Vergaderjaar 2025-2026

36 764 Regels ter implementatie van 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 (PbEU 2022, L 333) (Cyberbeveiligingswet)

A **GEWIJZIGD VOORSTEL VAN WET**
15 april 2026

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben dat het gelet op 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 (*PbEU* 2022, L 333) noodzakelijk is om wettelijke bepalingen vast te stellen ter bevordering van de digitale veiligheid;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

HOOFDSTUK 1. BEGRIPSBEPALING

Artikel 1 (begripsbepaling)

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

– Aanbeveling 2003/361/EG: Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (*PbEU* 2003, L 124);

– 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;

– 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;

– belangrijke entiteit: een entiteit als bedoeld in artikel 12 of 13;

– 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;

– beveiligingsscan: technisch onderzoek van netwerk- en informatiesystemen om inzicht te krijgen in kwetsbaarheden en risico's van deze systemen;

– bevoegde autoriteit: de bevoegde autoriteit, bedoeld in artikel 8, eerste lid, van de NIS2-richtlijn en bedoeld in artikel 15;

– bevoegde autoriteit van een andere lidstaat van de Europese Unie: een bevoegde autoriteit van een andere lidstaat van de Europese Unie als bedoeld in artikel 8, eerste lid, van de NIS2-richtlijn en die als zodanig is aangewezen in het nationale recht van die andere lidstaat;

– 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;

– centraal contactpunt: het centrale contactpunt, bedoeld in artikel 8, derde lid, van de NIS2-richtlijn en bedoeld in artikel 14;

– centraal contactpunt van een andere lidstaat van de Europese Unie: het centrale contactpunt van een andere lidstaat van de Europese Unie als bedoeld in artikel 8, derde lid, van de NIS2-richtlijn en dat als zodanig is aangewezen in het nationale recht van die andere lidstaat;

– CER-richtlijn: Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (*PbEU* 2022, L 333);

– 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;

– coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden: de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden, bedoeld in artikel 12, eerste lid, van de NIS2-richtlijn en bedoeld in artikel 17;

– CSIRT: een Computer security incident response team, bedoeld in artikel 10 van de NIS2-richtlijn en bedoeld in artikel 16;

– CSIRT van een andere lidstaat van de Europese Unie: een CSIRT van een andere lidstaat van de Europese Unie als bedoeld in artikel 10 van de NIS2-richtlijn en dat als zodanig is aangewezen in het nationale recht van die andere lidstaat;

– CSIRT-netwerk: het netwerk van CSIRT's, genoemd in artikel 15 van de NIS2-richtlijn;

– cyberbeveiliging: de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen;

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

– 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;

– digitale dienst: elke dienst van de informatiemaatschappij, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht, waarbij onder “op afstand” wordt verstaan: een dienst die wordt geleverd zonder dat de partijen gelijktijdig aanwezig zijn, onder “langs elektronische weg” wordt verstaan: een dienst die wordt verzonden en ontvangen via elektronische apparatuur voor de verwerking (met inbegrip van digitale compressie) en de opslag van gegevens, en die geheel via draden, radio, optische middelen of andere elektromagnetische middelen wordt verzonden, doorgeleid en ontvangen, en onder “op individueel verzoek van een afnemer van diensten” wordt verstaan: een dienst die op individueel verzoek via de transmissie van gegevens wordt geleverd;

– DNS-dienstverlener: een entiteit die openbare recursieve domeinnaamomzettingsdiensten voor interneteindgebruikers verleent, of die gezaghebbende domeinnaamomzettingsdiensten voor gebruik door derden, met uitzondering van root-naamservers, verleent;

– 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;

– elektronisch communicatienetwerk: hetgeen hieronder wordt verstaan in artikel 1.1 van de Telecommunicatiewet;

– elektronische communicatiedienst: hetgeen hieronder wordt verstaan in artikel 1.1 van de Telecommunicatiewet;

– Enisa: het Agentschap van de Europese Unie voor cyberbeveiliging, genoemd in titel II van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (*PbEU* 2019, L 151);

– entiteit: een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een maatschap als bedoeld in artikel 1655 van boek 7A van het Burgerlijk Wetboek, een vennootschap onder firma als bedoeld in artikel 16 van het Wetboek van Koophandel en een commanditaire

vennootschap als bedoeld in artikel 19 van het Wetboek van Koophandel, alsmede een samenwerkingsverband naar buitenlands recht dat met één van deze rechtsvormen vergelijkbaar is;

– entiteit die domeinnaamregistratiediensten verleent: een registrator of een agent die namens registrators optreedt, zoals een aanbieder van privacy- of proxy-registratiediensten of wederverkoper;

– essentiële entiteit: een entiteit als bedoeld in de artikelen 8, 9, 10 of 11;

– gekwalificeerde verlener van vertrouwensdiensten: een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan, bedoeld in artikel 46 ter van de Verordening (EU) nr. 910/2014, de status van gekwalificeerde heeft gekregen;

– gekwalificeerde vertrouwensdienst: een vertrouwensdienst die voldoet aan de toepasselijke eisen zoals vastgelegd in Verordening (EU) nr. 910/2014;

– hoofdvestiging: de hoofdvestiging van een entiteit, bedoeld in artikel 26, tweede lid, van de NIS2-richtlijn;

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

– ICT-product: een element of groep elementen van een netwerk- of informatiesysteem;

– 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;

– 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;

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

– 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;

– netwerk- en informatiesysteem:

a. een elektronisch communicatienetwerk; of

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;

– NIS2-richtlijn: 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 (*PbEU* 2022, L 333);

– norm: een door een erkende normalisatie-instelling vastgestelde technische specificatie voor herhaalde of voortdurende toepassing, waarvan de naleving niet verplicht is en die tot een van de volgende categorieën behoort:

a. “internationale norm”: een door een internationale normalisatie-instelling vastgestelde norm;

b. “Europese norm”: een door een Europese normalisatieorganisatie vastgestelde norm;

c. “geharmoniseerde norm”: een Europese norm die op verzoek van de Commissie is vastgesteld met het oog op de toepassing van harmonisatiewetgeving van de Unie;

d. “nationale norm”: een door een nationale normalisatie-instelling vastgestelde norm;

– 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;

– onlinemarktplaats: een dienst die gebruikmaakt van software, waaronder een website, een deel van een website of een door of namens een handelaar beheerde applicatie, en die consumenten in staat stelt op afstand overeenkomsten te sluiten met andere handelaren of consumenten;

– onlinezoekmachine: een digitale dienst die het gebruikers mogelijk maakt zoekvragen in te voeren om zoekacties uit te voeren op in beginsel alle websites of alle websites in een bepaalde taal, op basis van een zoekvraag over eender welk onderwerp in de vorm van een trefwoord, een gesproken opdracht, een frase of andere input, en die resultaten in eender welk formaat oplevert met informatie over de opgevraagde inhoud;

– Onze Minister: Onze Minister van Justitie en Veiligheid;

– openbaar elektronisch communicatienetwerk: hetgeen hieronder wordt verstaan in artikel 1.1 van de Telecommunicatiewet;

– overheidsinstantie: een entiteit die overeenkomstig het Nederlands recht als zodanig in Nederland is erkend, met uitzondering van de rechtbanken, de gerechtshoven, de Hoge Raad, het College van Beroep voor het bedrijfsleven, de Centrale Raad van Beroep, de Afdeling bestuursrechtspraak van de Raad van State, de beide Kamers der Staten-Generaal en De Nederlandsche Bank N.V., 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; en

d. zij heeft de bevoegdheid om ten aanzien van natuurlijke personen 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;

– platform voor sociale netwerkdiensten: 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;

– 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;

– Richtlijn (EU) 2018/1972: Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (*PbEU* 2018, L 321);

– 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;

– root-naamserver: een gezaghebbende naamserver voor de root-zone van het domeinnaamsysteem (DNS) van het internet;

– samenwerkingsgroep: de samenwerkingsgroep, bedoeld in artikel 14 van de NIS2-richtlijn;

– significant incident: een incident als bedoeld in artikel 25, tweede lid;

– 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;

– verlener van vertrouwensdiensten: een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten;

– Verordening (EG) nr. 300/2008: Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (*PbEU* 2008, L 97);

– Verordening (EU) nr. 910/2014: Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU* 2014, L 257), zoals laatstelijk gewijzigd bij Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (*PbEU* 2024, L 1183);

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

– Verordening (EU) 2022/2554: Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (*PbEU* 2022, L 333);

– vertegenwoordiger: een in de Europese Unie gevestigde natuurlijk persoon 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 wet;

– vertrouwensdienst: een elektronische dienst die gewoonlijk tegen betaling wordt verricht en uit één van de volgende elementen bestaat:

a. het uitgeven van certificaten voor elektronische handtekeningen, certificaten voor elektronische zegels, certificaten voor websiteauthenticatie of certificaten voor het verlenen van andere vertrouwensdiensten;

b. het valideren van certificaten voor elektronische handtekeningen, certificaten voor elektronische zegels, certificaten voor websiteauthenticatie of certificaten voor het verlenen van andere vertrouwensdiensten;

c. het aanmaken van elektronische handtekeningen of elektronische zegels;

d. het valideren van elektronische handtekeningen of elektronische zegels;

e. het bewaren van elektronische handtekeningen, elektronische zegels, certificaten voor elektronische handtekeningen of certificaten voor elektronische zegels;

f. het beheer van middelen voor het op afstand aanmaken van elektronische handtekeningen of middelen voor het op afstand aanmaken van elektronische zegels;

g. het uitgeven van elektronische attesteringen van attributen;

h. het valideren van elektronische attesteringen van attributen;

i. het aanmaken van elektronische tijdstempels;

j. het valideren van elektronische tijdstempels;

k. het verlenen van diensten voor elektronisch aangetekende bezorging;

l. het valideren van gegevens die via diensten voor elektronisch aangetekende bezorging zijn verzonden en het bewijs daarvoor;

m. het elektronisch archiveren van elektronische gegevens en elektronische documenten;

n. het opslaan van elektronische gegevens in elektronische registers.

HOOFDSTUK 2. ALGEMEEN

Artikel 2 (doel van deze wet)

Deze wet is, met het oog op het in stand houden van kritieke maatschappelijke of economisch belangrijke functies of activiteiten, gericht op het verhogen van de cyberbeveiliging door regels te stellen ten aanzien van:

a. het beheersen van risico’s voor de beveiliging van netwerk- en informatiesystemen;

b. het voorkomen van incidenten;

c. het beperken van gevolgen van incidenten; en

d. het verkrijgen en verstrekken van informatie over incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden.

Artikel 3 (uitvoering uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren)

Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld ter uitvoering van de op grond van de NIS2-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren.

HOOFDSTUK 3. TOEPASSINGSBEREIK EN JURISDICTIE

Artikel 4 (toepassingsbereik en jurisdictie)

1. Het bepaalde bij of krachtens deze wet met betrekking tot essentiële entiteiten en belangrijke entiteiten is van toepassing op die entiteiten, indien zij in Nederland zijn gevestigd en hun diensten verlenen of hun activiteiten verrichten in Nederland of een andere lidstaat van de Europese Unie.

2. In afwijking van het eerste lid is het bepaalde bij of krachtens deze wet met betrekking tot essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn, van toepassing op die aanbieders, indien zij hun diensten in Nederland aanbieden.

3. In afwijking van het eerste lid is het bepaalde bij of krachtens deze wet met betrekking tot essentiële entiteiten en belangrijke entiteiten van toepassing op de volgende entiteiten, indien zij hun hoofdvestiging of vertegenwoordiger in Nederland hebben en hun diensten verlenen of hun activiteiten verrichten in Nederland of een andere lidstaat van de Europese Unie:

a. DNS-dienstverleners;
b. registers voor topleveldomeinnamen;
c. aanbieders van cloudcomputingdiensten;
d. aanbieders van datacentrumdiensten;
e. aanbieders van netwerken voor de levering van inhoud;
f. aanbieders van beheerde diensten;
g. aanbieders van beheerde beveiligingsdiensten;
h. aanbieders van onlinemarktplaatsen;
i. aanbieders van onlinezoekmachines;
j. aanbieders van platforms voor socialenetwerkdiensten.

4. Het bepaalde bij of krachtens deze wet met betrekking tot entiteiten die domeinnaamregistratiediensten verlenen is van toepassing op die entiteiten, indien zij hun hoofdvestiging of vertegenwoordiger in Nederland hebben.

5. Een entiteit als bedoeld in het derde of vierde lid wordt geacht haar hoofdvestiging in Nederland te hebben indien de beslissingen met betrekking tot de maatregelen voor het beheersen van cyberbeveiligingsrisico’s hoofdzakelijk in Nederland worden genomen. Indien deze beslissingen niet hoofdzakelijk in Nederland of een andere lidstaat van de Europese Unie worden genomen of indien niet kan worden bepaald in welke lidstaat van de Europese Unie die beslissingen hoofdzakelijk worden genomen, wordt de hoofdvestiging geacht zich in Nederland te bevinden indien de cyberbeveiligingsactiviteiten in Nederland worden uitgevoerd. Indien de cyberbeveiligingsactiviteiten niet in Nederland of een andere lidstaat van de Europese Unie worden uitgevoerd of niet kan worden bepaald in welke lidstaat van de Europese Unie de cyberbeveiligingsactiviteiten worden uitgevoerd, wordt de hoofdvestiging geacht zich te bevinden in Nederland indien de vestiging van de betrokken entiteit in Nederland het grootste aantal werknemers in de Europese Unie heeft.

6. Onverminderd het eerste, derde en vierde lid is het bepaalde bij of krachtens de artikelen 42, 60 en 61 van toepassing.

Artikel 5 (overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving)

1. Deze wet, met uitzondering van artikel 96, is niet van toepassing op:

a. het Ministerie van Defensie;
b. de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017;
c. het openbaar ministerie;
d. de politie;
e. de veiligheidsregio's, bedoeld in artikel 9 van de Wet veiligheidsregio's; en
f. indien van toepassing, de andere bij algemene maatregel van bestuur aangewezen overheidsinstanties die in hoofdzaak 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.

2. In afwijking van het eerste lid is deze wet wel van toepassing op overheidsinstanties als bedoeld in het eerste lid, wanneer en voor zover zij optreden als verleners van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers.

Artikel 6 (root-naamservers)

Deze wet is niet van toepassing op root-naamservers.

Artikel 7 (entiteiten uitgezonderd van Verordening (EU) 2022/2554)

Deze wet is niet van toepassing op de entiteiten die zijn uitgezonderd van de Verordening (EU) 2022/2554 op grond van artikel 2, vierde lid, van die verordening.

HOOFDSTUK 4. ESSENTIËLE ENTITEITEN EN BELANGRIJKE ENTITEITEN

§ 4.1 Essentiële entiteiten

Artikel 8 (essentiële entiteit van rechtswege)

1. De volgende entiteiten zijn essentiële entiteiten:
a. gekwalificeerde verleners van vertrouwensdiensten;
b. aanbieders van registers voor topleveldomeinnamen;
c. DNS-dienstverleners;
d. aanbieders van openbare elektronische communicatienetwerken, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;
e. aanbieders van openbare elektronische communicatiediensten, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;

f. andere entiteiten, genoemd in bijlage 1 van deze wet, die de in artikel 2, eerste lid, van de bijlage bij Aanbeveling 2003/361/EG bedoelde drempel voor middelgrote ondernemingen overschrijden;

g. de ministeries, met inbegrip van de daartoe behorende dienstonderdelen doch met uitzondering van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017, en zelfstandige bestuursorganen van de centrale overheid, voor zover deze zelfstandige bestuursorganen kwalificeren als overheidsinstantie;

h. provincies, gemeenten en waterschappen, alsmede openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties als bedoeld in artikel 8, eerste, tweede, onderscheidenlijk derde lid, van de Wet gemeenschappelijke regelingen, voor zover deze openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties kwalificeren als overheidsinstantie;

i. kritieke entiteiten als bedoeld in artikel 6, eerste lid, van de Wet weerbaarheid kritieke entiteiten.

