

Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet)

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

Alzo Wij in overweging genomen hebben dat het gelet op richtlijn (EU) 2016/1148 noodzakelijk is om wettelijke bepalingen vast te stellen ter bevordering van de beveiliging van netwerk- en informatiesystemen;

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. BEGRIPSBEPALINGEN

Artikel 1 (begripsbepalingen)

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

- *aanbieder*: overheidsorganisatie of privaatrechtelijke rechtspersoon die een dienst exploiteert, beheert of beschikbaar stelt;
- *aanbieder van een essentiële dienst*: aanbieder van een essentiële dienst als bedoeld in artikel 4 van de NIB-richtlijn, aangewezen op grond van artikel 5, eerste lid, onder a;
- *beveiliging van netwerk- en informatiesystemen, digitale dienst, incident, netwerk- en informatiesysteem, norm, onderscheidenlijk risico*: hetgeen daaronder wordt verstaan in artikel 4 van de NIB-richtlijn;
- *bevoegde autoriteit*: bevoegde autoriteit, genoemd in artikel 4;
- *CSIRT*: Computer security incident response team als bedoeld in artikel 9 van de NIB-richtlijn;
- *CSIRT voor digitale diensten*: CSIRT, aangewezen op grond van artikel 4, tweede lid, onder b;
- *digitaledienstverlener*: rechtspersoon die een digitale dienst aanbiedt en gelet op artikel 18, eerste en tweede lid, van de NIB-richtlijn onder de jurisdictie van Nederland valt, met uitzondering van kleine en micro-ondernemingen als bedoeld in artikel 16, elfde lid, van de NIB-richtlijn;
- *NIB-richtlijn*: richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194);
- *Onze Minister*: Onze Minister van Veiligheid en Justitie;
- *vitale aanbieder*:
 - a. aanbieder van een essentiële dienst;
 - b. aanbieder van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving.

HOOFDSTUK 2. TAKEN VAN ONZE MINISTER

Artikel 2 (centraal contactpunt; CSIRT voor essentiële diensten)

Onze Minister is:

- a. het centrale contactpunt, bedoeld in artikel 8 van de NIB-richtlijn;
- b. voor aanbieders van een essentiële dienst: het CSIRT.

Artikel 3 (taken van Onze Minister)

1. Onze Minister heeft, ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen van vitale aanbieders, en van andere aanbieders die onderdeel zijn van de rijksoverheid, ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving en ter uitvoering van de NIB-richtlijn, de volgende taken:

- a. de taken van het centrale contactpunt, bedoeld in artikel 8 van de NIB-richtlijn;

- b. voor aanbieders van een essentiële dienst: de taken van het CSIRT, genoemd in bijlage I van de NIB-richtlijn;
 - c. het bijstaan van de in de aanhef bedoelde aanbieders bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen;
 - d. het informeren en adviseren van deze aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot de in de aanhef bedoelde netwerk- en informatiesystemen;
 - e. het verrichten van analyses en technisch onderzoek ten behoeve van de onder b, c en d genoemde taken, naar aanleiding van de onder d bedoelde dreigingen en incidenten of aanwijzingen daarvoor, niet zijnde onderzoek naar personen of organisaties die voor die dreigingen of incidenten verantwoordelijk zijn of die daar anderszins aan bijdragen of hebben bijgedragen.
2. Voorts heeft Onze Minister, ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland, tot taak: het verstrekken van ingevolge het eerste lid, onder e, verkregen gegevens over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen dan bedoeld in de aanhef van het eerste lid aan:
- a. organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren;
 - b. CSIRT's;
 - c. computercrisisteam, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie;
 - d. aanbieders van internettoegangs- en internetcommunicatiediensten ten behoeve van het informeren van gebruikers van die diensten.

