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

van 14 december 2022

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

(Voor de EER relevante tekst)

(PB L 333 van 27.12.2022, blz. 80)

Gerectificeerd bij:

►**C1** Rectificatie PB L 112 van 27.4.2023, blz. 50 (2022/2555)
►**C2** Rectificatie PB L 154 van 15.6.2023, blz. 50 (2022/2555)

▼B

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

van 14 december 2022

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

(Voor de EER relevante tekst)

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp

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

2. Met het oog hierop voorziet deze richtlijn in:

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

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

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

d) toezichts- en handhavingsverplichtingen voor de lidstaten.

Artikel 2

Toepassingsgebied

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

▼B

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

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

a) de diensten verleend worden door:

i) aanbieders van openbare elektronischecommunicatienetwerken of van openbare elektronischecommunicatiediensten;

ii) aanbieders van vertrouwensdiensten;

▼C1

iii) registers voor topleveldomeinnamen en aanbieders van domeinnaamsysteemdiensten;

▼B

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

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

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

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

f) de entiteit een overheidsinstantie is:

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

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

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

▼B

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

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

a) overheidsinstanties op lokaal niveau;

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

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

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

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

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

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

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

12. Deze richtlijn is van toepassing onverminderd Verordening (EU) 2016/679, Richtlijn 2002/58/EG, Richtlijnen 2011/93/EU ([1]) en 2013/40/EU ([2]) van het Europees Parlement en de Raad, en Richtlijn (EU) 2022/2557.

([1]) 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).

([2]) 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).

▼B

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

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

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

Artikel 3

Essentiële en belangrijke entiteiten

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

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

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

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

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

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

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

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

▼B

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

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

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

a) de naam van de entiteit;

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

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

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

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

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

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

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

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

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

▼B

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

Artikel 4

Sectorspecifieke rechtshandelingen van de Unie

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

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

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

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

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

Artikel 5

Minimumharmonisatie

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

Artikel 6

Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

▼B

1) “netwerk- en informatiesysteem”:

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

16) “norm”: een norm zoals gedefinieerd in artikel 2, punt 1), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad ([3]);

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

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

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

([3]) 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).

▼B

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

a) openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers, of

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

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

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

23) “digitale dienst”: een dienst zoals gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad ([4]);

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

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

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

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

28) “onlinemarktplaats”: een onlinemarktplaats zoals gedefinieerd in artikel 2, punt n), van Richtlijn 2005/29/EG van het Europees Parlement en de Raad ([5]);

29) “onlinezoekmachine”: een onlinezoekmachine zoals gedefinieerd in artikel 2, punt 5), van Verordening (EU) 2019/1150 van het Europees Parlement en de Raad ([6]);

([4]) 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).

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

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

▼B

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

▼C2

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

▼B

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

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

HOOFDSTUK II

GECOÖRDINEERDE KADERS OP HET GEBIED VAN CYBERBEVEILIGING

Artikel 7

Nationale cyberbeveiligingsstrategie

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

j) voor het bevorderen van actieve cyberbescherming.

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

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

Artikel 8

Bevoegde autoriteiten en centrale contactpunten

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

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

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

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

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

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

▼B

Artikel 9

Nationale kaders voor cybercrisisbeheer

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

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

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

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

a) de doelstellingen van nationale paraatheidsmaatregelen en -activiteiten;

b) de taken en verantwoordelijkheden van de cybercrisisbeheerautoriteiten;

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

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

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

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

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

▼B

Artikel 10

Computer security incident response teams (CSIRT's)

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

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

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

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

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

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

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

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

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

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

▼B

Artikel 11

Eisen, technische capaciteiten en taken van de CSIRT's

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

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

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

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

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

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

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

De CSIRT's kunnen deelnemen aan internationale samenwerkingsnetwerken.