2. Ten aanzien van het bepaalde in het eerste lid, onderdelen d tot en met f, is artikel 3, vierde lid, van de bijlage bij Aanbeveling 2003/361/EG niet van toepassing.

Artikel 9 (essentiële entiteit op basis van criteria)

1. Bij regeling of besluit van Onze Minister die het aangaat, na overleg met Onze Minister, wordt een in bijlage 1 of bijlage 2 van deze wet genoemde entiteit aangewezen als essentiële entiteit, op grond van de toepasselijkheid van één of meer van de volgende criteria:

a. de entiteit is in Nederland de enige aanbieder van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten;

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

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

d. de entiteit is kritiek 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 Nederland.

2. Onze Minister die het aangaat trekt de aanwijzing in, indien de entiteit niet langer voldoet aan één of meer van de criteria, genoemd in het eerste lid.

Artikel 10 (essentiële entiteit die aanbieder van een essentiële dienst was)

Bij regeling of besluit van Onze Minister die het aangaat, na overleg met Onze Minister, kan worden aangewezen als essentiële entiteit: een aanbieder die voor 16 januari 2023 op grond van de Wet beveiliging

netwerk- en informatiesystemen is aangewezen als aanbieder van een essentiële dienst.

Artikel 11 (aanwijzing instelling voor hoger onderwijs als essentiële entiteit)

1. Bij regeling of besluit van Onze Minister van Onderwijs, Cultuur en Wetenschap, na overleg met Onze Minister, kan een instelling voor hoger onderwijs als bedoeld in artikel 1.1, onder g, van de Wet op het hoger onderwijs en wetenschappelijk onderzoek als essentiële entiteit worden aangewezen.
2. Onze Minister van Onderwijs, Cultuur en Wetenschap trekt de aanwijzing, bedoeld in het eerste lid, in, indien er voor die aanwijzing geen grond meer aanwezig is.

§ 4.2 Belangrijke entiteiten

Artikel 12 (belangrijke entiteit van rechtswege)

1. De volgende entiteiten zijn belangrijke entiteiten:
a. entiteiten, genoemd in bijlage 1 van deze wet, niet zijnde een essentiële entiteit, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG;
b. entiteiten, genoemd in bijlage 2 van deze wet, niet zijnde een essentiële entiteit, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG of de in het eerste lid van laatstgenoemd artikel vastgestelde drempels voor middelgrote ondernemingen overschrijden;
c. aanbieders van openbare elektronische communicatienetwerken, genoemd in bijlage 1 van deze wet, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit;
d. aanbieders van openbare elektronische communicatiediensten, genoemd in bijlage 1 van deze wet, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit;
e. verleners van vertrouwensdiensten, genoemd in bijlage 1 van deze wet, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit.
2. Ten aanzien van het bepaalde in het eerste lid is artikel 3, vierde lid, van de bijlage bij de Aanbeveling 2003/361/EG niet van toepassing.

Artikel 13 (aanwijzing instelling voor hoger onderwijs als belangrijke entiteit)

1. Bij regeling of besluit van Onze Minister van Onderwijs, Cultuur en Wetenschap, na overleg met Onze Minister, kan een instelling voor hoger onderwijs als bedoeld in artikel 1.1, onder g, van de Wet op het hoger

onderwijs en wetenschappelijk onderzoek als belangrijke entiteit worden aangewezen.

2. Onze Minister van Onderwijs, Cultuur en Wetenschap trekt de aanwijzing, bedoeld in het eerste lid, in, indien er voor die aanwijzing geen grond meer aanwezig is.

HOOFDSTUK 5. AANWIJZING EN TAKEN VAN INSTANTIES

Artikel 14 (aanwijzing en taken centraal contactpunt)

Onze Minister is het centrale contactpunt en heeft in die hoedanigheid de volgende taken:

a. het zorgen voor grensoverschrijdende samenwerking van de autoriteiten van Nederland met de relevante autoriteiten van andere lidstaten van de Europese Unie, de Europese Commissie en Enisa, door middel van het vervullen van een verbindingsfunctie;

b. het zorgen voor sectoroverschrijdende samenwerking tussen de bevoegde autoriteiten binnen Nederland, door middel van het vervullen van een verbindingsfunctie; en

c. de overige in deze wet genoemde taken.

Artikel 15 (aanwijzing en taken bevoegde autoriteit)

1. De bevoegde autoriteit is voor de entiteiten in de sectoren en subsectoren, genoemd in bijlage 1 en bijlage 2 van deze wet:

Bevoegde autoriteit	***Sector***	***Subsector (indien van toepassing)***
Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties	overheid	centrale overheden
		decentrale overheden, uitgezonderd de waterschappen
Onze Minister van Economische Zaken	digitale infrastructuur	
	beheer van ICT-diensten (business-to-business)	
	ruimtevaart	
	post- en koeriersdiensten	
	vervaardiging	vervaardiging van informaticaproducten en van elektronische en optische producten

		vervaardiging van elektrische apparatuur
		vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd
		vervaardiging van motorvoertuigen, aanhangers en opleggers
		vervaardiging van andere transportmiddelen
	digitale aanbieders	
Onze Minister van Financiën	bankwezen	
	infrastructuur voor de financiële markt	
Onze Minister van Infrastructuur en Waterstaat	vervoer	lucht
		spoor
		water
		weg
	drinkwater	
	afvalwater	
	afvalstoffenbeheer	
	vervaardiging, productie en distributie van chemische stoffen	
	overheid	decentrale overheden, alleen voor wat betreft de waterschappen
Onze Minister van Klimaat en Groene Groei	energie	elektriciteit
		stadsverwarming en -koeling
		aardolie
		aardgas
		waterstof
Onze Minister van Landbouw, Visserij, Voedselzekerheid en Natuur	productie, verwerking en distributie van levensmiddelen	
Onze Minister van Volksgezondheid, Welzijn en Sport	gezondheidszorg	
	vervaardiging	vervaardiging van medische

		hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek

2. Onze Minister van Economische Zaken is de bevoegde autoriteit voor de entiteiten die domeinnaamregistratiediensten verlenen.

3. Onze Minister van Onderwijs, Cultuur en Wetenschap is de bevoegde autoriteit voor de instellingen voor hoger onderwijs als bedoeld in artikel 1.1, onder g, van de Wet op het hoger onderwijs en wetenschappelijk onderzoek, die op grond van artikel 11 zijn aangewezen als essentiële entiteit of op grond van artikel 13 zijn aangewezen als belangrijke entiteit.

4. De bevoegde autoriteit voor een entiteit in de sector onderzoek, genoemd in bijlage 2 van deze wet, is Onze Minister die is aangewezen als bevoegde autoriteit voor de entiteiten in de sector of subsector waarin de betrokken entiteit haar onderzoeksactiviteiten verricht. De bevoegde autoriteit voor een entiteit in de sector onderzoek, genoemd in bijlage 2 van deze wet, die niet valt in een sector of subsector waarvoor reeds een bevoegde autoriteit is aangewezen, is Onze Minister die het aangaat.

5. De bevoegde autoriteit, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten, van een op grond van artikel 6, eerste lid, van de Wet weerbaarheid kritieke entiteiten aangewezen kritieke entiteit is tevens de bevoegde autoriteit in de zin van deze wet voor die entiteit.

6. De bevoegde autoriteit heeft de volgende taken:

a. het zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens deze wet ten aanzien van essentiële entiteiten, belangrijke entiteiten, entiteiten die domeinnaamregistratiediensten verlenen en leden van het bestuur van essentiële entiteiten en belangrijke entiteiten;

b. het zorgen voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie; en

c. de overige in deze wet genoemde taken van de bevoegde autoriteit.

Artikel 16 (aanwijzing, taken en eisen CSIRT)

1. Bij of krachtens algemene maatregel van bestuur wordt het CSIRT aangewezen voor elke essentiële entiteit en belangrijke entiteit.

2. Het CSIRT heeft de volgende taken:

a. het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en het op verzoek verlenen van bijstand aan de betrokken essentiële entiteit of belangrijke entiteit met betrekking tot het realtime of bijna-realtime monitoren van haar netwerk- en informatiesysteem;

b. het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie aan de betrokken

essentiële entiteit of belangrijke entiteit, de bevoegde autoriteiten, Onze Minister van Economische Zaken, ten behoeve van de uitvoering van de taken, bedoeld in artikel 2, eerste lid, van de Wet bevordering digitale weerbaarheid bedrijven, en andere relevante partijen over cyberdreigingen, kwetsbaarheden en incidenten, indien mogelijk in bijna-realtime;

c. indien van toepassing, het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële entiteit of belangrijke entiteit;

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

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

f. het deelnemen aan het CSIRT-netwerk en, in overeenstemming met zijn capaciteiten en bevoegdheden, het verlenen van wederzijdse bijstand aan andere leden van het CSIRT-netwerk op verzoek van een lid van dat netwerk;

g. het deelnemen aan de op grond van artikel 19 van de NIS2-richtlijn georganiseerde collegiale toetsingen;

h. indien van toepassing, het optreden als coördinator ten behoeve van het proces van gecoördineerde bekendmaking van kwetsbaarheden, bedoeld in artikel 17; en

i. het bijdragen aan de uitrol van veilige instrumenten voor het delen van informatie, bedoeld in artikel 10, derde lid, van de NIS2-richtlijn.

3. Het CSIRT kan een openbaar toegankelijk netwerk- en informatiesysteem van een essentiële entiteit en belangrijke entiteit proactief en niet-intrusief scannen met het oog op het opsporen van een kwetsbaar of onveilig geconfigureerd netwerk- en informatiesysteem en het informeren van de betrokken entiteit. Deze scan leidt niet tot negatieve gevolgen voor de dienstverlening van de betrokken entiteit.

4. Bij de uitvoering van de taken, bedoeld in het tweede en derde lid, kan het CSIRT op grond van een risicogebaseerde benadering prioriteit geven aan bepaalde taken.

5. Het CSIRT brengt samenwerkingsrelaties tot stand met essentiële entiteiten, belangrijke entiteiten, Onze Minister van Economische Zaken en andere relevante partijen, teneinde de doelstellingen van deze wet te verwezenlijken.

6. Met het oog op de samenwerking, bedoeld in het vijfde lid, bevordert het CSIRT 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.

7. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de functionele, financiële, technische en organisatorische vereisten ten aanzien van de organisatie die bij of krachtens algemene maatregel van bestuur als CSIRT wordt aangewezen.

Artikel 17 (aanwijzing en taken coördinator bekendmaking kwetsbaarheden)

1. Bij of krachtens algemene maatregel van bestuur wordt een CSIRT aangewezen als de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.
2. De coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden heeft de volgende taken:
a. het optreden als tussenpersoon en het waar nodig vergemakkelijken van de interactie tussen de natuurlijke persoon of rechtspersoon die een kwetsbaarheid op grond van artikel 34 meldt en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten, op verzoek van een van beide partijen;
b. het identificeren van en contact opnemen met de betrokken entiteiten;
c. het bijstaan van de natuurlijke persoon of rechtspersoon die een kwetsbaarheid meldt;
d. het onderhandelen over tijdschema’s voor de bekendmaking en het beheren van kwetsbaarheden die van invloed zijn op meerdere entiteiten; en
e. wanneer een gemelde kwetsbaarheid significante gevolgen kan hebben voor entiteiten in meer dan één lidstaat van de Europese Unie: het binnen het CSIRT-netwerk samenwerken met de door andere lidstaten van de Europese Unie aangewezen coördinatoren met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.

Artikel 18 (aanwijzing en taken cybercrisisbeheerautoriteit)

Onze Minister is de cybercrisisbeheerautoriteit, bedoeld in artikel 9, eerste lid, van de NIS2-richtlijn, en heeft in die hoedanigheid de taken die zijn opgenomen in het nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons, genoemd in artikel 20.

HOOFDSTUK 6. NATIONALE CYBERBEVEILIGINGSSTRATEGIE EN NATIONAAL PLAN VOOR GROOTSCHALIGE CYBERBEVEILIGINGSINCIDENTEN EN CRISISRESPONS

Artikel 19 (nationale cyberbeveiligingsstrategie)

1. Onze Minister stelt in overeenstemming met Onze Ministers die het aangaan een nationale cyberbeveiligingsstrategie als bedoeld in artikel 7, eerste lid, van de NIS2-richtlijn vast.
2. In het kader van de nationale cyberbeveiligingsstrategie stelt Onze Minister respectievelijk Onze Minister die het aangaat beleid vast over de in artikel 7, tweede lid, van de NIS2-richtlijn genoemde onderwerpen die onder zijn beleidsverantwoordelijkheid vallen.
3. Onze Minister beoordeelt in overeenstemming met Onze Ministers die het aangaan de nationale cyberbeveiligingsstrategie regelmatig en ten

minste om de vijf jaar, op basis van kernprestatie-indicatoren. Hij werkt de nationale cyberbeveiligingsstrategie in overeenstemming met Onze Minister die het aangaat zo nodig bij.

Artikel 20 (nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons)

Onze Minister stelt een nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons als bedoeld in artikel 9, vierde lid, van de NIS2-richtlijn vast.

HOOFDSTUK 7. ZORGPLICHT EN GOVERNANCE

Artikel 21 (zorgplicht)

1. De essentiële entiteit of belangrijke entiteit neemt passende en evenredige technische, operationele en organisatorische maatregelen om de risico’s voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. Ook neemt zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken.
2. De maatregelen, bedoeld in het eerste lid, zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico’s, bedoeld in het eerste lid. Bij het nemen van de maatregelen houdt de entiteit in ieder geval rekening met de stand van de techniek, de uitvoeringskosten en, indien van toepassing, de desbetreffende Europese en internationale normen. Ten aanzien van de evenredigheid van de maatregelen, bedoeld in het eerste lid, houdt de entiteit naar behoren rekening met de mate waarin zij 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.
3. De maatregelen, bedoeld in het eerste lid, 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 herstelplannen, en crisisbeheer;
d. de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen de 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 beheersen van cyberbeveiligingsrisico’s te beoordelen;

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

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

i. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets; en

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

4. Wanneer de entiteit overweegt welke maatregelen als bedoeld in het derde lid, onderdeel d, passend zijn, houdt zij rekening met:

a. de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener;

b. de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van haar leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures; en

c. de resultaten van de door de samenwerkingsgroep op grond van artikel 22, eerste lid, van de NIS2-richtlijn uitgevoerde gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens.

5. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de maatregelen, bedoeld in het eerste lid, en kunnen met betrekking tot die maatregelen eisen worden gesteld aan entiteiten, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten.

6. De voordracht voor een krachtens het vijfde lid vast te stellen algemene maatregel van bestuur wordt niet eerder gedaan dan vier weken nadat het ontwerp aan beide Kamers der Staten-Generaal is overgelegd.