HOOFDSTUK 3. TAKEN VAN ANDERE INSTANTIES

Artikel 4 (bevoegde autoriteit; CSIRT voor digitale diensten)

1. De bevoegde autoriteit, bedoeld in artikel 8, eerste lid, van de NIB-richtlijn, is voor de sectoren, genoemd in bijlage II van die richtlijn:

Bevoegde autoriteit	Sector
Onze Minister van Economische Zaken	energie
	digitale infrastructuur
De Nederlandsche Bank	bankwezen
	infrastructuur voor de financiële markt
Onze Minister van Infrastructuur en Milieu	vervoer
	levering en distributie van drinkwater
Onze Minister van Volksgezondheid, Welzijn en Sport	gezondheidszorg

2. Voor de digitale diensten, genoemd in bijlage III van de NIB-richtlijn, is:
- a. de bevoegde autoriteit, bedoeld in artikel 8, eerste lid, van de NIB-richtlijn: Onze Minister van Economische Zaken;
 - b. het CSIRT: de bij algemene maatregel van bestuur aangewezen instantie.
3. De bevoegde autoriteit heeft voor de aanbieders van een essentiële dienst in de betrokken sector of sectoren, onderscheidenlijk voor de digitaaldienstverleners, tot taak zorg te dragen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens deze wet.
4. Het CSIRT voor digitale diensten heeft voor digitaaldienstverleners de taken van het CSIRT, genoemd in bijlage I van de NIB-richtlijn.

HOOFDSTUK 4. BEVEILIGINGSEISEN EN MELDING VAN INCIDENTEN

§ 1. Algemeen

Artikel 5 (aanwijzing van vitale aanbieders)

1. Bij algemene maatregel van bestuur of bij besluit van een bij die maatregel genoemd bestuursorgaan worden aangewezen:
 - a. aanbieders van een essentiële dienst of categorieën van zodanige aanbieders;
 - b. andere vitale aanbieders of categorieën van zodanige aanbieders.
2. Bij de toepassing van het eerste lid, onder a, worden de artikelen 5 en 6 van de NIB-richtlijn en bijlage II van die richtlijn in acht genomen.

Artikel 6 (voorrang voor sectorspecifieke EU-regels)

Ter uitvoering van artikel 1, zevende lid, van de NIB-richtlijn kan bij algemene maatregel van bestuur worden bepaald dat daarbij aangewezen, bij of krachtens deze wet gestelde voorschriften niet gelden voor daarbij aangewezen categorieën van aanbieders van essentiële diensten of digitaalendienstverleners.

§ 2. Beveiliging

Artikel 7 (risico's beheersen)

1. De aanbieder van een essentiële dienst en de digitaalendienstverlener nemen passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De maatregelen zorgen, gezien de stand van de techniek, voor een niveau van beveiliging dat is afgestemd op de risico's die zich voordoen.
2. De in het eerste lid bedoelde maatregelen van de digitaalendienstverlener houden in elk geval rekening met de volgende aspecten:
 - a. de beveiliging van systemen en voorzieningen;
 - b. behandeling van incidenten;
 - c. het beheer van de bedrijfscontinuïteit;
 - d. toezicht, controle en testen;
 - e. inachtneming van de internationale normen.

Artikel 8 (gevolgen van incidenten voorkomen en minimaliseren)

De aanbieder van een essentiële dienst en de digitaalendienstverlener nemen passende maatregelen om de gevolgen van incidenten die de beveiliging van de voor de verlening van de betrokken dienst gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en te minimaliseren, teneinde de continuïteit van die dienst te waarborgen.

Artikel 9 (nadere regels)

Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gegeven over de maatregelen, bedoeld in de artikelen 7 en 8.

§ 3. Meldplicht voor incidenten

Artikel 10 (aangewezen vitale aanbieder)

1. De vitale aanbieder, aangewezen op grond van artikel 5, eerste lid, onder a of b, meldt onverwijld bij Onze Minister:
 - a. een incident met aanzienlijke gevolgen voor de continuïteit van de door hem verleende dienst;
 - b. een inbreuk op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kan hebben voor de continuïteit van de door hem verleende dienst.
2. De aanbieder van een essentiële dienst meldt een incident als bedoeld in het eerste lid, onder a, ook onverwijld bij de bevoegde autoriteit.

3. Onverminderd artikel 13 meldt de aanbieder van een essentiële dienst een incident bij een digitaledienstverlener onverwijld bij Onze Minister en bij de bevoegde autoriteit, als dat incident aanzienlijke gevolgen heeft voor de continuïteit van zijn essentiële dienst.
4. Om te bepalen of een incident aanzienlijke gevolgen heeft voor de continuïteit van de essentiële dienst, worden in elk geval in aanmerking genomen:
 - a. het aantal gebruikers dat door de verstoring van de dienst wordt getroffen;
 - b. de duur van het incident;
 - c. de omvang van het geografische gebied dat door het incident is getroffen.
5. In afwijking van artikel 1 wordt in het derde lid onder digitaledienstverlener tevens de digitaledienstverlener verstaan die niet valt onder de jurisdictie van Nederland.