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

3. De CSIRT's hebben de volgende taken:

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

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

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

▼B

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

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

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

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

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

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

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

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

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

a) procedures voor de incidentenbehandeling;

b) crisisbeheer, en

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

Artikel 12

Gecoördineerde bekendmaking van de kwetsbaarheden en een Europese kwetsbaarheidsdatabase

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

▼B

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

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

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

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

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

a) informatie die de kwetsbaarheid beschrijft;

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

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

Artikel 13

Samenwerking op nationaal niveau

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

▼B

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

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

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

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

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

HOOFDSTUK III

SAMENWERKING OP UNIE- EN INTERNATIONAAL NIVEAU

Artikel 14

Samenwerkingsgroep

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

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

▼B

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

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

Het secretariaat wordt verzorgd door de diensten van de Commissie.

4. De samenwerkingsgroep heeft de volgende taken:

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

Artikel 15

CSIRT-netwerk

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

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

3. Het CSIRT-netwerk heeft de volgende taken:

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

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

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

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

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

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

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

▼B

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

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

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

   i) categorieën van cyberdreigingen en -incidenten;

   ii) vroegtijdige waarschuwingen;

   iii) wederzijdse bijstand;

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

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

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

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

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

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

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

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

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

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

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

▼B

Artikel 16

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

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

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

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

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

3. EU-CyCLONe heeft tot taak:

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

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

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

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

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

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

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

▼B

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

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

Artikel 17

Internationale samenwerking

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

Artikel 18

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

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

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

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

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

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

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

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

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

▼B

Artikel 19

Collegiale toetsingen

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

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

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

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

c) de operationele capaciteit van de CSIRT's;

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

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

f) specifieke kwesties van grens- of sectoroverschrijdende aard.

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

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

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

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

▼B

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

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

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

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

HOOFDSTUK IV

RISICOBEHEERSMAATREGELEN EN RAPPORTAGEVERPLICHTINGEN OP HET GEBIED VAN CYBERBEVEILIGING

Artikel 20

Governance

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

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

▼B

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

Artikel 21

Maatregelen voor het beheer van cyberbeveiligingsrisico's

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

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

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

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

Artikel 22

Op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens

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

▼B

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

Artikel 23

Rapportageverplichtingen

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

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

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

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

3. Een incident wordt als significant beschouwd als het:

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

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

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

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

▼B

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

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

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

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

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

iii) toegepaste en lopende risicobeperkende maatregelen;

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

▼B

Artikel 24

Gebruik van Europese cyberbeveiligingscertificeringsregelingen

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

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

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

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

Artikel 25

Normalisatie

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

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

HOOFDSTUK V

JURISDICTIE EN REGISTRATIE

Artikel 26

Jurisdictie en territorialiteit

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

▼B

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

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

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

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

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

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

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

Artikel 27

Register van entiteiten

1. Enisa creëert en onderhoudt een register van DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, op basis van de informatie die is ontvangen van de centrale contactpunten in

▼B

overeenstemming met lid 4. Op verzoek geeft Enisa bevoegde autoriteiten toegang tot dat register, waarbij zij er zo nodig voor zorgt dat de vertrouwelijkheid van de informatie wordt beschermd.

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

a) de naam van de entiteit;

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

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

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

e) de lidstaten waar de entiteit diensten verleent, en

f) de IP-bereiken van de entiteit.

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

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

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

Artikel 28

Database met domeinnaamregistratiegegevens

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

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

▼B

a) de domeinnaam;

b) de registratiedatum van registratie;

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

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

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

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

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

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

HOOFDSTUK VI

INFORMATIE-UITWISSELING

Artikel 29

Informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging

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

▼B

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

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

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

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

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

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

Artikel 30

Vrijwillige melding van relevante informatie

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

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

▼B

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

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

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

HOOFDSTUK VII

TOEZICHT EN HANDHAVING

Artikel 31

Algemene aspecten van het toezicht en de handhaving

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

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

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

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

▼B

Artikel 32

Toezichts- en handhavingsmaatregelen met betrekking tot essentiële entiteiten

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

   i) herhaalde inbreuken;

   ii) niet melden of niet verhelpen van significante incidenten;

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

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

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

b) de duur van de inbreuk;

c) eventuele relevante eerdere inbreuken door de betrokken entiteit;

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

▼B

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

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

g) de naleving van goedgekeurde gedragscodes of goedgekeurde certificeringsmechanismen;