Artikel 21a (weren producten en diensten van leveranciers)

1. Indien dat naar het oordeel van Onze Minister die het aangaat, ter uitwerking van artikel 21, noodzakelijk is om risico’s voor de beveiliging van netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen, legt hij in overeenstemming met Onze Minister een essentiële entiteit of een belangrijke entiteit de verplichting op om in de daarbij aangewezen onderdelen van haar netwerk- en informatiesystemen uitsluitend gebruik te maken van producten of diensten van anderen dan de daarbij door Onze Minister die het aangaat genoemde partij die:

a. een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft om de beveiliging van de netwerk- en informatiesystemen van de essentiële entiteit of belangrijke entiteit aan te tasten of om incidenten bij de essentiële entiteit of belangrijke entiteit te veroorzaken; of

b. nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld in onderdeel a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

2. In het kader van de beoordeling van de noodzaak, bedoeld in het eerste lid, beoordeelt Onze Minister die het aangaat in elk geval of beheersmaatregelen mogelijk en realiseerbaar zijn die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen.

3. Indien de verplichting, bedoeld in het eerste lid, betrekking heeft op reeds in gebruik zijnde producten en diensten ten behoeve van de daarbij aangewezen onderdelen, stelt Onze Minister die het aangaat in het belang van de continuïteit van de dienstverlening een termijn vast voor het vervangen respectievelijk beëindigen van de betreffende producten en diensten.

4. Het eerste lid is niet van toepassing ten aanzien van essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn.

Artikel 22 (sectorspecifieke rechtshandelingen zorgplicht)

1. Indien sectorspecifieke rechtshandelingen van de Europese Unie voorschrijven dat een essentiële entiteit of belangrijke entiteit risicobeheersmaatregelen op het gebied van cyberbeveiliging neemt en indien deze verplichtingen ten minste gelijkwaardig zijn aan de verplichtingen, bedoeld in artikel 21, is artikel 21 niet van toepassing op die entiteit.

2. De verplichtingen, bedoeld in het eerste lid, worden geacht gelijkwaardig te zijn aan de verplichtingen, bedoeld in artikel 21, wanneer de door sectorspecifieke rechtshandelingen van de Europese Unie voorgeschreven risicobeheersmaatregelen op het gebied van cyberbeveiliging ten minste een vergelijkbare uitwerking hebben als de verplichtingen, bedoeld in artikel 21.

Artikel 23 (ontheffing zorgplicht)

1. Onze Minister die het aangaat kan bij regeling of besluit, in overeenstemming met Onze Minister, een essentiële entiteit respectievelijk een belangrijke entiteit die activiteiten uitvoert op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving of die uitsluitend diensten verleent aan een overheidsinstantie als bedoeld in artikel 5, eerste lid, met betrekking tot die activiteiten of diensten ontheffen van de verplichtingen, bedoeld in artikel 21.

2. Het eerste lid is niet van toepassing wanneer en voor zover een entiteit optreedt als verlener van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers.

Artikel 24 (governance)

1. De maatregelen, bedoeld in artikel 21, behoeven de goedkeuring van het bestuur van de essentiële entiteit of belangrijke entiteit.

2. Ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit beschikt over kennis en vaardigheden om:

a. risico’s voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren;

b. risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen; en

c. de gevolgen van de risico’s en risicobeheersmaatregelen voor de diensten die door de entiteit worden verleend te kunnen beoordelen.

3. Ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit voldoet binnen twee jaar na de inwerkingtreding van het tweede lid aan het bepaalde in het tweede lid. Indien een lid na de inwerkingtreding van het tweede lid wordt benoemd, voldoet dit lid binnen twee jaar na diens benoeming aan het bepaalde in het tweede lid.

4. Ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit houdt de kennis en vaardigheden, bedoeld in het tweede lid, aantoonbaar actueel.

5. Met het oog op het aantonen van de kennis en vaardigheden bezit ieder lid van het bestuur van een essentiële entiteit of belangrijke entiteit een certificaat, waaruit de deelname blijkt aan een training die de onderwerpen, bedoeld in het tweede lid, behandelt.

6. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de training en het certificaat, bedoeld in het vijfde lid, waaronder de duur en het niveau van de training.

7. Indien een rechtspersoon het bestuur of een lid van het bestuur van een essentiële entiteit of belangrijke entiteit is, is het bepaalde bij of krachtens het tweede tot en met zesde lid van overeenkomstige toepassing op de natuurlijke persoon of natuurlijke personen die namens die rechtspersoon zitting heeft of hebben in het bestuur van de essentiële entiteit of belangrijke entiteit.

8. Indien de essentiële entiteit of belangrijke entiteit toepassing heeft gegeven aan de artikelen 129a of 239a van Boek 2 van het Burgerlijk Wetboek, is het bepaalde bij of krachtens het eerste tot en met zesde lid uitsluitend van toepassing op de uitvoerende bestuurders van die essentiële entiteit of belangrijke entiteit.

9. Indien de essentiële entiteit of belangrijke entiteit een maatschap is, is het bepaalde bij of krachtens het eerste tot en met zesde lid van overeenkomstige toepassing op iedere maat van die maatschap.

10. Indien de essentiële entiteit of belangrijke entiteit een vennootschap onder firma is, is het bepaalde bij of krachtens het eerste tot en met zesde lid van overeenkomstige toepassing op iedere vennoot van die vennootschap onder firma.

11. Indien de essentiële entiteit of belangrijke entiteit een commanditaire vennootschap is, is het bepaalde bij of krachtens het eerste tot en met zesde lid van overeenkomstige toepassing op de beherende vennoten van die commanditaire vennootschap.

12. Indien de essentiële entiteit een overheidsinstantie is, wordt voor de toepassing van dit artikel als het bestuur aangemerkt:

a. bij ministeries: de minister;

b. bij zelfstandige bestuursorganen van de centrale overheid: het zelfstandige bestuursorgaan;

c. bij provincies: gedeputeerde staten;
d. bij gemeenten: het college van burgemeester en wethouders;
e. bij waterschappen: het dagelijks bestuur;
f. bij gemeenschappelijke regelingen: het dagelijks bestuur van het openbaar lichaam, het bestuur van de bedrijfsvoeringsorganisatie onderscheidenlijk het gemeenschappelijk orgaan.
13. Dit artikel is niet van toepassing op een essentiële entiteit of belangrijke entiteit indien artikel 21 niet van toepassing is op die entiteit.

HOOFDSTUK 8. SIGNIFICANTE INCIDENTEN, INCIDENTEN, BIJNA-INCIDENTEN, SIGNIFICANTE CYBERDREIGINGEN, CYBERDREIGINGEN EN KWETSBAARHEDEN

§ 8.1 Meldplicht

Artikel 25 (meldplicht significante incidenten)

1. De essentiële entiteit of belangrijke entiteit meldt overeenkomstig de artikelen 26 tot en met 29 ieder significant incident.
2. Een incident is een significant incident als het:
a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of
b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.
3. Bij of krachtens algemene maatregel van bestuur kunnen de criteria worden vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in het tweede lid, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten.
4. Ten aanzien van de entiteiten waarvoor in uitvoeringshandelingen op grond van artikel 23, elfde lid, van de NIS2-richtlijn nader is gespecificeerd in welke gevallen een incident bij die entiteiten als significant wordt beschouwd, kunnen bij of krachtens algemene maatregel van bestuur naast de hiervoor bedoelde specificaties in uitvoeringshandelingen, aanvullende criteria worden vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in het tweede lid, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren, soorten entiteiten en entiteiten.

Artikel 26 (vroegtijdige waarschuwing)

1. De essentiële entiteit of belangrijke entiteit geeft ten behoeve van de melding, bedoeld in artikel 27, eerste lid, een vroegtijdige waarschuwing over het significante incident aan haar CSIRT en haar bevoegde autoriteit. Dit doet zij onverwijld of, indien dat niet mogelijk is, binnen 24 uur nadat zij kennis heeft gekregen van het significante incident.
2. Bij de vroegtijdige waarschuwing, bedoeld in het eerste lid:
a. geeft de entiteit aan of het significante incident vermoedelijk door een onrechtmatige of kwaadwillige handeling is veroorzaakt;

b. geeft de entiteit aan of het significante incident grensoverschrijdende gevolgen kan hebben; en

c. verstrekt de entiteit de contactgegevens van de functionaris die verantwoordelijk is voor de melding.

Artikel 27 (melding, update en initiële beoordeling)

1. De essentiële entiteit of belangrijke entiteit dient onverwijld of, indien dat niet mogelijk is, binnen 72 uur nadat zij kennis heeft gekregen van het significante incident een melding in bij haar CSIRT en haar bevoegde autoriteit met:

a. indien van toepassing, een update van de informatie, bedoeld in artikel 26;

b. indien van toepassing, een initiële beoordeling van het significante incident, met inbegrip van de ernst en de gevolgen ervan;

c. indien van toepassing en beschikbaar, de indicatoren voor aantasting; en

d. alle beschikbare informatie die het CSIRT en de bevoegde autoriteit in staat stelt om eventuele grensoverschrijdende gevolgen van het incident te bepalen.

2. In afwijking van het eerste lid dient een essentiële entiteit of belangrijke entiteit die een vertrouwensdienst aanbiedt onverwijld of, indien dat niet mogelijk is, binnen 24 uur nadat zij kennis heeft gekregen van het significante incident een melding van het significante incident in bij haar CSIRT en haar bevoegde autoriteit als dat incident gevolgen heeft voor de verlening van haar vertrouwensdienst.

Artikel 28 (tussentijds verslag)

De essentiële entiteit of belangrijke entiteit dient in het kader van de melding, bedoeld in artikel 27, eerste lid, op verzoek van haar CSIRT of haar bevoegde autoriteit een tussentijds verslag in over relevante updates van de situatie.

Artikel 29 (voortgangsverslag en eindverslag)

1. De essentiële entiteit of belangrijke entiteit dient uiterlijk één maand na de melding, bedoeld in artikel 27, eerste lid, een eindverslag in bij haar CSIRT en haar bevoegde autoriteit waarin het volgende is opgenomen:

a. een gedetailleerde beschrijving van het incident, de ernst en de gevolgen ervan;

b. het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;

c. toegepaste en lopende risicobeperkende maatregelen; en

d. in voorkomend geval, de grensoverschrijdende gevolgen van het incident.

2. Indien het incident nog voortduurt op het moment dat het eindverslag had moeten worden ingediend, dient de essentiële entiteit of belangrijke entiteit op dat moment in plaats van een eindverslag een voortgangsverslag in waarin wordt ingegaan op de aspecten, genoemd in

het eerste lid. Zij dient een eindverslag in binnen één maand nadat het incident is afgehandeld.

§ 8.2 Informeren van ontvangers van diensten

Artikel 30 (informeren van ontvangers van diensten)

1. De essentiële entiteit of belangrijke entiteit stelt in voorkomend geval onverwijld de ontvangers van haar diensten in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten.
2. De essentiële entiteit of belangrijke entiteit deelt de ontvangers van haar diensten, die mogelijkerwijs door een significante cyberdreiging in relatie tot het ontvangen van die diensten worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stelt de entiteit die ontvangers ook in kennis van de desbetreffende significante cyberdreiging.

§ 8.3 Sectorspecifieke rechtshandelingen en ontheffing

Artikel 31 (sectorspecifieke rechtshandelingen meldplicht)

1. Indien sectorspecifieke rechtshandelingen van de Europese Unie voorschrijven dat een essentiële entiteit of belangrijke entiteit significante incidenten moet melden en indien deze eisen ten minste gelijkwaardig zijn aan die uit deze wet, zijn de verplichtingen uit de artikelen 25 tot en met 30 niet van toepassing op die specifieke entiteit.
2. De eisen, bedoeld in het eerste lid, worden geacht gelijkwaardig te zijn wanneer de sectorspecifieke rechtshandeling voorziet in onmiddellijke toegang, in voorkomend geval automatisch en rechtstreeks, tot de meldingen van incidenten door het CSIRT, de bevoegde autoriteit of het centrale contactpunt, en wanneer de eisen voor het melden van significante incidenten ten minste een vergelijkbare uitwerking hebben als de eisen, bedoeld in de artikelen 25 tot en met 30, 36 en 39, eerste en tweede lid.

Artikel 32 (ontheffing meldplicht)

1. Onze Minister die het aangaat kan bij regeling of besluit, in overeenstemming met Onze Minister, een essentiële entiteit of belangrijke entiteit die activiteiten uitvoert op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving of die uitsluitend diensten verleent aan een overheidsinstantie als bedoeld in artikel 5, eerste lid, met betrekking tot die activiteiten of diensten ontheffen van de verplichtingen, bedoeld in de artikelen 25 tot en met 30.
2. Het eerste lid is niet van toepassing wanneer een entiteit optreedt als verlener van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers.

§ 8.4 Vrijwillige meldingen

Artikel 33 (vrijwillige meldingen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)

1. Onverminderd artikel 25 kan op vrijwillige basis een melding worden ingediend door:
a. een essentiële entiteit of belangrijke entiteit bij haar CSIRT, over incidenten, bijna-incidenten en cyberdreigingen;
b. eenieder bij een CSIRT, over significante incidenten als bedoeld in artikel 25, tweede lid, incidenten, bijna-incidenten en cyberdreigingen.
2. Het CSIRT verwerkt de vrijwillige meldingen, bedoeld in het eerste lid, overeenkomstig de in artikel 36 omschreven procedure. Het CSIRT kan daarbij voorrang geven aan de verwerking van verplichte meldingen als bedoeld in artikel 25 boven vrijwillige meldingen als bedoeld in het eerste lid.
3. Het CSIRT kan de vrijwillige melding ter behandeling doorsturen naar een ander CSIRT.

Artikel 34 (vrijwillige meldingen van kwetsbaarheden)

1. Eenieder kan op vrijwillige basis een melding maken van een kwetsbaarheid bij de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.
2. De melding kan anoniem worden gedaan.
3. De coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden geeft opvolging aan de melding door het verrichten van de taken, genoemd in artikel 17, tweede lid, en waarborgt de anonimiteit van de natuurlijke persoon of rechtspersoon die de kwetsbaarheid meldt.

§ 8.5 Nadere regels

Artikel 35 (nadere regels over meldingen)

Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld ter uitwerking van de artikelen 26 tot en met 30, 33 en 34, waaronder regels over de gegevens waar de vroegtijdige waarschuwing, de melding, het tussentijds verslag en het eindverslag in ieder geval uit moeten bestaan en de wijze waarop dit geschiedt.

§ 8.6 Taken en bevoegdheden van het CSIRT en de bevoegde autoriteit bij significante incidenten en significante cyberdreigingen

Artikel 36 (taken CSIRT na melding significant incident)

1. Het CSIRT verstrekt onverwijld en zo mogelijk binnen 24 uur na ontvangst van de vroegtijdige waarschuwing, bedoeld in artikel 26, een antwoord aan de meldende entiteit, met inbegrip van een eerste terugkoppeling over het significante incident en, op verzoek van de

entiteit, richtsnoeren of operationeel advies voor de uitvoering van mogelijke risicobeperkende maatregelen.

2. Het CSIRT verleent aanvullende technische ondersteuning indien de betrokken entiteit daar om verzoekt.

3. Wanneer wordt vermoed dat het significante incident van criminele aard is, geeft het CSIRT ook richtsnoeren aan de meldende entiteit voor het melden van het significante incident aan de rechtshandhavingsinstanties.