Artikel 11 (bij de melding te verstrekken gegevens)

De in artikel 10 bedoelde melding omvat in ieder geval:

- a. de aard en omvang van het incident;
- b. het vermoedelijke tijdstip van de aanvang van het incident;
- c. de mogelijke gevolgen in en buiten Nederland van het incident;
- d. een prognose van de hersteltijd;
- e. zo mogelijk, de door de aanbieder genomen of te nemen maatregelen om de gevolgen van het incident te beperken of herhaling hiervan te voorkomen;
- f. de contactgegevens van de functionaris die verantwoordelijk is voor het doen van de melding.

Artikel 12 (verstrekking nadere gegevens door aangewezen vitale aanbieder)

1. Desgevraagd verstrekt de aanbieder die een melding als bedoeld in artikel 10, eerste of derde lid, bij Onze Minister heeft gedaan, Onze Minister onverwijld alle overige gegevens die noodzakelijk zijn om:
 - a. de aanbieder bij te staan bij het treffen van maatregelen om de continuïteit van zijn diensten te waarborgen of te herstellen;
 - b. de risico's in te schatten voor de netwerk- en informatiesystemen, bedoeld in artikel 3, eerste lid, aanhef.
2. Het eerste lid is van overeenkomstige toepassing als de aanbieder een incident heeft gemeld bij de bevoegde autoriteit en deze de door haar ontvangen gegevens heeft verstrekt aan Onze Minister.

Artikel 13 (digitaledienstverlener)

1. Een digitaledienstverlener meldt een incident met aanzienlijke gevolgen voor de verlening van de door hem verleende dienst in de Europese Unie onverwijld bij:
 - a. het CSIRT voor digitale diensten, en
 - b. de bevoegde autoriteit.
2. Om te bepalen of een incident aanzienlijke gevolgen heeft als bedoeld in het eerste lid, worden in elk geval in aanmerking genomen:
 - a. het aantal gebruikers dat door de verstoring van de dienst wordt getroffen;
 - b. de duur van het incident;
 - c. de omvang van het geografische gebied dat door het incident is getroffen.
 - d. de omvang van de verstoring van de werking van de dienst;
 - e. de omvang van de gevolgen voor de economische en maatschappelijke activiteiten.
3. Het eerste lid geldt alleen als de digitaledienstverlener toegang heeft tot de informatie die nodig is om te beoordelen of het incident aanzienlijke gevolgen heeft als bedoeld in dat lid.

Artikel 14 (nadere regels meldplicht)

Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gegeven over de artikelen 10 tot en met 13, waaronder regels over:

- a. de gegevens die ter uitvoering van de artikelen 10, 11 en 13 worden verstrekt;

b. de wijze waarop een melding als bedoeld in artikel 10 of 13 wordt gedaan en waarop gegevens als bedoeld in artikel 12 worden verstrekt.

§ 4. Vrijwillige melding van incidenten

Artikel 15 (vrijwillige melding van incidenten)

1. Als een incident aanzienlijke gevolgen heeft voor de continuïteit van een dienst maar niet valt onder de meldplicht van paragraaf 3, kan de betrokken dienstverlener dat incident melden bij een bij algemene maatregel van bestuur aangewezen instantie.
2. De in het eerste lid bedoelde instantie neemt de melding niet in behandeling als dat haar onevenredig of overmatig zou belasten.

HOOFDSTUK 5. VERWERKING VAN GEGEVENS

Artikel 16 (verwerking van gegevens door Onze Minister en andere instanties)

1. Onze Minister verwerkt gegevens, waaronder persoonsgegevens, ten behoeve van de in artikel 3 genoemde doeleinden en taken. Hij is verwerkingsverantwoordelijke.
2. De bevoegde autoriteit verwerkt gegevens, waaronder persoonsgegevens, ten behoeve van de in artikel 4, derde lid, genoemde taak. Zij is verwerkingsverantwoordelijke.
3. Het CSIRT voor digitale diensten verwerkt gegevens, waaronder persoonsgegevens, ten behoeve van de taken, genoemd in bijlage I van de NIB-richtlijn. Het is verwerkingsverantwoordelijke.
4. De in artikel 15, eerste lid, bedoelde instantie verwerkt gegevens, waaronder persoonsgegevens, ten behoeve van de behandeling van de in dat lid bedoelde incidenten. Zij is verwerkingsverantwoordelijke.

