	a) Lucht	— Luchtvaartmaatschappijen als bedoeld in artikel 3, punt 4, van Verordening (EG) nr. 300/2008([44]), **die voor commerciële doeleinden worden gebruikt**
		— Luchthavenbeheerders als bedoeld in artikel 2, punt 2, van Richtlijn 2009/12/EG([45]), 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([46]) zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden
		— Exploitanten op het gebied van

[44] 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).

[45] 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).

[46] 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).

		verkeersbeheer en -controle die luchtverkeersleidingsdiensten als bedoeld in artikel 2, punt 1, van Verordening (EG) nr. 549/2004([47]) aanbieden
	b) Spoor	— Infrastructuurbeheerders als bedoeld in artikel 3, punt 2, van Richtlijn 2012/34/EU([48])
		— Spoorwegondernemingen als bedoeld in artikel 3, punt 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienst-voorzieningen als bedoeld in artikel 3, punt 12, van Richtlijn 2012/34/EU
	c) Water	— Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht als bedoeld in bijlage I bij Verordening (EG) nr. 725/2004([49]), met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen
		— Beheerders van havens als bedoeld in artikel 3, punt 1, van Richtlijn 2005/65/EG([50]), inclusief hun havenfaciliteiten als bedoeld in artikel 2, punt 11, van Verordening (EG) nr. 725/2004; alsook entiteiten die werken en uitrusting beheren in havens

[47] 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).

[48] 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).

[49] 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).

[50] 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).

		— Exploitanten van verkeers-begeleidingssystemen als bedoeld in artikel 3, punt o), van Richtlijn 2002/59/EG([51])
	d) Weg	— Wegenautoriteiten als bedoeld in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962([52]) van de Commissie die verantwoordelijk zijn voor het verkeersbeheer**, met uitzondering van overheids-instanties voor wie verkeers-beheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteiten is**
		— Exploitanten van intelligente vervoerssystemen als bedoeld in artikel 4, punt 1, van Richtlijn 2010/40/EU([53])
3. Bankwezen		— Kredietinstellingen als bedoeld in artikel 4, punt 1, van Verordening (EU) nr. 575/2013 ([54])**, [met uitzondering van de in artikel 2, lid 5, punt 8, van Richtlijn 2013/36/EU bedoelde krediet-instellingen die zijn vrijgesteld overeenkomstig artikel 2, lid 4, van Verordening XX [DORA]]**

[51] 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 zeescheep-vaart en tot intrekking van Richtlijn 93/75/EEG van de Raad (PB L 208 van 5.8.2002, blz. 10).

[52] 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).

[53] 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).

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

4. Infrastructuur voor de financiële markt		— Exploitanten van handelsplatformen als bedoeld in artikel 4, punt 24, van Richtlijn 2014/65/EU([55])
		— Centrale tegenpartijen als bedoeld in artikel 2, punt 1, Verordening (EU) nr. 648/2012([56])
5. Volksgezondheid		— Zorgaanbieders als bedoeld in artikel 3, punt g), van Richtlijn 2011/24/EU([57])
		— EU-referentielaboratoria als bedoeld in artikel 15 van Verordening XXXX/XXXX inzake ernstige grensoverschrijdende bedreigingen van de gezondheid[58]
		— Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen als bedoeld in artikel 1, punt 2, van Richtlijn 2001/83/EG([59]) — Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 vervaardigen — Entiteiten die medische hulp-middelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd ("de lijst

[55] 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).

[56] 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).

[57] 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).

[58] [Verordening van het Europees Parlement en de Raad inzake ernstige grensoverschrijdende bedreigingen van de gezondheid en houdende intrekking van Besluit nr. 1082/2013/EU, verwijzing bij te werken zodra voorstel COM(2020)727 final is aangenomen].

[59] 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).

		van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen") als bedoeld in artikel 20 van Verordening XXXX[60]
6. Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water als bedoeld in artikel 2, lid 1, punt a), van Richtlijn 98/83/EG van de Raad([61]), maar met uitzondering van distributeurs voor wie de distributie van water voor menselijke consumptie slechts een **niet-essentieel** deel is van hun algemene activiteit van distributie van andere waren en goederen [...]
7. Afvalwater		Ondernemingen die stedelijk, huishoudelijk en industrieel afvalwater als bedoeld in de artikel 2, punten 1, 2 en 3, van Richtlijn 91/271/EEG([62]) van de Raad opvangen, lozen of behandelen, **met uitzondering van ondernemingen voor wie het opvangen, lozen of behandelen van stedelijk, huishoudelijk en industrieel afvalwater slechts een niet-essentieel onderdeel van hun algemene activiteit is.** […]
8. Digitale infrastructuur		— Internetknooppunten
		— Aanbieders van DNS-diensten**, met uitzondering van exploitanten van root-naamservers**
		— Registers voor toplevel-domeinnamen
		— Aanbieders van