Artikel 37 (openbaarmaking significant incident door CSIRT of bevoegde autoriteit)

Het CSIRT respectievelijk de bevoegde autoriteit kan, na raadpleging van de betrokken entiteit, het publiek informeren over een significant incident of de entiteit verplichten om dit te doen, wanneer:

a. publieke bewustmaking nodig is om een significant incident te voorkomen;

b. dat nodig is om een lopend incident te beheersen; of

c. de bekendmaking van het significante incident anderszins in het algemeen belang is.

Artikel 38 (inkennisstelling natuurlijke personen of rechtspersonen door entiteit)

De bevoegde autoriteit kan de essentiële entiteit of belangrijke entiteit verplichten om de natuurlijke personen of rechtspersonen aan wie de entiteit diensten verleent of voor wie de entiteit activiteiten uitvoert en 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 personen of rechtspersonen kunnen nemen als reactie op die dreiging.

§ 8.7 Informatieverstrekking in verband met meldingen

Artikel 39 (informatieverstrekking over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)

1. Het CSIRT stelt het centrale contactpunt in kennis van de op grond van artikel 25 ontvangen meldingen van significante incidenten en, indien nodig, van de op grond van artikel 33, eerste lid, onderdeel a, ontvangen vrijwillige meldingen van incidenten, bijna-incidenten en cyberdreigingen. In geval van een grensoverschrijdend of sectoroverschrijdend significant incident, zorgt het CSIRT ervoor dat de relevante informatie die hierover is gemeld tijdig aan het centrale contactpunt wordt verstrekt.

2. Als dat passend is en in elk geval als het aan het CSIRT gemelde incident, bijna-incident of cyberdreiging, bedoeld in het eerste lid, betrekking heeft op twee of meer lidstaten van de Europese Unie, stelt het centrale contactpunt de centrale contactpunten van de andere getroffen lidstaten en Enisa onverwijld daarvan in kennis. Die kennisgeving omvat, in geval van een significant incident, de informatie

die overeenkomstig de artikelen 26 tot en met 29 is ontvangen. Daarbij beschermt het centrale contactpunt de beveiligingsbelangen en commerciële belangen van de entiteit en de vertrouwelijkheid van de verstrekte informatie.

3. Op verzoek van het CSIRT of de bevoegde autoriteit stuurt het centrale contactpunt de op grond van de artikelen 25 en 33 ontvangen meldingen door naar de centrale contactpunten van de andere betrokken lidstaten van de Europese Unie.

4. Als uit gegevens die het centrale contactpunt heeft ontvangen van een centraal contactpunt van een andere lidstaat van de Europese Unie blijkt dat een daar gemeld incident, bijna-incident of cyberdreiging gevolgen heeft voor de verlening van de diensten van een essentiële entiteit of belangrijke entiteit in Nederland, stelt het centrale contactpunt het betrokken CSIRT en de betrokken bevoegde autoriteit daarvan op de hoogte.

5. Het centrale contactpunt dient elke drie maanden bij Enisa een samenvattend verslag in met geanonimiseerde en geaggregeerde gegevens over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen.

Artikel 40 (informatieverstrekking over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen door essentiële entiteiten die tevens kritieke entiteiten zijn)

1. De bevoegde autoriteit verstrekt de bevoegde autoriteit, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten, informatie over een significant incident dat overeenkomstig artikel 25 is gemeld door een essentiële entiteit die tevens een kritieke entiteit is als bedoeld in de Wet weerbaarheid kritieke entiteiten.

2. Het CSIRT verstrekt de bevoegde autoriteit, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten, informatie over een incident, bijna-incident of cyberdreiging dat overeenkomstig artikel 33, eerste lid, onderdeel a, is gemeld door een essentiële entiteit die tevens een kritieke entiteit is als bedoeld in de Wet weerbaarheid kritieke entiteiten.

Artikel 41 (informatieverstrekking in verband met incidenten met betrekking tot financiële entiteiten)

Indien het centrale contactpunt informatie van de bevoegde autoriteiten uit hoofde van de Verordening (EU) 2022/2554 ontvangt over incidenten met betrekking tot financiële entiteiten, kan hij deze informatie doorsturen naar een CSIRT of een bevoegde autoriteit.

HOOFDSTUK 9. AANWIJZING VERTEGENWOORDIGER

Artikel 42 (aanwijzing vertegenwoordiger)

1. Indien een hierna genoemde essentiële entiteit of belangrijke entiteit, als bedoeld in deze wet of in het nationale recht van een lidstaat

van de Europese Unie waarin de NIS2-richtlijn is geïmplementeerd, niet in de Europese Unie is gevestigd, maar wel in Nederland diensten aanbiedt, en deze entiteit geen vertegenwoordiger heeft aangewezen in een lidstaat van de Europese Unie waar die diensten worden aangeboden, wijst deze entiteit een vertegenwoordiger aan die is gevestigd in een lidstaat van de Europese Unie waar deze entiteit die diensten aanbiedt:

a. DNS-dienstverleners;
b. registers voor topleveldomeinnamen;
c. aanbieders van cloudcomputingdiensten;
d. aanbieders van datacentrumdiensten;
e. aanbieders van netwerken voor de levering van inhoud;
f. aanbieders van beheerde diensten;
g. aanbieders van beheerde beveiligingsdiensten;
h. aanbieders van onlinemarktplaatsen;
i. aanbieders van onlinezoekmachines;
j. aanbieders van platforms voor socialenetwerkdiensten.

2. Indien een entiteit die domeinnaamregistratiediensten verleent niet in de Europese Unie is gevestigd, maar wel in Nederland diensten aanbiedt, en deze entiteit geen vertegenwoordiger heeft aangewezen in een lidstaat van de Europese Unie waar die diensten worden aangeboden, wijst deze entiteit een vertegenwoordiger aan die is gevestigd in een lidstaat van de Europese Unie, waar deze genoemde entiteit die diensten aanbiedt.

HOOFDSTUK 10. NATIONAAL REGISTER VAN ESSENTIËLE ENTITEITEN, BELANGRIJKE ENTITEITEN EN ENTITEITEN DIE DOMEINNAAMREGISTRATIEDIENSTEN VERLENEN

Artikel 43 (nationaal register van entiteiten)

1. In het belang van de goede uitvoering van deze wet beheert Onze Minister een nationaal register van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen.

2. Onze Minister evalueert het nationale register en past het indien nodig aan, ten minste elke twee jaren, of vaker indien daartoe aanleiding bestaat.

3. Onze Minister wijzigt, weigert of beëindigt in overeenstemming met de bevoegde autoriteit die het aangaat een in het eerste lid bedoelde registratie, indien de grond voor registratie is gewijzigd, vervallen of ontbreekt.

Artikel 44 (informatieverstrekking ten behoeve van nationale register)

1. Een essentiële entiteit, belangrijke entiteit en een entiteit die domeinnaamregistratiediensten verleent verstrekt ten behoeve van de registratie in het nationale register, bedoeld in artikel 43, aan Onze Minister de volgende informatie middels het daarvoor opgezette mechanisme:

a. de naam van de entiteit;
b. het adres en de actuele contactgegevens van de entiteit, met inbegrip van e-mailadressen, IP-bereiken en telefoonnummers;
c. indien van toepassing, de sectoren en subsectoren, bedoeld in bijlage 1 of 2 van deze wet, waartoe de entiteit behoort;
d. indien van toepassing, een vermelding van de lidstaten van de Europese Unie waar de entiteit haar diensten als bedoeld in bijlage 1 of bijlage 2 van deze wet verleent;
e. indien van toepassing, de deelname aan en terugtrekking uit een informatie-uitwisselingsregeling als bedoeld in artikel 62, tweede lid; en
f. indien van toepassing, de andere bij of krachtens algemene maatregel van bestuur genoemde gegevens.
2. De entiteiten, bedoeld in het eerste lid, melden Onze Minister onverwijld of in elk geval binnen twee weken na de datum van de wijziging, elke wijziging van de informatie die zij op grond van het eerste lid hebben verstrekt.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de informatieverstrekking, bedoeld in het eerste lid, waaronder regels over de wijze waarop de informatie wordt verstrekt.

Artikel 45 (ontheffing verplichting informatieverstrekking nationale register)

1. Onze Minister die het aangaat kan bij regeling of besluit, in overeenstemming met Onze Minister, een essentiële entiteit, een belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent ontheffen van de verplichtingen, bedoeld in artikel 44, indien de desbetreffende entiteit uitsluitend activiteiten verricht op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving of uitsluitend diensten verleent aan een overheidsinstantie als bedoeld in artikel 5, eerste lid.
2. Het eerste lid is niet van toepassing wanneer en voor zover een entiteit optreedt als verlener van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers.

Artikel 46 (toegang tot nationale register)

Onze Minister verleent de bevoegde autoriteit en het CSIRT toegang tot het nationale register, bedoeld in artikel 43, ten behoeve van de uitoefening van hun taken, voor zover de toegang ziet op informatie over de entiteiten waarvoor zij zijn aangewezen als de bevoegde autoriteit respectievelijk het CSIRT.

HOOFDSTUK 11. REGISTER VAN ENISA

Artikel 47 (informatieverstrekking ten behoeve van register van Enisa)

1. Ten behoeve van het register van Enisa, bedoeld in artikel 27, eerste lid, van de NIS2-richtlijn, verstrekken de volgende entiteiten aan het centrale contactpunt de informatie, bedoeld in het derde lid van dit artikel, middels het daarvoor opgezette mechanisme, voor zover zij een essentiële entiteit of belangrijke entiteit zijn:

a. DNS-dienstverleners;

b. registers voor topleveldomeinnamen;

c. aanbieders van cloudcomputingdiensten;

d. aanbieders van datacentrumdiensten;

e. aanbieders van netwerken voor de levering van inhoud;

f. aanbieders van beheerde diensten;

g. aanbieders van beheerde beveiligingsdiensten;

h. aanbieders van onlinemarktplaatsen;

i. aanbieders van onlinezoekmachines;

j. aanbieders van platforms voor socialenetwerkdiensten.

2. Ten behoeve van het register van Enisa, bedoeld in artikel 27, eerste lid, van de NIS2-richtlijn, verstrekken entiteiten die domeinnaamregistratiediensten verlenen aan het centrale contactpunt de informatie, bedoeld in het derde lid van dit artikel, middels het daarvoor opgezette mechanisme.

3. De entiteiten, bedoeld in het eerste en tweede lid, verstrekken de volgende informatie aan het centrale contactpunt:

a. de naam van de entiteit;

b. indien van toepassing, de sector, subsector en soort entiteit, bedoeld in bijlage 1 of 2 van deze wet;

c. het adres van de hoofdvestiging van de entiteit en haar andere wettelijke vestigingen in de Europese Unie of, indien deze niet in de Europese Unie zijn gevestigd, van haar op grond van artikel 42 aangewezen vertegenwoordiger;

d. actuele contactgegevens, met inbegrip van e-mailadressen en telefoonnummers van de entiteit en, indien van toepassing, haar op grond van artikel 42 aangewezen vertegenwoordiger;

e. de lidstaten van de Europese Unie waar de entiteit haar diensten als bedoeld in bijlage 1 of 2 van deze wet of haar domeinnaamregistratiediensten verleent; en

f. de IP-bereiken van de entiteit.

4. De entiteiten, bedoeld in het eerste en tweede lid, verstrekken de informatie, bedoeld in het derde lid, uiterlijk op 17 januari 2025. Indien het eerste, tweede en derde lid na 17 januari 2025 in werking treden, verstrekken zij de informatie, bedoeld in het derde lid, binnen één maand na de inwerkingtreding van die leden. Indien een entiteit na de inwerkingtreding van het eerste, tweede en derde lid kwalificeert als een entiteit, bedoeld in het eerste en tweede lid, verstrekt die entiteit de informatie, bedoeld in het derde lid, binnen één maand nadat zij zich als zodanig kwalificeert.

5. De entiteiten, bedoeld in het eerste en tweede lid, stellen het centrale contactpunt onverwijld of in elk geval binnen drie maanden na de datum waarop de wijziging van kracht is geworden, in kennis van wijzigingen van de gegevens, bedoeld in het derde lid.

Artikel 48 (ontheffing verplichting informatieverstrekking register van Enisa)

1. Onze Minister die het aangaat kan bij regeling of besluit, in overeenstemming met Onze Minister, een entiteit als bedoeld in artikel 47, eerste en tweede lid, die uitsluitend activiteiten verricht op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving of die uitsluitend diensten verleent aan een overheidsinstantie als bedoeld in artikel 5, eerste lid, ontheffen van de verplichtingen, bedoeld in artikel 47.

2. Het eerste lid is niet van toepassing wanneer en voor zover een entiteit optreedt als verlener van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers.

HOOFDSTUK 12. DATABASE MET DOMEINNAAMREGISTRATIEGEGEVENS

Artikel 49 (database met domeinnaamregistratiegegevens)

1. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen verzamelen nauwkeurige en volledige domeinnaamregistratiegegevens in een database en houden die gegevens bij.

2. De database, bedoeld in het eerste lid, bevat de volgende gegevens:

a. de domeinnaam;

b. de datum van registratie;

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

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

3. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen stellen het beleid en de procedures vast, waaronder verificatieprocedures, om ervoor te zorgen dat de database, bedoeld in het eerste lid, juiste en volledige informatie bevat. Zij maken dat beleid en die procedures openbaar.

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

5. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen werken samen om te voorkomen dat domeinnaamregistratiegegevens tweemaal worden verzameld.

6. Bij regeling van Onze Minister van Economische Zaken kunnen nadere regels worden gesteld ten aanzien van het bepaalde in dit artikel.

Artikel 50 (verzoeken om toegang tot gegevens over registratie van domeinnamen)

1. Het register voor topleveldomeinnamen respectievelijk de entiteit die domeinnaamregistratiediensten verleent, verleent op een rechtmatig en naar behoren gemotiveerd verzoek van een legitieme partij die daar om verzoekt, toegang tot specifieke gegevens over de registratie van domeinnamen.
2. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen beantwoorden een verzoek om toegang als bedoeld in het eerste lid onverwijld of, indien dat niet mogelijk is, binnen 72 uur na ontvangst van het verzoek.
3. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen stellen het beleid en de procedures met betrekking tot de bekendmaking van de gegevens, bedoeld in het eerste lid, vast en maken dat beleid en die procedures openbaar.
4. Bij regeling van Onze Minister van Economische Zaken kunnen nadere regels worden gesteld ten aanzien van het bepaalde in dit artikel.

HOOFDSTUK 13. SAMENWERKING EN INFORMATIE-UITWISSELING

§ 13.1 Samenwerking en informatie-uitwisseling met betrekking tot instanties

Artikel 51 (samenwerking en informatie-uitwisseling tussen instanties)

1. De bevoegde autoriteiten, de CSIRT’s en het centrale contactpunt werken met elkaar samen voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet en wisselen daartoe onderling alle daarvoor noodzakelijke gegevens uit, waaronder persoonsgegevens.
2. De bevoegde autoriteiten, de CSIRT’s en het centrale contactpunt werken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet samen met de volgende instanties in Nederland en wisselen in het kader van die samenwerking alle daarvoor noodzakelijke gegevens uit, waaronder persoonsgegevens:
a. de politie, het openbaar ministerie en de bijzondere opsporingsdiensten, genoemd in artikel 2 van de Wet op de bijzondere opsporingsdiensten;
b. de Autoriteit persoonsgegevens;
c. de nationale bevoegde autoriteiten, bedoeld in de Verordening (EG) nr. 300/2008 en Verordening (EU) 2018/1139;
d. Onze Minister van Economische Zaken uit hoofde van de Verordening (EU) nr. 910/2014;
e. de bevoegde autoriteiten uit hoofde van de Verordening (EU) 2022/2554;

f. Onze Minister van Economische Zaken uit hoofde van de Richtlijn (EU) 2018/1972;

g. de bevoegde autoriteiten, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten;

h. de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017; en

i. de bij of krachtens algemene maatregel van bestuur aangewezen autoriteiten.