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

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

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

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

Artikel 33

Toezichts- en handhavingsmaatregelen met betrekking tot belangrijke entiteiten

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

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

▼B

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▼B

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

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

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

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

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

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

Artikel 34

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

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

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

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

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

▼B

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

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

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

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

Artikel 35

Inbreuken die een inbreuk in verband met persoonsgegevens inhouden

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

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

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

▼B

Artikel 36

Sancties

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

Artikel 37

Wederzijdse bijstand

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

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

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

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

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

▼B

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

HOOFDSTUK VIII

GEDELEGEERDE HANDELINGEN EN UITVOERINGSHANDELINGEN

Artikel 38

Uitoefening van de bevoegdheidsdelegatie

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

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

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

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

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

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

Artikel 39

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.

▼B

2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

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

HOOFDSTUK IX

SLOTBEPALINGEN

Artikel 40

Evaluatie

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

Artikel 41

Omzetting

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

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

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

Artikel 42

Wijziging van Verordening (EU) nr. 910/2014

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

Artikel 43

Wijziging van Richtlijn (EU) 2018/1972

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

▼B

Artikel 44

Intrekking

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

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

Artikel 45

Inwerkingtreding

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

Artikel 46

Adressaten

Deze richtlijn is gericht tot de lidstaten.

▼B

BIJLAGE I

ZEER KRITIEKE SECTOREN

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

▼B

Sector	Subsector	Soort entiteit
		— LNG-systeembeheerders zoals gedefinieerd in artikel 2, punt 12, van Richtlijn 2009/73/EG
		— Aardgasbedrijven zoals gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/73/EG
		— Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
	e) Waterstof	— Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof
2. Vervoer	a) Lucht	— Luchtvaartmaatschappijen zoals gedefinieerd in artikel 3, punt 4, Verordening (EG) nr. 300/2008 die voor commerciële doeleinden worden gebruikt
		— Luchthavenbeheerders zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 2009/12/EG van het Europees Parlement en de Raad ([6]), luchthavens als bedoeld in artikel 2, punt 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013 van het Europees Parlement en de Raad ([7]) zijn opgenomen, alsook de entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden
		— Exploitanten op het gebied van verkeersbeheer en -controle die luchtverkeersleidingsdiensten zoals gedefinieerd in artikel 2, punt 1, van Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad ([8]) aanbieden
	b) Spoor	— Infrastructuurbeheerders zoals gedefinieerd in artikel 3, punt 2, van Richtlijn 2012/34/EU van het Europees Parlement en de Raad ([9])
		— Spoorwegondernemingen zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienstvoorzieningen zoals gedefinieerd in artikel 3, punt 12, van die richtlijn
	c) Water	— Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht, die in bijlage I bij Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad ([10]) als bedrijven in maritiem vervoer worden gedefinieerd, met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen

▼B

Sector	Subsector	Soort entiteit
		— Beheerders van havens zoals gedefinieerd in artikel 3, punt 1, van Richtlijn 2005/65/EG van het Europees Parlement en de Raad ([11]), inclusief hun havenfaciliteiten zoals gedefinieerd in artikel 2, punt 11, van Verordening (EG) nr. 725/2004; alsook entiteiten die werken en uitrusting in havens beheren
		— Exploitanten van verkeersbegeleidingssystemen (VBS) zoals gedefinieerd in artikel 3, punt o), van Richtlijn 2002/59/EG van het Europees Parlement en de Raad ([12])
	d) Weg	— Wegenautoriteiten zoals gedefinieerd in artikel 2, punt 12, van gedelegeerde Verordening (EU) 2015/962 van de Commissie ([13]) die verantwoordelijk zijn voor het verkeersbeheer, met uitzondering van overheidsinstanties waarvoor verkeersbeheer of de exploitatie van intelligente vervoerssystemen slechts een niet-essentieel onderdeel van hun algemene activiteit is
		— Exploitanten van intelligente vervoerssystemen zoals gedefinieerd in artikel 4, punt 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad ([14])
3. Bankwezen		Kredietinstellingen zoals gedefinieerd in artikel 4, punt 1, Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ([15])
4. Infrastructuur voor de financiële markt		— Exploitanten van handelsplatformen zoals gedefinieerd in artikel 4, punt 24, van Richtlijn 2014/65/EU van het Europees Parlement en de Raad ([16])
		— Centrale tegenpartijen zoals gedefinieerd in artikel 2, punt 1, Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad ([17])
5. Gezondheidszorg		— Zorgaanbieders zoals gedefinieerd in artikel 3, punt g), van Richtlijn 2011/24/EU van het Europees Parlement en de Raad ([18])
		— EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371 van het Europees Parlement en de Raad inzake ernstige grensoverschrijdende bedreigingen van de gezondheid ([19])
		— Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen zoals gedefinieerd in artikel 1, punt 2, van Richtlijn 2001/83/EG van het Europees Parlement en de Raad ([20]) — Entiteiten die farmaceutische basisproducten en farmaceutische bereidingen als bedoeld in sectie C, afdeling 21, van NACE Rev. 2 vervaardigen — Entiteiten die medische hulpmiddelen vervaardigen die in het kader van de noodsituatie op het gebied van de volksgezondheid als kritiek worden beschouwd (“de lijst van in een noodsituatie op het gebied van de volksgezondheid kritieke hulpmiddelen”) in de zin van artikel 22 van Verordening (EU) 2022/123 van het Europees Parlement en de Raad ([21])

▼B

Sector	Subsector	Soort entiteit
6. Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water zoals gedefinieerd in artikel 2, punt 1, a), van Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad ([22]), met uitzondering van distributeurs waarvoor de distributie van water voor menselijke consumptie een niet-essentieel deel is van hun algemene activiteit van distributie van andere waren en goederen die niet worden beschouwd als essentiële of belangrijke diensten
7. Afvalwater		Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater zoals gedefinieerd in artikel 2, punten 1, 2 en 3, van Richtlijn 91/271/EEG van de Raad ([23]) opvangen, lozen of behandelen, met uitzondering van ondernemingen waarvoor het opvangen, lozen of behandelen van stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater een niet-essentieel onderdeel van hun algemene activiteit is
8. Digitale infrastructuur		— Aanbieders van internetknooppunten
		— DNS-dienstverleners, met uitzondering van exploitanten van root-naamservers
		— Register voor topleveldomeinnamen
		— Aanbieders van cloudcomputingdiensten
		— Aanbieders van datacenterdiensten
		— Aanbieders van netwerken voor de levering van inhoud
		— Verleners van vertrouwensdiensten
		— Aanbieders van openbare elektronischecommunicatienetwerken
		— Aanbieders van openbare elektronischecommunicatiediensten
9. Beheer van ICT-diensten (business-to-business)		— Aanbieders van beheerde diensten — Aanbieders van beheerde beveiligingsdiensten
10. Overheid		— Overheidsinstanties van centrale overheden zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht
		— Overheidsinstanties op regionaal niveau zoals gedefinieerd door een lidstaat overeenkomstig het nationale recht

▼B

Sector	Subsector	Soort entiteit
11. Ruimtevaart		Exploitanten van grondfaciliteiten die in het bezit zijn van of beheerd of geëxploiteerd worden door de lidstaten of door particuliere partijen en die de verlening van vanuit de ruimte opererende diensten ondersteunen, met uitzondering van aanbieders van openbare elektronischecommunicatienetwerken