60 [Verordening van het Europees Parlement en de Raad betreffende een grotere rol van het Europees Geneesmiddelenbureau inzake crisisparaatheid en -beheersing op het gebied van geneesmiddelen en medische hulpmiddelen, verwijzing bij te werken zodra voorstel COM(2020)725 final is aangenomen].

61 Richtlijn 98/83/EG van de Raad van 3 november 1998 betreffende de kwaliteit van voor menselijke consumptie bestemd water (PB L 330 van 5.12.1998, blz. 32).

62 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).

		cloudcomputingdiensten
		— Aanbieders van datacenterdiensten
		— Aanbieders van netwerken voor content delivery
		— Verleners van vertrouwensdiensten als bedoeld in artikel 3, punt 19, van Verordening (EU) 910/2014([63])
		— Aanbieders van openbare elektronischecommunicatienetwerken als bedoeld in artikel 2, punt 8, van Richtlijn (EU) 2018/1972([64]) of aanbieders van elektronischecommunicatiediensten als bedoeld in artikel 2, punt 4, van Richtlijn (EU) 2018/1972 voor zover hun diensten voor het publiek beschikbaar zijn
8.a Beheer van ICT-diensten **(B2B)**		**— Aanbieders van beheerde diensten ("managed service providers" — MSP's)** **— Aanbieders van beheerde beveiligingsdiensten ("managed security services providers" — MSSP's)**

[63] 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).

[64] 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).

9. Overheids**instanties**		— Overheidsinstanties van centrale overheden, **zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht** — [...][65][...] — […]
10. Ruimtevaart		— Exploitanten van grondfaciliteiten die in het bezit zijn van en beheerd en geëxploiteerd worden door de lidstaten of door private partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronischecommunicatienetwerken als bedoeld in artikel 2, punt 8, van Richtlijn (EU) 2018/1972

65 [...]

BIJLAGE II

SECTOREN, SUBSECTOREN EN SOORTEN ENTITEITEN

Sector	Deelsector	Soort entiteit
1. Post- en koeriersdiensten		Aanbieders van postdiensten als bedoeld in artikel 2, punt 1[...], van Richtlijn 97/67/EG([66]), **waaronder** [...] aanbieders van koerierdiensten
2. Afvalstoffenbeheer		Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren als bedoeld in artikel 3, punt 9, van Richtlijn 2008/98/EG([67]), met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is

[66] 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), **zoals gewijzigd bij Richtlijn 2008/6/EG van het Europees Parlement en de Raad van 20 februari 2008 tot wijziging van Richtlijn 97/67/EG wat betreft de volledige voltooiing van de interne markt voor postdiensten in de Gemeenschap (PB L 52 van 27.2.2008, blz. 3).**

[67] 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).

3. Vervaardiging, productie en distributie van chemische stoffen		Ondernemingen die stoffen en [...] **mengsels** vervaardigen[...] en distribueren bedoeld in artikel 3, punten [...], 9 en 14, van Verordening (EG) nr. 1907/2006([68]) **en ondernemingen die uit stoffen of mengsels artikelen vervaardigen als bedoeld in artikel 3, punt 3, van die verordening.**
4. Productie, verwerking en distributie van levensmiddelen		Levensmiddelenbedrijven als bedoeld in artikel 3, punt (2), van Verordening (EG) nr.178/2002 ([69]) **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 als bedoeld in artikel 2, punt 1, van Verordening (EU) 2017/745([70]) vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek als bedoeld in artikel 2, punt 2, van Verordening (EU) 2017/746([71])

[68] 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).

[69] 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).

[70] 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).

[71] 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).

		vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen die zijn opgenomen in bijlage 1, punt 5.
	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, aanhangwagens en opleggers	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2
	f) Vervaardiging van andere vervoermiddelen	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2
6. Digitale aanbieders		— Aanbieders van onlinemarktplaatsen
		— Aanbieders van onlinezoekmachines
		— Aanbieders van platforms voor socialenetwerkdiensten