3. Indien Nederland wordt onderworpen aan een collegiale toetsing als bedoeld in artikel 19, eerste lid, van de NIS2-richtlijn, wisselen de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt met de cyberbeveiligingsdeskundigen, bedoeld in artikel 19, eerste lid, van de NIS2-richtlijn, de informatie uit die noodzakelijk is voor de door de cyberbeveiligingsdeskundigen uit te voeren collegiale toetsing.

§ 13.2 Samenwerking en informatie-uitwisseling met betrekking tot CSIRT's

Artikel 52 (samenwerking en informatie-uitwisseling tussen CSIRT's)

De CSIRT's werken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet samen met elkaar en met de CSIRT's van de andere lidstaten van de Europese Unie en wisselen in het kader van die samenwerking alle daarvoor noodzakelijke gegevens uit, waaronder persoonsgegevens.

Artikel 53 (informatie-uitwisseling met entiteiten en gemeenschappen van entiteiten)

De CSIRT's wisselen relevante informatie uit met essentiële entiteiten, belangrijke entiteiten, entiteiten die domeinnaamregistratiediensten verlenen en gemeenschappen van entiteiten als bedoeld in artikel 29 van de NIS2-richtlijn.

Artikel 54 (samenwerking en informatie-uitwisseling met derde landen)

1. Een CSIRT kan een samenwerkingsrelatie tot stand brengen met een gelijkwaardig orgaan van een derde land. Binnen die samenwerkingsrelatie kan relevante informatie worden uitgewisseld, met inbegrip van persoonsgegevens. Een CSIRT gaat alleen over tot de uitwisseling van persoonsgegevens voor zover dat noodzakelijk is voor de doeltreffende en doelmatige uitvoering van haar taken uit hoofde van deze wet.

2. Een CSIRT kan samenwerken met een gelijkwaardig orgaan van een derde land. Deze samenwerking kan bestaan uit het verlenen van bijstand op het gebied van cyberbeveiliging.

§ 13.3 Samenwerking en informatie-uitwisseling met betrekking tot de bevoegde autoriteit

Artikel 55 (samenwerking en informatie-uitwisseling tussen bevoegde autoriteiten van deze wet)

De bevoegde autoriteiten werken met elkaar samen voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet en wisselen daartoe onderling alle daarvoor noodzakelijke gegevens uit, waaronder persoonsgegevens.

Artikel 56 (samenwerking en informatie-uitwisseling met bevoegde autoriteiten Wet weerbaarheid kritieke entiteiten)

1. De bevoegde autoriteiten, bedoeld in artikel 15, en de bevoegde autoriteiten, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten, werken met elkaar samen voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet en de Wet weerbaarheid kritieke entiteiten. In het kader van die samenwerking wisselen zij alle daarvoor noodzakelijke gegevens uit, met inbegrip van persoonsgegevens, waaronder gegevens over:

a. het aanmerken van entiteiten als kritieke entiteiten als bedoeld in de Wet weerbaarheid kritieke entiteiten;

b. cyberbeveiligingsrisico’s, cyberdreigingen, cyberincidenten en niet-cybergerelateerde risico’s, dreigingen en incidenten die gevolgen hebben voor essentiële entiteiten die op grond van de Wet weerbaarheid kritieke entiteiten zijn aangemerkt als kritieke entiteiten; en

c. de maatregelen die zij in reactie op dergelijke risico’s, dreigingen en incidenten hebben genomen.

2. De betrokken bevoegde autoriteit, bedoeld in artikel 15, stelt de betrokken bevoegde autoriteit, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten, op de hoogte van haar beoordeling van de naleving van het bepaalde bij of krachtens deze wet door een essentiële entiteit die tevens kritieke entiteit is als bedoeld in de Wet weerbaarheid kritieke entiteiten en van de uitoefening van toezichts- en handhavingsbevoegdheden om ervoor te zorgen dat die entiteit voldoet aan het bepaalde bij of krachtens deze wet.

3. Het tweede lid is van overeenkomstige toepassing op de beoordeling van de naleving van en de uitoefening van toezichts- en handhavingsbevoegdheden met betrekking tot het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

4. De betrokken bevoegde autoriteit, bedoeld in artikel 15, kan de betrokken bevoegde autoriteit, bedoeld in artikel 8 van de Wet weerbaarheid kritieke entiteiten, verzoeken om toezichts- en handhavingsbevoegdheden uit te oefenen of uit te laten oefenen voor de

naleving van het bepaalde bij of krachtens de Wet weerbaarheid kritieke entiteiten door een essentiële entiteit die tevens kritieke entiteit als bedoeld in de Wet weerbaarheid kritieke entiteiten is.

5. Het vierde lid is van overeenkomstige toepassing op het toezicht op de naleving van en de handhaving van het bepaalde in de op grond van artikel 13, zesde lid, van de CER-richtlijn vastgestelde uitvoeringshandelingen, voor zover in die uitvoeringshandelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 57 (samenwerking met bevoegde autoriteit Verordening (EU) 2022/2554)

1. De bevoegde autoriteiten, bedoeld in artikel 15, werken samen met de bevoegde autoriteiten, bedoeld in artikel 46 van de Verordening (EU) 2022/2554 en wisselen in het kader van die samenwerking alle daarvoor noodzakelijke gegevens uit, waaronder persoonsgegevens.

2. De bevoegde autoriteit stelt het oversightforum dat is opgericht op grond van artikel 32, eerste lid, van de Verordening (EU) 2022/2554 in kennis wanneer zij haar toezichts- en handhavingsbevoegdheden uitoefent om ervoor te zorgen dat een essentiële entiteit of belangrijke entiteit, die op grond van artikel 31 van de Verordening (EU) 2022/2554 als kritieke derde aanbieder van ICT-diensten is aangewezen, voldoet aan het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 58 (samenwerking met toezichthoudende autoriteiten in het kader van inbreuken in verband met persoonsgegevens)

1. De bevoegde autoriteiten werken samen met de Autoriteit persoonsgegevens bij de behandeling van incidenten die leiden tot inbreuken in verband met persoonsgegevens en wisselen in het kader van die samenwerking alle daarvoor noodzakelijke gegevens uit, waaronder persoonsgegevens.

2. Wanneer de bevoegde autoriteit bij toezicht of handhaving er kennis van krijgt dat een overtreding van de artikelen 21, 25, 26, 27, 28, 29 of 30 door een essentiële entiteit of belangrijke entiteit een inbreuk in verband met persoonsgegevens als bedoeld in artikel 4, onderdeel 12, van de Algemene verordening gegevensbescherming kan inhouden, die op grond van artikel 33 van die verordening moet worden gemeld, stelt zij de Autoriteit persoonsgegevens dan wel de bevoegde toezichthoudende autoriteiten, bedoeld in de artikelen 55 en 56 van de Algemene verordening gegevensbescherming daarvan onverwijld in kennis.

3. Indien de Autoriteit persoonsgegevens dan wel de bevoegde toezichthoudende autoriteiten, bedoeld in de artikelen 55 en 56 van de

Algemene verordening gegevensbescherming een bestuurlijke boete opleggen op grond van artikel 58, tweede lid, onderdeel i, van de Algemene verordening gegevensbescherming, legt de bevoegde autoriteit geen bestuurlijke boete op op grond van de artikelen 80 en 87 voor een inbreuk als bedoeld in het tweede lid die voortvloeit uit dezelfde gedraging als die waarvoor de bestuurlijke boete op grond van artikel 58, tweede lid, onderdeel i, van de Algemene verordening gegevensbescherming is opgelegd.

4. Wanneer de op grond van de Algemene verordening gegevensbescherming bevoegde toezichthoudende autoriteit in een andere lidstaat van de Europese Unie is gevestigd, stelt de bevoegde autoriteit de Autoriteit persoonsgegevens in kennis van de potentiële inbreuk in verband met persoonsgegevens, bedoeld in het tweede lid.

5. Het tweede, derde en vierde lid zijn van overeenkomstige toepassing op een overtreding van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 59 (informatie-uitwisseling met andere bevoegde autoriteiten)

De bevoegde autoriteiten, Onze Minister van Economische Zaken uit hoofde van de Verordening (EU) 910/2014, de bevoegde autoriteiten, bedoeld in de Verordening (EU) 2022/2554, en Onze Minister van Economische Zaken uit hoofde van de Richtlijn (EU) 2018/1972 wisselen informatie uit over relevante incidenten en cyberdreigingen.

Artikel 60 (samenwerking met en bijstandsverzoek van de bevoegde autoriteit van een andere lidstaat van de Europese Unie)

1. De bevoegde autoriteit werkt samen met de betrokken bevoegde autoriteit van een andere lidstaat van de Europese Unie en verleent op gemotiveerd verzoek van die autoriteit bijstand, wanneer een essentiële entiteit of belangrijke entiteit of een entiteit die domeinnaamregistratiediensten verleent, als bedoeld in deze wet of in het nationale recht van de betrokken lidstaat van de Europese Unie waarin de NIS2-richtlijn is geïmplementeerd:

a. diensten verricht in meer dan één lidstaat; of

b. diensten verricht in één of meer lidstaten en zijn netwerk- en informatiesystemen zich in één of meer andere lidstaten bevinden.

2. Onverminderd het eerste lid kan de bevoegde autoriteit naar aanleiding van een gemotiveerd verzoek om bijstand van een bevoegde autoriteit van een andere lidstaat van de Europese Unie die ten aanzien van de betrokken entiteit krachtens artikel 26, eerste lid, onderdeel b, van de NIS2-richtlijn jurisdictie heeft, binnen de grenzen van dat verzoek, toezichts- en handhavingsmaatregelen nemen ten aanzien van entiteiten

die domeinnaamregistratiediensten verlenen en de volgende essentiële entiteiten en belangrijke entiteiten, bedoeld in het nationale recht van de betrokken lidstaat van de Europese Unie waarin de NIS2-richtlijn is geïmplementeerd, wanneer die entiteit in Nederland diensten verleent of waarvan een netwerk- en informatiesysteem zich in Nederland bevindt:

a. DNS-dienstverleners;

b. registers voor topleveldomeinnamen;

c. aanbieders van cloudcomputingdiensten;

d. aanbieders van datacentrumdiensten

e. aanbieders van netwerken voor de levering van inhoud;

f. aanbieders van beheerde diensten;

g. aanbieders van beheerde beveiligingsdiensten;

h. de aanbieders van onlinemarktplaatsen;

i. aanbieders van onlinezoekmachines;

j. aanbieders van platforms voor socialenetwerkdiensten.

3. Na de ontvangst van het gemotiveerde verzoek om bijstand, genoemd in het eerste en tweede lid, verleent de bevoegde autoriteit bijstand in verhouding tot haar eigen middelen. De bevoegde autoriteit wijst het verzoek alleen af als:

a. zij niet bevoegd is om de verzochte bijstand te verlenen;

b. de verzochte bijstand niet in verhouding staat tot de toezichthoudende taken van de bevoegde autoriteit; of

c. 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 de nationale veiligheid, de openbare veiligheid of de defensie.

4. Voordat de bevoegde autoriteit het verzoek afwijst, raadpleegt zij de betrokken bevoegde autoriteit van de andere lidstaat van de Europese Unie over de voorgenomen afwijzing en, wanneer de lidstaat daartoe verzoekt, de Europese Commissie en Enisa.

5. In het kader van de samenwerking informeert de bevoegde autoriteit het centrale contactpunt over de door haar genomen toezichts- en handhavingsmaatregelen met betrekking tot een entiteit als bedoeld in het eerste lid, waarna het centrale contactpunt de betrokken bevoegde autoriteit van een andere lidstaat van de Europese Unie informeert over die genomen toezichts- en handhavingsmaatregelen.

6. Het verzoek om bijstand, bedoeld in het eerste, tweede en derde lid, kan zien op het verstrekken van informatie en het nemen van toezichts- en handhavingsmaatregelen, met inbegrip van inspecties ter plaatse, toezicht elders en beveiligingsaudits.

Artikel 61 (bijstandsverzoek aan de bevoegde autoriteit van een andere lidstaat van de Europese Unie)

1. De bevoegde autoriteit kan een bevoegde autoriteit van een andere lidstaat van de Europese Unie gemotiveerd verzoeken om bijstand, wanneer een essentiële entiteit of belangrijke entiteit of een entiteit die domeinnaamregistratiediensten verleent, als bedoeld in deze wet of in het nationale recht van de andere betrokken lidstaat van de Europese Unie waarin de NIS2-richtlijn is geïmplementeerd:

a. diensten verricht in meer dan één lidstaat; of
b. diensten verricht in één of meer lidstaten en haar netwerk- en informatiesystemen zich in één of meer andere lidstaten bevinden.
2. Onverminderd het eerste lid kan de bevoegde autoriteit een bevoegde autoriteit van een andere lidstaat van de Europese Unie gemotiveerd verzoeken om bijstand ten aanzien van de volgende entiteiten, wanneer die entiteit haar hoofdvestiging heeft in die andere lidstaat:
a. DNS-dienstverleners;
b. registers voor topleveldomeinnamen;
c. aanbieders van cloudcomputingdiensten;
d. entiteiten die domeinnaamregistratiediensten verlenen;
e. aanbieders van datacentrumdiensten;
f. aanbieders van netwerken voor de levering van inhoud;
g. aanbieders van beheerde diensten;
h. aanbieders van beheerde beveiligingsdiensten;
i. de aanbieders van onlinemarktplaatsen;
j. aanbieders van onlinezoekmachines;
k. aanbieders van platforms voor socialenetwerkdiensten.
3. Het verzoek om bijstand, bedoeld in het eerste en tweede lid, kan zien op het verstrekken van informatie en het nemen van toezichts- en handhavingsmaatregelen, met inbegrip van inspecties ter plaatse, toezicht elders en beveiligingsaudits.

§ 13.4 Informatie-uitwisseling tussen entiteiten

Artikel 62 (informatie-uitwisseling tussen entiteiten)

1. Essentiële entiteiten, belangrijke entiteiten, entiteiten die domeinnaamregistratiediensten verlenen en andere entiteiten die niet de hiervoor genoemde entiteiten betreffen, kunnen op vrijwillige basis relevante informatie over cyberbeveiliging uitwisselen om incidenten te voorkomen, te detecteren, erop te reageren of ervan te herstellen of de gevolgen ervan te beperken en om het cyberbeveiligingsniveau te verhogen.
2. De informatie-uitwisseling, bedoeld in het eerste lid, kan plaatsvinden binnen gemeenschappen van entiteiten en, indien van toepassing, hun leveranciers en dienstverleners op basis van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld ter uitvoering van het bepaalde in artikel 29, derde lid, van de NIS2-richtlijn.

HOOFDSTUK 14. VERWERKING VAN GEGEVENS

Artikel 63 (verwerkingsverantwoordelijkheid)

De bevoegde autoriteit, het centrale contactpunt, het CSIRT en Onze Minister zijn de verwerkingsverantwoordelijken voor de verwerking van persoonsgegevens ten behoeve van de taken die op grond van deze wet aan hen zijn toegewezen.