([1]) Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (PB L 158 van 14.6.2019, blz. 125).
([2]) Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit (PB L 158 van 14.6.2019, blz. 54).
([3]) Richtlijn (EU) 2018/2001 van het Europees Parlement en de Raad van 11 december 2018 ter bevordering van het gebruik van energie uit hernieuwbare bronnen (PB L 328 van 21.12.2018, blz. 82).
([4]) Richtlijn 2009/119/EG van de Raad van 14 september 2009 houdende verplichting voor de lidstaten om minimumvoorraden ruwe aardolie en/of aardolieproducten in opslag te houden (PB L 265 van 9.10.2009, blz. 9).
([5]) Richtlijn 2009/73/EG van het Europees Parlement en de Raad van 13 juli 2009 betreffende gemeenschappelijke regels voor de interne markt voor aardgas en tot intrekking van Richtlijn 2003/55/EG (PB L 211 van 14.8.2009, blz. 94).
([6]) Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden (PB L 70 van 14.3.2009, blz. 11).
([7]) Verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende richtsnoeren van de Unie voor de ontwikkeling van het trans-Europees vervoersnetwerk en tot intrekking van Besluit nr. 661/2010/EU (PB L 348 van 20.12.2013, blz. 1).
([8]) Verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim (de kaderverordening) (PB L 96 van 31.3.2004, blz. 1).
([9]) Richtlijn 2012/34/EU van het Europees Parlement en de Raad van 21 november 2012 tot instelling van één Europese spoorwegruimte, (PB L 343 van 14.12.2012, blz. 32).
([10]) Verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad van 31 maart 2004 betreffende de verbetering van de beveiliging van schepen en havenfaciliteiten (PB L 129 van 29.4.2004, blz. 6).
([11]) Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens (PB L 310 van 25.11.2005, blz. 28).
([12]) Richtlijn 2002/59/EG van het Europees Parlement en de Raad van 27 juni 2002 betreffende de invoering van een communautair monitoring en informatiesysteem voor de zeescheepvaart en tot intrekking van Richtlijn 93/75/EEG van de Raad (PB L 208 van 5.8.2002, blz. 10).
([13]) Gedelegeerde verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtime-verkeersinformatiediensten betreft (PB L 157 van 23.6.2015, blz. 21).
([14]) Richtlijn 2010/40/EU van het Europees Parlement en de Raad van 7 juli 2010 betreffende het kader voor het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen (PB L 207 van 6.8.2010, blz. 1).
([15]) Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en tot wijziging van Verordening (EU) nr. 648/2012, PB L 176 van 27.6.2013, blz. 1.
([16]) Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU (PB L 173 van 12.6.2014, blz. 349).
([17]) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).
([18]) Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PB L 88 van 4.4.2011, blz. 45).
([19]) Verordening (EU) 2022/2371 van het Europees Parlement en de Raad van 23 november 2022 inzake ernstige grensoverschrijdende bedreigingen van de gezondheid en houdende intrekking van Besluit nr. 1082/2013/EU (PB L 314 van 6.12.2022, blz. 26).
([20]) Richtlijn 2001/83/EG van het Europees Parlement en de Raad van 6 november 2001 tot vaststelling van een communautair wetboek betreffende geneesmiddelen voor menselijk gebruik (PB L 311 van 28.11.2001, blz. 67).
([21]) Verordening (EU) 2022/123 van het Europees Parlement en de Raad van 25 januari 2022 betreffende een grotere rol van het Europees Geneesmiddelenbureau inzake crisisparaatheid en -beheersing op het gebied van geneesmiddelen en medische hulpmiddelen (PB L 20 van 31.1.2022, blz. 1).
([22]) Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water (PB L 435 van 23.12.2020, blz. 1).
([23]) Richtlijn 91/271/EEG van de Raad van 21 mei 1991 inzake de behandeling van stedelijk afvalwater (PB L 135 van 30.5.1991, blz. 40).

▼B

BIJLAGE II

ANDERE KRITIEKE SECTOREN

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

02022L2555 — NL — 27.12.2022 — 000.002 — 56

▼B

Sector	Subsector	Soort entiteit
	d) Vervaardiging van machines, apparaten en werktuigen, n.e.g.	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2
	e) Vervaardiging van motorvoertuigen, aanhangers en opleggers	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2
	f) Vervaardiging van andere transportmiddelen	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2
6. Digitale aanbieders		— Aanbieders van onlinemarktplaatsen
		— Aanbieders van onlinezoekmachines
		— Aanbieders van platforms voor socialenetwerkdiensten
7. Onderzoek		Onderzoeksorganisaties