Artikel 64 (bijzondere categorieën van persoonsgegevens)

1. De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid door de bevoegde autoriteit geschiedt alleen voor zover de verwerking van deze gegevens noodzakelijk is voor de uitoefening van haar taken op grond van deze wet.
2. De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid door het CSIRT geschiedt alleen voor zover de verwerking van deze gegevens noodzakelijk is voor de uitoefening van haar taken op grond van artikel 16, tweede lid, onderdelen a tot en met e.

Artikel 65 (bewaring van gegevens)

1. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de periode gedurende welke de persoonsgegevens die bij of krachtens deze wet zijn verwerkt, worden bewaard.
2. De persoonsgegevens, bedoeld in artikel 64, eerste lid, die door de bevoegde autoriteit worden verwerkt worden niet langer bewaard dan noodzakelijk is ter uitvoering van haar taken op grond van deze wet, doch uiterlijk binnen 60 maanden na de eerste verwerking verwijderd.
3. De persoonsgegevens, bedoeld in artikel 64, tweede lid, die door het CSIRT worden verwerkt worden niet langer bewaard dan noodzakelijk is ter uitvoering van haar taken op grond van deze wet, doch uiterlijk binnen 12 maanden na de eerste verwerking verwijderd.

Artikel 66 (vertrouwelijke gegevens)

1. De bevoegde autoriteit, het centrale contactpunt, het CSIRT en Onze Minister kunnen in het kader van de uitoefening van hun taken op grond van deze wet vertrouwelijke gegevens verstrekken, doch uitsluitend voor zover:
a. dat noodzakelijk is ter uitvoering van hun taken uit hoofde van deze wet;
b. de verstrekking beperkt blijft tot die vertrouwelijke gegevens die relevant zijn voor de ontvangende partij en verstrekking evenredig is aan het doel van die verstrekking;
c. de vertrouwelijkheid van die vertrouwelijke gegevens is gewaarborgd; en

d. de veiligheids- en commerciële belangen van de betrokken entiteit worden beschermd.

2. De Wet open overheid is niet van toepassing op vertrouwelijke gegevens als bedoeld in het eerste lid, behalve voor zover die gegevens milieu-informatie inhouden als bedoeld in artikel 19.1a van de Wet milieubeheer. De eerste volzin geldt ook als de gegevens bij een ander overheidsorgaan berusten na verstrekking op grond van dit artikel.

Artikel 67 (verstrekking van gegevens in relatie tot nationale veiligheid, openbare veiligheid en defensie)

Het bepaalde bij of krachtens deze wet omvat niet de verstrekking van informatie waarvan de bekendmaking strijdig is met de wezenlijke belangen van nationale veiligheid, openbare veiligheid of defensie.

HOOFDSTUK 15. HANDHAVING

§ 15.1 Algemeen

Artikel 68 (toezichthouders)

1. Met het toezicht op de naleving van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, zijn belast: de bij besluit van de bevoegde autoriteit aangewezen ambtenaren.

2. De ambtenaren, bedoeld in het eerste lid, zijn tevens belast met het verlenen van bijstand als bedoeld in artikel 60 aan een bevoegde autoriteit van een andere lidstaat van de Europese Unie.

3. Ten behoeve van het verlenen van de bijstand, bedoeld in het tweede lid, kunnen de toezichthouders hun toezichthoudende bevoegdheden toepassen.

4. Van een besluit als bedoeld in het eerste lid wordt mededeling gedaan door plaatsing in de Staatscourant.

Artikel 69 (toepassing handhavingsinstrumentarium)

Onverminderd artikel 3:4, tweede lid, van de Algemene wet bestuursrecht houdt de bevoegde autoriteit bij de toepassing van de artikelen 70, 72, eerste lid, onderdeel c, 73 tot en met 78, 80, 83, eerste lid, onderdeel c, 84 tot en met 87 en 89 tot en met 93 rekening met de omstandigheden van elk afzonderlijk geval, alsmede:

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

1°. herhaalde overtredingen;
2°. het niet melden of niet verhelpen van significante incidenten;
3°. het niet verhelpen van tekortkomingen naar aanleiding van bindende aanwijzingen van de bevoegde autoriteit;
4°. het belemmeren van audits of monitoringsactiviteiten waartoe de bevoegde autoriteit opdracht heeft gegeven naar aanleiding van de vaststelling van een overtreding;
5°. het verstrekken van valse of zeer onnauwkeurige informatie met betrekking tot de verplichtingen, bedoeld in de artikelen 21 en 25 tot en met 30;
b. de duur van de overtreding;
c. eventuele relevante eerdere overtredingen door de betrokken entiteit;
d. elke veroorzaakte materiële of immateriële schade, met inbegrip van elke financiële of economische schade, effecten op andere diensten en het aantal getroffen gebruikers;
e. opzet of nalatigheid van de overtreder;
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; en
h. de mate waarin de overtreder meewerkt met de bevoegde autoriteiten.

§ 15.2 Handhaving ten aanzien van essentiële entiteiten

Artikel 70 (controlefunctionaris)

1. De bevoegde autoriteit kan voor een bepaalde periode een controlefunctionaris aanwijzen bij een essentiële entiteit.
2. De controlefunctionaris is een onafhankelijke deskundige zijnde een natuurlijk persoon en heeft tot taak:
a. het monitoren van de naleving van het bepaalde bij of krachtens de artikelen 21 en 25 tot en met 30 en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, door de betrokken essentiële entiteit; en
b. het informeren van de bevoegde autoriteit en het bestuur van de betrokken essentiële entiteit over de naleving van het bepaalde bij of krachtens de artikelen 21 en 25 tot en met 30 en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, door de betrokken essentiële entiteit.
3. De essentiële entiteit draagt de kosten van de controlefunctionaris.

4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het bepaalde in het eerste en tweede lid, waaronder de vereisten die gelden voor de aanwijzing van de controlefunctionaris.

Artikel 71 (beveiligingsscan)

1. De bevoegde autoriteit kan een beveiligingsscan op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria uitvoeren of door een onafhankelijke en gekwalificeerde deskundige laten uitvoeren bij een essentiële entiteit.
2. De bevoegde autoriteit draagt de kosten van de beveiligingsscan.

Artikel 72 (audit)

1. De bevoegde autoriteit kan een essentiële entiteit verplichten om:
a. een onafhankelijke en gekwalificeerde deskundige te laten onderzoeken of de entiteit voldoet aan het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie;
b. de resultaten van dat onderzoek binnen een bij het besluit gestelde redelijke termijn te verstrekken aan de bevoegde autoriteit; of
c. de aanbevelingen naar aanleiding van het onderzoek binnen een redelijke termijn uit te voeren.
2. Het onderzoek is gebaseerd op de door de bevoegde autoriteit of de betrokken essentiële entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.
3. Het onderzoek wordt uitgevoerd op een door de bevoegde autoriteit voorgeschreven wijze.
4. De essentiële entiteit draagt de kosten van het onderzoek, tenzij de kosten naar het oordeel van de bevoegde autoriteit redelijkerwijs moeten worden gedragen door de bevoegde autoriteit.
5. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste tot en met derde lid.

Artikel 73 (openbaarmaking overtreding)

De bevoegde autoriteit kan een essentiële entiteit verplichten om onderdelen van een door de entiteit begane overtreding van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de

Europese Unie, openbaar te maken, op een door de bevoegde autoriteit bepaalde wijze.

Artikel 74 (aanwijzing)

De bevoegde autoriteit kan een essentiële entiteit een bindende aanwijzing geven om binnen een daarbij gestelde redelijke termijn de daarin omschreven handelingen te verrichten of de daarin omschreven maatregelen te nemen ter naleving van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 75 (last onder bestuursdwang)

De bevoegde autoriteit is bevoegd tot oplegging van een last onder bestuursdwang aan een essentiële entiteit ter handhaving van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 76 (einddatum beëindiging overtreding)

1. De bevoegde autoriteit kan na een overtreding door een essentiële entiteit van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, een einddatum bepalen waarop de entiteit de daarbij genoemde maatregelen moet hebben genomen om de overtreding te beëindigen of waarop de entiteit aan de daarbij nader omschreven eisen moet hebben voldaan ter beëindiging van de overtreding.

2. De bevoegde autoriteit kan het besluit, bedoeld in het eerste lid, alleen nemen:

a. nadat zij alle in het derde lid genoemde maatregelen heeft opgelegd aan de betrokken entiteit en deze maatregelen niet ertoe hebben geleid dat de overtreding is beëindigd; of

b. nadat zij één of meer van de in het derde lid genoemde maatregelen heeft opgelegd aan de betrokken entiteit, de opgelegde maatregel of maatregelen niet ertoe hebben geleid dat de overtreding is beëindigd en

het opleggen van de andere in het derde lid genoemde maatregel of maatregelen naar het oordeel van de bevoegde autoriteit niet ertoe zullen leiden dat de betrokken entiteit de overtreding beëindigt.

3. De maatregelen, bedoeld in het tweede lid, zijn:

a. een waarschuwing van de bevoegde autoriteit aan de betrokken entiteit over een overtreding van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie;

b. een verplichting van de bevoegde autoriteit aan de betrokken entiteit over de uitvoering van de aanbevelingen naar aanleiding van het onderzoek als bedoeld in artikel 72, eerste lid, onderdeel c;

c. een aanwijzing als bedoeld in artikel 74;

d. een last onder bestuursdwang als bedoeld in artikel 75;

e. een last onder bestuursdwang als bedoeld in artikel 75 in samenhang met artikel 5:32, eerste lid, van de Algemene wet bestuursrecht.

Artikel 77 (verzoek tot schorsing certificering of vergunning)

Indien de essentiële entiteit niet uiterlijk op de daarbij bepaalde einddatum heeft voldaan aan het besluit, bedoeld in artikel 76, kan de bevoegde autoriteit de instantie of organisatie die een certificering of vergunning heeft afgegeven verzoeken die certificering of vergunning tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de essentiële entiteit verleende diensten of verrichte activiteiten, zolang de entiteit niet voldoet aan het besluit.

Artikel 78 (verzoek tot schorsing leden van het bestuur)

1. Indien de essentiële entiteit niet uiterlijk op de daarbij bepaalde einddatum heeft voldaan aan het besluit, bedoeld in artikel 76, kan de bevoegde autoriteit de burgerlijke rechter van de rechtbank van het arrondissement waarbinnen de vestigingsplaats van de bevoegde autoriteit is gelegen verzoeken om één of meer leden van het bestuur van de betrokken essentiële entiteit te schorsen, zolang de entiteit niet voldoet aan het besluit.

2. De rechtbank regelt zo nodig alle overige gevolgen van de door haar uitgesproken schorsing.

3. De griffier van de rechtbank, of in geval van hoger beroep, van het gerechtshof, biedt een afschrift van de onherroepelijke uitspraak waarin een schorsing is opgelegd met bekwame spoed aan de Kamer van Koophandel aan, die terstond de schorsing in het Handelsregister opneemt.

4. Zodra is voldaan aan het besluit, bedoeld in artikel 76, verzoekt de bevoegde autoriteit de Kamer van Koophandel de opname van de schorsing uit het Handelsregister te verwijderen.

Artikel 79 (uitzondering voor overheidsinstanties)

De artikelen 76, 77 en 78 zijn niet van toepassing op overheidsinstanties.

Artikel 80 (bestuurlijke boete)

1. De bevoegde autoriteit kan in geval van overtreding van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, aan een essentiële entiteit een bestuurlijke boete opleggen:

a. tezamen met of na het geven van een waarschuwing aan de betrokken entiteit over de overtreding; of

b. tezamen met of na de toepassing van de artikelen 38, 70, 72, eerste lid, onderdeel c, 73, 74, 75, 76, 77 of 78.

2. De bevoegde autoriteit kan tevens aan een essentiële entiteit een bestuurlijke boete opleggen in geval van overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht.

3. De boete bedraagt ten hoogste:

a. in geval van overtreding van het bepaalde bij of krachtens de artikelen 21, 21a en 25 tot en met 30 en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie: € 10.000.000,- of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de essentiële entiteit behoort, indien het laatstbedoelde bedrag hoger is;

b. in geval van een andere overtreding: € 1.000.000,-.

4. De werking van het besluit tot oplegging van de boete wordt opgeschort totdat het besluit onherroepelijk is.

5. Verzet schorst de tenuitvoerlegging van een dwangbevel dat strekt tot invordering van de boete.

6. Artikel 184 van het Wetboek van Strafrecht is niet van toepassing op de overtreding, bedoeld in het tweede lid.

§ 15.3 Handhaving ten aanzien van belangrijke entiteiten

Artikel 81 (reikwijdte)

De artikelen 82 tot en met 87 zijn alleen van toepassing voor zover de bevoegde autoriteit het bewijs, de aanwijzing of informatie heeft van een mogelijke overtreding door een belangrijke entiteit van het bepaalde bij of

krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 82 (beveiligingsscan)

1. De bevoegde autoriteit kan een beveiligingsscan op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria uitvoeren of door een onafhankelijke deskundige laten uitvoeren bij een belangrijke entiteit.
2. De bevoegde autoriteit draagt de kosten van de beveiligingsscan.

Artikel 83 (audit)

1. De bevoegde autoriteit kan een belangrijke entiteit verplichten om:
a. een onafhankelijke en gekwalificeerde deskundige te laten onderzoeken of de entiteit voldoet aan het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie;
b. de resultaten van dat onderzoek binnen een bij het besluit gestelde redelijke termijn te verstrekken aan de bevoegde autoriteit; of
c. de aanbevelingen naar aanleiding van het onderzoek binnen een redelijke termijn uit te voeren.
2. Het onderzoek is gebaseerd op de door de bevoegde autoriteit of de betrokken belangrijke entiteit verrichte risicobeoordelingen of op andere beschikbare risicogerelateerde informatie.
3. Het onderzoek wordt uitgevoerd op een door de bevoegde autoriteit voorgeschreven wijze.
4. De belangrijke entiteit draagt de kosten van het onderzoek, tenzij de kosten naar het oordeel van de bevoegde autoriteit redelijkerwijs moeten worden gedragen door de bevoegde autoriteit.
5. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste tot en met derde lid.

Artikel 84 (openbaarmaking overtreding)

De bevoegde autoriteit kan een belangrijke entiteit verplichten om onderdelen van een door de entiteit begane overtreding van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die

uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, openbaar te maken, op een door de bevoegde autoriteit bepaalde wijze.

Artikel 85 (aanwijzing)

De bevoegde autoriteit kan een belangrijke entiteit een bindende aanwijzing geven om binnen een daarbij gestelde redelijke termijn de daarin omschreven handelingen te verrichten of de daarin omschreven maatregelen te nemen ter naleving van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 86 (last onder bestuursdwang)

De bevoegde autoriteit is bevoegd tot oplegging van een last onder bestuursdwang aan een belangrijke entiteit ter handhaving van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

Artikel 87 (bestuurlijke boete)

1. De bevoegde autoriteit kan in geval van overtreding van het bepaalde bij of krachtens deze wet en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie, aan een belangrijke entiteit een bestuurlijke boete opleggen:

a. tezamen met of na het geven van een waarschuwing aan de betrokken entiteit over de overtreding; of

b. tezamen met of na de toepassing van de artikelen 38, 83, eerste lid, onderdeel c, 84, 85 of 86.

2. De bevoegde autoriteit kan tevens aan een belangrijke entiteit een bestuurlijke boete opleggen in geval van overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht.

3. De boete bedraagt ten hoogste:

a. in geval van overtreding van het bepaalde bij of krachtens de artikelen 21, 21a en 25 tot en met 30 en het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, van de NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, van de NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie: € 7.000.000,- of 1,4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar van de onderneming waartoe de belangrijke entiteit behoort, indien het laatstbedoelde bedrag hoger is;

b. in geval van een andere overtreding: € 1.000.000,-.

4. De werking van het besluit tot oplegging van de boete wordt opgeschort totdat het besluit onherroepelijk is.

5. Verzet schorst de tenuitvoerlegging van een dwangbevel dat strekt tot invordering van de boete.

6. Artikel 184 van het Wetboek van Strafrecht is niet van toepassing op de overtreding, bedoeld in het tweede lid.

§ 15.4 Handhaving ten aanzien van entiteiten die domeinnaamregistratiediensten verlenen

Artikel 88 (reikwijdte)

De artikelen 89 tot en met 91 zijn alleen van toepassing op de entiteit die domeinnaamregistratiediensten verleent, indien zij op grond van deze wet niet tevens essentiële entiteit of belangrijke entiteit is.

Artikel 89 (aanwijzing)

De bevoegde autoriteit kan een entiteit die domeinnaamregistratiediensten verleent, een bindende aanwijzing geven om binnen een daarbij gestelde redelijke termijn de daarin omschreven handelingen te verrichten ter naleving van de artikelen 42, 44, 47, 49 en 50, indien zij niet voldoet aan het bepaalde bij of krachtens de hiervoor genoemde artikelen.

Artikel 90 (last onder dwangsom)

De bevoegde autoriteit kan een entiteit die domeinnaamregistratiediensten verleent een last onder dwangsom opleggen in geval van overtreding van het bepaalde bij of krachtens de artikelen 42, 44, 47, 49 en 50.

Artikel 91 (bestuurlijke boete)

1. De bevoegde autoriteit kan een entiteit die domeinnaamregistratiediensten verleent een bestuurlijke boete opleggen in geval van:

a. overtreding van het bepaalde bij of krachtens de artikelen 42, 44, 47, 49 en 50;

b. overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht.

2. De boete, bedoeld in het eerste lid, bedraagt ten hoogste € 1.000.000,-.

3. De werking van het besluit tot oplegging van de boete wordt opgeschort totdat het besluit onherroepelijk is.

4. Verzet schorst de tenuitvoerlegging van een dwangbevel dat strekt tot invordering van de boete.

5. Artikel 184 van het Wetboek van Strafrecht is niet van toepassing op de overtreding, bedoeld in het eerste lid, onderdeel b.

§ 15.5 Handhaving ten aanzien van de verplichtingen, bedoeld in artikel 24, tweede tot en met zesde lid

Artikel 92 (last onder dwangsom)

De bevoegde autoriteit kan een lid van het bestuur van een essentiële entiteit of belangrijke entiteit een last onder dwangsom opleggen in geval van overtreding van het bepaalde bij of krachtens artikel 24, tweede tot en met zesde lid.

Artikel 93 (bestuurlijke boete)

1. De bevoegde autoriteit kan een lid van het bestuur van een essentiële entiteit of belangrijke entiteit een bestuurlijke boete opleggen in geval van:

a. overtreding van het bepaalde bij of krachtens artikel 24, tweede tot en met zesde lid;

b. overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht.

2. De boete, bedoeld in het eerste lid, bedraagt ten hoogste € 25.000,-.

3. De werking van het besluit tot oplegging van de boete wordt opgeschort totdat het besluit onherroepelijk is.

4. Verzet schorst de tenuitvoerlegging van een dwangbevel dat strekt tot invordering van de boete.

5. Artikel 184 van het Wetboek van Strafrecht is niet van toepassing op de overtreding, bedoeld in het eerste lid, onderdeel b.

HOOFDSTUK 16. SLOTBEPALINGEN

§ 16.1 Evaluatie

Artikel 94 (evaluatiebepaling)

1. Onze Minister zendt binnen achttien maanden na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag waarin de resultaten van een invoeringstoets over de uitvoerbaarheid, de

handhaafbaarheid, de regeldruk, de samenloop en de werkbaarheid van deze wet in de praktijk zijn opgenomen.

2. Onze Minister zendt binnen twee jaar na de inwerkingtreding van deze wet aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk, en vervolgens elke drie jaar.

§ 16.2 Overgangsrecht

Artikel 95 (besluiten en meldingen op grond van de Wet beveiliging netwerk- en informatiesystemen)

1. Indien voor de inwerkingtreding van artikel 106 een besluit is genomen op grond van de Wet beveiliging netwerk- en informatiesystemen, blijft het oude recht van toepassing tot het tijdstip waarop:

a. het besluit onherroepelijk is geworden en volledig is uitgevoerd of ten uitvoer is gelegd;

b. het besluit is ingetrokken of is komen te vervallen; of

c. als het besluit gaat om de oplegging van een last onder dwangsom:

1°. de last volledig is uitgevoerd;

2°. de dwangsom volledig is verbeurd en betaald; of

3°. de last is opgeheven.

2. Indien voor de inwerkingtreding van artikel 106 een melding als bedoeld in artikel 10 of 13 van de Wet beveiliging netwerk- en informatiesystemen is gedaan, en artikel 25 met ingang van de dag van de inwerkingtreding van laatstgenoemd artikel van toepassing is op de melder, wordt de op grond van de Wet beveiliging netwerk- en informatiesystemen gedane melding aangemerkt als een vroegtijdige waarschuwing van een significant incident als bedoeld in artikel 26. Indien de melding ziet op een inbreuk op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kan hebben voor de continuïteit van de door de melder verleende dienst als bedoeld in artikel 10, eerste lid, onderdeel b, van de Wet beveiliging netwerk- en informatiesystemen, zendt Onze Minister de melding door aan de bevoegde autoriteit.

Artikel 96 (bijstand ten behoeve van andere entiteiten)

1. De organisaties, niet zijnde essentiële entiteiten of belangrijke entiteiten, die op de dag voorafgaand aan de inwerkingtreding van artikel 106 vitale aanbieder dan wel andere aanbieder die onderdeel is van de rijksoverheid zijn als bedoeld in artikel 3, eerste lid, van de Wet beveiliging netwerk- en informatiesystemen, zoals die wet luidde op de dag voorafgaand aan de inwerkingtreding van artikel 106, hebben recht op:

a. bijstand bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen door Onze Minister of een andere in afwijking hiervan bij of krachtens algemene maatregel van bestuur hiervoor aan te wijzen instantie; en

b. informatie en advies over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen van Onze Minister of een andere in afwijking hiervan bij of krachtens algemene maatregel van bestuur hiervoor aan te wijzen instantie.

2. Onze Minister onderscheidenlijk de andere instantie, bedoeld in het eerste lid, verricht ten behoeve van het uitvoeren van de in het eerste lid bedoelde taken analyses en technisch onderzoek, naar aanleiding van de in het eerste lid genoemde dreigingen en incidenten of aanwijzingen daarvoor, niet zijnde onderzoek naar personen of organisaties die voor die dreigingen en incidenten verantwoordelijk zijn of die daar anderszins aan bijdragen of hebben bijgedragen.

3. Artikel 16, tweede lid, aanhef en onderdeel e, en derde lid, is van overeenkomstige toepassing, met dien verstande dat onder “CSIRT” wordt verstaan: Onze Minister of de andere instantie, bedoeld in het eerste lid.

4. Onze Minister onderscheidenlijk de andere instantie, bedoeld in het eerste lid, is de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens ten behoeve van de in het eerste tot en met derde lid bedoelde taken.

§ 16.3 Inwerkingtreding zorgplicht ten aanzien van instellingen voor hoger onderwijs

Artikel 97 (inwerkingtreding zorgplicht ten aanzien van instellingen voor hoger onderwijs)

Het bepaalde bij of krachtens de artikelen 21 en 24 is van toepassing op de op grond van artikel 11 aangewezen essentiële entiteit en de op grond van artikel 13 aangewezen belangrijke entiteit vanaf 36 maanden na de aanwijzing.

§ 16.4 Totstandkoming nationaal register

Artikel 98 (totstandkoming nationaal register)

Het nationale register, genoemd in artikel 43, komt uiterlijk één maand na de inwerkingtreding van artikel 43 tot stand.

§ 16.5 Wijzigingen bestaande wetgeving

Artikel 99 (wijziging Telecommunicatiewet)

De Telecommunicatiewet wordt als volgt gewijzigd:

A

Het opschrift “Hoofdstuk 11a. Continuïteit” wordt vervangen door “Hoofdstuk 11a. Beveiligingsmaatregelen”.

B

Artikel 11.a1 wordt als volgt gewijzigd:

1. Het eerste lid komt te luiden:
1. Aanbieders van openbare elektronische communicatiediensten nemen passende en evenredige technische, operationele en organisatorische maatregelen om de risico’s voor de beveiliging van hun diensten te beheersen, waaronder in voorkomend geval versleuteling, teneinde de gevolgen van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden. Deze maatregelen zorgen, gezien de stand van de techniek, voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen.

2. Onder vernummering van het tweede tot en met vijfde lid tot derde tot en met zesde lid wordt na het eerste lid een lid toegevoegd, luidende:
2. Aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten nemen bij of krachtens algemene maatregel van bestuur vastgestelde technische, operationele en organisatorische maatregelen om de risico’s voor de beveiliging van hun netwerken of diensten te beheersen, teneinde de gevolgen van beveiligingsincidenten op de nationale veiligheid of openbare orde te beperken.

3. In het vierde lid (nieuw) wordt “in dit artikel” vervangen door “in het eerste en derde lid”.

C

De artikelen 11a.2 en 11a.2a vervallen.

D

Artikel 11a.3 wordt als volgt gewijzigd:

1. Het eerste lid komt te luiden:
1. Een aanbieder van een bij of krachtens algemene maatregel van bestuur aangewezen antenne-opstelpunt als bedoeld in artikel 5a.3, derde lid, alsmede een aanbieder van een openbaar elektronisch communicatienetwerk dat bestaat uit radioapparaten die geschikt zijn voor het verspreiden van programma’s en dat door een aangewezen antenne-opstelpunt als bedoeld in artikel 5a.3, derde lid, wordt ondersteund, draagt, ieder voor zich, zorg voor de opstelling en de uitvoering van een continuïteitsplan dat een beschrijving bevat van de technische en organisatorische maatregelen die de aanbieder neemt om de risico’s voor de veiligheid in en op het opstelpunt te beheersen voor zover van belang voor de continuïteit van de verspreiding van programma's door middel van openbare elektronische communicatienetwerken die worden ondersteund door dat opstelpunt.

2. Het vierde lid komt te luiden:

4. Voor een aangewezen antenne-opstelpunt dragen de in het eerste lid bedoelde aanbieder of aanbieders zorg voor de opstelling en de uitvoering van een gezamenlijk continuïteitsplan dat voorziet in onderlinge afstemming van de maatregelen, bedoeld in het eerste lid.

E

In artikel 15.1, eerste lid, onderdeel l, vervalt “11a.2,”.

Artikel 100 (wijziging Wet bevordering digitale weerbaarheid bedrijven)

De Wet bevordering digitale weerbaarheid bedrijven wordt als volgt gewijzigd:

A

Artikel 1 komt te luiden:

Artikel 1 Begripsbepalingen

In deze wet en de daarop berustende bepalingen wordt verstaan onder:
bedrijf: in Nederland gevestigde natuurlijke persoon of privaatrechtelijke rechtspersoon die bedrijfsmatige activiteiten uitvoert, niet zijnde essentiële entiteit of belangrijke entiteit;
belangrijke entiteit: belangrijke entiteit als bedoeld in artikel 1 van de Cyberbeveiligingswet;
CSIRT: krachtens artikel 16, eerste lid, van de Cyberbeveiligingswet aangewezen Computer security incident response team;
essentiële entiteit: essentiële entiteit als bedoeld in artikel 1 van de Cyberbeveiligingswet;
incident: incident als bedoeld in artikel 6, onder 6, van de NIS2-richtlijn;
netwerk- en informatiesysteem: netwerk- en informatiesysteem als bedoeld in artikel 6, onder 1, van de NIS2-richtlijn;
NIS2-richtlijn: 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 (*PbEU* 2022, L 333);
Onze Minister: Onze Minister van Economische Zaken.

B

Artikel 2, tweede lid, wordt als volgt gewijzigd:

1. In onderdeel c wordt “de Minister van Justitie en Veiligheid, ten behoeve van de uitvoering van diens taken, bedoeld in artikel 3, eerste lid, van de Wet beveiliging netwerk- en informatiesystemen;” vervangen door

“een CSIRT, ten behoeve van de uitvoering van diens taken als bedoeld in artikel 16, tweede lid, van de Cyberbeveiligingswet.”.

2. Onderdeel d vervalt.

C

Artikel 4 wordt als volgt gewijzigd:

1. In het eerste lid vervalt “en d”.

2. Het tweede lid komt te luiden:
2. Ter uitvoering van de in artikel 2, tweede lid, onder c, genoemde taken kan Onze Minister vertrouwelijke gegevens met betrekking tot een essentiële entiteit of belangrijke entiteit die hij ingevolge deze wet verkrijgt, zonder dier instemming verstrekken aan een CSIRT, ten behoeve van de uitvoering van diens taken als bedoeld in artikel 16, tweede lid, van de Cyberbeveiligingswet.

3. Het derde lid vervalt, onder vernummering van het vierde lid tot derde lid.

4. In het derde lid (nieuw) wordt “het eerste tot en met derde lid” vervangen door “het eerste en tweede lid” en wordt “in het tweede of derde lid bedoelde aanbieder onderscheidenlijk digitaledienstverlener” vervangen door “in het tweede lid bedoelde entiteit”.

Artikel 101 (wijziging Wet open overheid)

De bijlage bij artikel 8.8 van de Wet open overheid wordt als volgt gewijzigd:

1. In de alfabetische volgorde wordt ingevoegd:
Cyberbeveiligingswet: artikel 66

2. De onderdelen met betrekking tot de Telecommunicatiewet en de Wet beveiliging netwerk- en informatiesystemen komen te vervallen.

3. In het onderdeel met betrekking tot de Wet bevordering digitale weerbaarheid bedrijven wordt “artikel 4, vierde lid” vervangen door “artikel 4, derde lid”.

Artikel 102 (wijziging Wet op het financieel toezicht)

In artikel 1:93, eerste lid, van de Wet op het financieel toezicht wordt, onder vervanging van de punt aan het slot van onderdeel k door een puntkomma, een onderdeel toegevoegd, luidende:
l. Onze Minister en het bij of krachtens algemene maatregel van bestuur voor essentiële entiteiten en belangrijke entiteiten in de sectoren bankwezen en infrastructuur voor de financiële markt aangewezen CSIRT,

bedoeld in artikel 16, eerste lid, van de Cyberbeveiligingswet, voor zover de gegevens of inlichtingen dienstig zijn voor de uitoefening van hun taken op grond van de Cyberbeveiligingswet.