([1]) Richtlijn 2008/98/EG van het Europees Parlement en de Raad van 19 november 2008 betreffende afvalstoffen en tot intrekking van een aantal richtlijnen (PB L 312 van 22.11.2008, blz. 3).
([2]) Verordening (EG) nr. 1907/2006 van het Europees Parlement en de Raad van 18 december 2006 inzake de registratie en beoordeling van en de autorisatie en beperkingen ten aanzien van chemische stoffen (REACH), tot oprichting van een Europees Agentschap voor chemische stoffen, houdende wijziging van Richtlijn 1999/45/EG en houdende intrekking van Verordening (EEG) nr. 793/93 van de Raad en Verordening (EG) nr. 1488/94 van de Commissie alsmede Richtlijn 76/769/EEG van de Raad en de Richtlijnen 91/155/EEG, 93/67/EEG, 93/105/EG en 2000/21/EG van de Commissie (PB L 396 van 30.12.2006, blz. 1).
([3]) Verordening (EG) nr. 178/2002 van het Europees Parlement en de Raad van 28 januari 2002 tot vaststelling van de algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tot vaststelling van procedures voor voedselveiligheidsaangelegenheden (PB L 31 van 1.2.2002, blz. 1).
([4]) Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (PB L 117 van 5.5.2017, blz. 1).
([5]) Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176).

▼B

BIJLAGE III

CONCORDANTIETABEL

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

▼B

Richtlijn (EU) 2016/1148	Deze richtlijn
Artikel 11, lid 4	Artikel 14, lid 4, eerste alinea, punt r), en tweede alinea
Artikel 11, lid 5	Artikel 14, lid 8
Artikel 12, leden 1 tot en met 5	Artikel 15, leden 1 tot en met 5
Artikel 13	Artikel 17
Artikel 14, leden 1 en 2	Artikel 21, leden 1 tot en met 4
Artikel 14, lid 3	Artikel 23, lid 1
Artikel 14, lid 4	Artikel 23, lid 3
Artikel 14, lid 5	Artikel 23, leden 5, 6 en 8
Artikel 14, lid 6	Artikel 23, lid 7
Artikel 14, lid 7	Artikel 23, lid 11
Artikel 15, lid 1	Artikel 31, lid 1
Artikel 15, lid 2, eerste alinea, punt a)	Artikel 32, lid 2, punt e)
Artikel 15, lid 2, eerste alinea, punt b)	Artikel 32, lid 2, punt g)
Artikel 15, lid 2, tweede alinea	Artikel 32, lid 3
Artikel 15, lid 3	Artikel 32, lid 4, punt b)
Artikel 15, lid 4	Artikel 31, lid 3
Artikel 16, leden 1 en 2	Artikel 21, leden 1 tot en met 4
Artikel 16, lid 3	Artikel 23, lid 1
Artikel 16, lid 4	Artikel 23, lid 3
Artikel 16, lid 5	—
Artikel 16, lid 6	Artikel 23, lid 6
Artikel 16, lid 7	Artikel 23, lid 7
Artikel 16, leden 8 en 9	Artikel 21, lid 5, en artikel 23, lid 11
Artikel 16, lid 10	—
Artikel 16, lid 11	Artikel 2, leden 1, 2 en 3
Artikel 17, lid 1	Artikel 33, lid 1
Artikel 17, lid 2, punt a)	Artikel 32, lid 2, punt e)
Artikel 17, lid 2, punt b)	Artikel 32, lid 4, punt b)

▼B

Richtlijn (EU) 2016/1148	Deze richtlijn
Artikel 17, lid 3	Artikel 37, lid 1, punten a) en b)
Artikel 18, lid 1	Artikel 26, lid 1, punt b), en lid 2
Artikel 18, lid 2	Artikel 26, lid 3
Artikel 18, lid 3	Artikel 26, lid 4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	—
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Bijlage I, punt 1	Artikel 11, lid 1
Bijlage I, punt 2, punt a), i)-iv)	Artikel 11, lid 2, punten a) tot en met d)
Bijlage I, punt 2, punt a), v)	Artikel 11, lid 2, punt f)
Bijlage I, punt 2, punt b)	Artikel 11, lid 4
Bijlage I, punt 2, punt c), i)-ii)	Artikel 11, lid 5, punt a)
Bijlage II	Bijlage I
Bijlage III, punten 1 en 2	Bijlage II, punt 6
Bijlage III, punt 3	Bijlage I, punt 8