Artikel 103 (wijziging Algemene wet bestuursrecht)

Bijlage 2 bij de Algemene wet bestuursrecht wordt als volgt gewijzigd:

1. In artikel 7 vervalt “Wet beveiliging netwerk- en informatiesystemen” en wordt in de alfabetische volgorde ingevoegd:
Cyberbeveiligingswet, voor zover het een besluit betreft dat betrekking heeft op een essentiële entiteit of belangrijke entiteit in de sector energie, bankwezen, infrastructuur voor de financiële markt, digitale infrastructuur, beheer van ICT-diensten (business-to-business), post- en koeriersdiensten of productie, verwerking en distributie van levensmiddelen, of de subsector spoor of vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek

2. In artikel 11 vervalt “Wet beveiliging netwerk- en informatiesystemen” en wordt in de alfabetische volgorde ingevoegd:
Cyberbeveiligingswet, voor zover het een besluit betreft dat betrekking heeft op een essentiële entiteit of belangrijke entiteit in de sector energie, bankwezen, infrastructuur voor de financiële markt, digitale infrastructuur, beheer van ICT-diensten (business-to-business), post- en koeriersdiensten of productie, verwerking en distributie van levensmiddelen, of de subsector spoor

Artikel 103a (wijziging Wet bekostiging financieel toezicht 2019)

In artikel 2, tweede lid, onderdeel d, van de Wet bekostiging financieel toezicht 2019 wordt “Wet beveiliging netwerk- en informatiesystemen” vervangen door “Cyberbeveiligingswet”.

Artikel 103b (wijziging Wet coördinatie terrorismebestrijding en nationale veiligheid)

In artikel 6, onderdeel e, van de Wet coördinatie terrorismebestrijding en nationale veiligheid wordt “Wet beveiliging netwerk- en informatiesystemen” vervangen door “Cyberbeveiligingswet”.

§ 16.6 Wijzigingen van de NIS2-richtlijn

Artikel 104 (wijzigingen van de NIS2-richtlijn)

Een wijziging van een bepaling uit de NIS2-richtlijn waarnaar in deze wet is verwezen geldt voor de toepassing van de bepaling uit deze wet waarin de verwijzing is opgenomen met ingang van de dag waarop aan de betrokken wijziging uitvoering moet zijn gegeven, tenzij bij ministerieel besluit, dat in de Staatscourant wordt bekendgemaakt, een ander tijdstip wordt vastgesteld.

§ 16.7 Inwerkingtreding onderdelen van de Wet bestuur en toezicht rechtspersonen

Artikel 105 (inwerkingtreding onderdelen van de Wet bestuur en toezicht rechtspersonen)

Indien artikel I, onderdelen E, onder 1, FA, L en BBBA van de Wet bestuur en toezicht rechtspersonen in werking treden, wordt artikel 24 van deze wet als volgt gewijzigd:

Het achtste lid komt te luiden:
8. Indien de essentiële entiteit of belangrijke entiteit toepassing heeft gegeven aan de artikelen 44a, 129a, 239a of 291a van Boek 2 van het Burgerlijk Wetboek, is het bepaalde bij of krachtens het eerste tot en met zesde lid uitsluitend van toepassing op de uitvoerende bestuurders van die essentiële entiteit of belangrijke entiteit.

§ 16.8 Overig

Artikel 106 (intrekking Wet beveiliging netwerk- en informatiesystemen)

De Wet beveiliging netwerk- en informatiesystemen wordt ingetrokken.

Artikel 107 (inwerkingtreding)

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel 108 (citeertitel)

Deze wet wordt aangehaald als: Cyberbeveiligingswet.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Justitie en Veiligheid,

Bijlage 1

Sector	Subsector	Soort entiteit
Energie	Elektriciteit	— Elektriciteitsbedrijven als bedoeld in artikel 2, onderdeel 57, van Richtlijn (EU) 2019/944[1], die de functie verrichten van “levering” als bedoeld in artikel 2, onderdeel 12, van die richtlijn
		— Distributiesysteembeheerders als bedoeld in artikel 2, onderdeel 29, van Richtlijn (EU) 2019/944
		— Transmissiesysteembeheerders als bedoeld in artikel 2, onderdeel 35, van Richtlijn (EU) 2019/944
		— Producenten als bedoeld in artikel 2, onderdeel 38, van Richtlijn (EU) 2019/944, voor zover de opwekking van elektriciteit hun belangrijkste commerciële of professionele activiteit vormt, of zij één of meerdere productie-installaties met een cumulatief nominaal vermogen van ten minste 100 megawatt beheren
		— Benoemde elektriciteitsmarktbeheerders als bedoeld in artikel 2, onderdeel 8, van Verordening (EU) 2019/943[2] — Marktdeelnemers als bedoeld in artikel 2, onderdeel 25, van Verordening (EU) 2019/943 die aggregatie verrichten of vraagrespons- of energieopslagdiensten verstrekken als bedoeld in artikel 2, onderdelen 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
	Stadsverwarming en -koeling	— Exploitanten van stadsverwarming of stadskoeling als bedoeld in artikel 2, onderdeel 19, van Richtlijn (EU) 2018/2001[3]

	Aardolie	— Exploitanten van oliepijpleidingen
		— Exploitanten van voorzieningen voor de productie, raffinage en behandeling van olie, opslag en transport
		— Centrale entiteiten voor de voorraadvorming als bedoeld in artikel 2, onderdeel f, van Richtlijn 2009/119/EG[4]
	Aardgas	— Leveringsbedrijven als bedoeld in artikel 2, onderdeel 8, van Richtlijn 2009/73/EG[5]
		— Distributiesysteembeheerders als bedoeld in artikel 2, onderdeel 6, van Richtlijn 2009/73/EG
		— Transmissiesysteembeheerders als bedoeld in artikel 2, onderdeel 4, van Richtlijn 2009/73/EG
		— Opslagsysteembeheerders als bedoeld in artikel 2, onderdeel 10, van Richtlijn 2009/73/EG
		— LNG-systeembeheerders als bedoeld in artikel 2, onderdeel 12, van Richtlijn 2009/73/EG
		— Aardgasbedrijven als bedoeld in artikel 2, onderdeel 1, van Richtlijn 2009/73/EG
		— Exploitanten van voorzieningen voor de raffinage en behandeling van aardgas
	Waterstof	— Exploitanten van voorzieningen voor de productie, opslag en transmissie van waterstof
Vervoer	Lucht	— Luchtvaartmaatschappijen als bedoeld in artikel 3, onderdeel 4, Verordening (EG) nr. 300/2008 die voor commerciële doeleinden worden gebruikt
		— Luchthavenbeheerders als bedoeld in artikel 2, onderdeel 2, van Richtlijn 2009/12/EG[6], luchthavens als bedoeld in artikel 2, onderdeel 1, van die richtlijn, met inbegrip van de kernluchthavens die in bijlage II, afdeling 2, bij Verordening (EU) 1315/2013[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 als bedoeld in artikel 2, onderdeel 1, van Verordening (EG) nr. 549/2004[8] aanbieden
	Spoor	— Infrastructuurbeheerders als bedoeld in artikel 3, onderdeel 2, van Richtlijn 2012/34/EU[9]
		— Spoorwegondernemingen als bedoeld in artikel 3, onderdeel 1, van Richtlijn 2012/34/EU, inclusief exploitanten van dienstvoorzieningen als bedoeld in artikel 3, onderdeel 12, van die richtlijn
	Water	— Bedrijven voor vervoer over water (binnenvaart, kust- en zeevervoer) van passagiers en vracht zoals voor maritiem transport gedefinieerd in bijlage I bij Verordening (EG) nr. 725/2004[10], met uitzondering van de door deze bedrijven geëxploiteerde individuele vaartuigen
		— Beheerders van havens als bedoeld in artikel 3, onderdeel 1, van Richtlijn 2005/65/EG[11], inclusief hun havenfaciliteiten als bedoeld in artikel 2, onderdeel 11, van Verordening (EG) nr. 725/2004; alsook entiteiten die werken en uitrusting in havens beheren
		— Exploitanten van verkeersbegeleidingssystemen (VBS) als bedoeld in artikel 3, onderdeel o, van Richtlijn 2002/59/EG[12]
	Weg	— Wegenautoriteiten als bedoeld in artikel 2, onderdeel 12, van gedelegeerde Verordening (EU) 2015/962[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 als bedoeld in artikel 4, onderdeel 1, van Richtlijn 2010/40/EU[14]
Bankwezen		Kredietinstellingen als bedoeld in artikel 4, onderdeel 1, Verordening (EU) nr. 575/2013[15]
Infrastructuur voor de financiële markt		— Exploitanten van handelsplatformen als bedoeld in artikel 4, onderdeel 24, van Richtlijn 2014/65/EU[16]
		— Centrale tegenpartijen als bedoeld in artikel 2, onderdeel 1, Verordening (EU) nr. 648/2012[17]
Gezondheidszorg		— Een zorgaanbieder als bedoeld in artikel 1, eerste lid, van de Wet kwaliteit, klachten en geschillen zorg
		— EU-referentielaboratoria als bedoeld in artikel 15 van Verordening (EU) 2022/2371[18]
		— Entiteiten die onderzoeks- en ontwikkelingsactiviteiten uitvoeren met betrekking tot geneesmiddelen als bedoeld in artikel 1, onderdeel 2, van Richtlijn 2001/83/EG[19] — 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[20]
Drinkwater		Leveranciers en distributeurs van voor menselijke consumptie bestemd water als bedoeld in

		artikel 2, onderdeel 1, subonderdeel a, van Richtlijn (EU) 2020/2184[21], 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
Afvalwater		Ondernemingen die stedelijk afvalwater, huishoudelijk afvalwater of industrieel afvalwater als bedoeld in artikel 2, onderdelen 1, 2 en 3, van Richtlijn 91/271/EEG[22] 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
Digitale infrastructuur		— Aanbieders van internetknooppunten
		— DNS-dienstverleners
		— Register voor topleveldomeinnamen
		— Aanbieders van cloudcomputingdiensten
		— Aanbieders van datacentrumdiensten
		— Aanbieders van netwerken voor de levering van inhoud
		— Verleners van vertrouwensdiensten
		— Aanbieders van openbare elektronische communicatienetwerken
		— Aanbieders van openbare elektronische communicatiediensten
Beheer van ICT-diensten (business-to-business)		— Aanbieders van beheerde diensten — Aanbieders van beheerde beveiligingsdiensten

Overheid	Centrale overheden	— Ministeries met inbegrip van de daartoe behorende dienstonderdelen doch met uitzondering van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017
		— Zelfstandige bestuursorganen, voor zover zij kwalificeren als overheidsinstantie
	Decentrale overheden	— Provincies
		— Gemeenten
		— Waterschappen
		— Openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties als bedoeld in artikel 8, eerste, tweede, onderscheidenlijk derde lid, van de Wet gemeenschappelijke regelingen, voor zover deze openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties kwalificeren als overheidsinstantie
Ruimtevaart		Operators 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 elektronische communicatienetwerken

[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 (*PbEU* 2019, L 158).
[2] Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit (*PbEU* 2019, L 158).
[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 (*PbEU* 2018, L 328).
[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 (*PbEU* 2009, L 265).

[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 (*PbEU* 2009, L 211).
[6] Richtlijn 2009/12/EG van het Europees Parlement en de Raad van 11 maart 2009 inzake luchthavengelden (*PbEU* 2009, L 70).
[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 (*PbEU* 2013, L 348).
[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) (*PbEU* 2004, L 96).
[9] Richtlijn 2012/34/EU van het Europees Parlement en de Raad van 21 november 2012 tot instelling van één Europese spoorwegruimte, (*PbEU* 2012, L 343).
[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 (*PbEU* 2004, L 129).
[11] Richtlijn 2005/65/EG van het Europees Parlement en de Raad van 26 oktober 2005 betreffende het verhogen van de veiligheid van havens (*PbEU* 2005, L 310).
[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 (*PbEU* 2002, L 208).
[13] Gedelegeerde verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft (*PbEU* 2015, L 157).
[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 (*PbEU* 2010, L 207).
[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 (*PbEU* 2013, L 176).
[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 (*PbEU* 2014, L 173).
[17] Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (*PbEU* 2012, L 201).
[18] 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 (*PbEU* 2022, L 314).
[19] 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 (*PbEU* 2001, L 311).
[20] 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 (*PbEU* 2022, L 20).
[21] Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water (*PbEU* 2020, L 435).
[22] Richtlijn 91/271/EEG van de Raad van 21 mei 1991 inzake de behandeling van stedelijk afvalwater (*PbEU* 1991, L 135).

Bijlage 2

Sector	Subsector	Soort entiteit
Post- en koeriersdiensten		Aanbieders van postdiensten als bedoeld in artikel 2, onderdeel 1 bis, van Richtlijn 97/67/EG[1], met inbegrip van aanbieders van koeriersdiensten, voor zover zij ten minste een van de stappen in de postbestelketen verzorgen, met name het ophalen, sorteren, vervoeren en bestellen van postzendingen, met inbegrip van de ophaaldiensten, waarbij rekening moet worden gehouden met de mate waarin zij afhankelijk zijn van netwerk- en informatiesystemen. Uitgezonderd zijn vervoersdiensten die niet in samenhang met een van die stappen worden ondernomen.
Afvalstoffenbeheer		Ondernemingen die handelingen in het kader van afvalstoffenbeheer uitvoeren als bedoeld in artikel 3, onderdeel 9, van Richtlijn 2008/98/EG[2], met uitzondering van ondernemingen waarvoor afvalstoffenbeheer niet de voornaamste economische activiteit is
Vervaardiging, productie en distributie van chemische stoffen		Ondernemingen die stoffen vervaardigen en stoffen of mengsels distribueren als bedoeld in artikel 3, onderdelen 9 en 14, van Verordening (EG) nr. 1907/2006[3] en ondernemingen die voorwerpen als bedoeld in artikel 3, onderdeel 3, van die verordening produceren uit stoffen of mengsels

Productie, verwerking en distributie van levensmiddelen		Levensmiddelenbedrijven als bedoeld in artikel 3, onderdeel 2, Verordening (EG) nr. 178/2002[4] die zich bezighouden met groothandel en industriële productie en verwerking
Vervaardiging	Vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek	Entiteiten die medische hulpmiddelen als bedoeld in artikel 2, onderdeel 1, van Verordening (EU) 2017/745[5] vervaardigen en entiteiten die medische hulpmiddelen voor in-vitrodiagnostiek als bedoeld in artikel 2, onderdeel 2, van Verordening (EU) 2017/746[6] vervaardigen, met uitzondering van entiteiten die medische hulpmiddelen vervaardigen als bedoeld in bijlage I, onderdeel 5, vijfde streepje, van deze richtlijn
	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
	Vervaardiging van elektrische apparatuur	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 27, van NACE Rev. 2
	Vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 28, van NACE Rev. 2
	Vervaardiging van motorvoertuigen, aanhangers en opleggers	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 29, van NACE Rev. 2
	Vervaardiging van andere transportmiddelen	Ondernemingen die economische activiteiten uitvoeren als bedoeld in sectie C, afdeling 30, van NACE Rev. 2
Digitale aanbieders		— Aanbieders van onlinemarktplaatsen

		— Aanbieders van onlinezoekmachines
		— Aanbieders van platforms voor socialenetwerkdiensten
Onderzoek		Onderzoeksorganisaties, met als hoofddoel 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.

[1] Richtlijn 97/67/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende gemeenschappelijke regels voor de ontwikkeling van de interne markt voor postdiensten in de Gemeenschap en de verbetering van de kwaliteit van de dienst (*PbEU* 1998, L 15).
[2] Richtlijn 2008/98/EG van het Europees Parlement en de Raad van 19 november 2008 betreffende afvalstoffen en tot intrekking van een aantal richtlijnen (*PbEU* 2008, L 312).
[3] 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 (*PbEU* 2006, L 396).
[4] 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 (*PbEU* 2002, L 31).
[5] 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 (*PbEU* 2017, L 117).
[6] 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 (*PbEU* 2017, L 117).