Artikel 17 (verstrekking gegevens aan Onze Minister)

1. Onze Minister kan een rechtspersoon of een orgaan daarvan verzoeken om gegevens te verstrekken die noodzakelijk zijn voor de vervulling van de in artikel 3, eerste lid, onder b tot en met e, genoemde taken.
2. De rechtspersoon of het orgaan kan op grond van het eerste lid gevraagde persoonsgegevens ook aan Onze Minister verstrekken als die verstrekking onverenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verzameld.

Artikel 18 (verstrekking incidentinformatie aan en door centrale contactpunten)

1. Ter uitvoering van artikel 10, derde lid, eerste volzin, van de NIB-richtlijn stelt het CSIRT voor digitale diensten Onze Minister op de hoogte over gedane meldingen als bedoeld in artikel 13, eerste lid.
2. Als blijkt uit een melding door een aanbieder van een essentiële dienst van een incident als bedoeld in artikel 10, eerste lid, onder a, of derde lid, dat het incident aanzienlijke gevolgen heeft voor de continuïteit van een essentiële dienst in een andere lidstaat van de Europese Unie, stelt Onze Minister het centrale contactpunt van die lidstaat daarvan op de hoogte.
3. Op verzoek van de bevoegde autoriteit stuurt Onze Minister een melding van een incident als bedoeld in artikel 10, eerste lid, onder a, door naar het centrale contactpunt van de andere getroffen lidstaat.
4. Als dat passend is en in elk geval als twee of meer lidstaten getroffen zijn, stelt Onze Minister het centrale contactpunt van de getroffen lidstaten op de hoogte van een bij het CSIRT voor digitale diensten gemeld incident als bedoeld in artikel 13, eerste lid.
5. Als blijkt uit gegevens die Onze Minister heeft ontvangen van een centraal contactpunt in een andere lidstaat dat een daar gemeld incident aanzienlijke gevolgen heeft voor de continuïteit van:

- a. een essentiële dienst in Nederland: stelt Onze Minister de bevoegde autoriteit daarvan op de hoogte;
- b. een digitale dienst in Nederland: stelt Onze Minister het CSIRT voor digitale diensten en de bevoegde autoriteit daarvan op de hoogte.

Artikel 19 (verstrekking van vertrouwelijke gegevens door Onze Minister)

1. Ter uitvoering van de in artikel 3 genoemde taken verstrekt Onze Minister geen vertrouwelijke gegevens met betrekking tot een aanbieder als:
 - a. de geheimhouding van die gegevens onvoldoende is gewaarborgd, of
 - b. onvoldoende is gewaarborgd dat zij uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt.
2. Ter uitvoering van de in artikel 3 genoemde taken kan Onze Minister vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder, zonder diens instemming uitsluitend verstrekken voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. Ingevolge de eerste volzin worden uitsluitend gegevens verstrekt aan:
 - a. CSIRT's;
 - b. computercrisisteam, aangewezen bij regeling van Onze Minister of behorend tot een bij die regeling aangewezen categorie;
 - c. de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2017.
3. Als een vitale aanbieder, of een andere aanbieder die onderdeel is van de rijksoverheid, onvoldoende gevolg geeft aan een door Onze Minister gegeven advies, kan Onze Minister de in het advies opgenomen gegevens als bedoeld in het tweede lid verstrekken aan de bevoegde autoriteit of Onze betrokken Minister.
4. Voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken:
 - a. verstrekt Onze Minister onverwijld gegevens als bedoeld in het tweede lid aan de bevoegde autoriteit of Onze betrokken Minister;
 - b. kan Onze Minister, na raadpleging van de betrokken aanbieder, gegevens als bedoeld in het tweede lid verstrekken aan andere organisaties of over die gegevens mededelingen doen aan het publiek.
5. Het eerste lid geldt niet voor de in het vierde lid, onder b, bedoelde mededelingen aan het publiek.
6. Het tweede lid geldt niet voor zover dat nodig is ter uitvoering van artikel 18, tweede tot en met vijfde lid.
7. De Wet openbaarheid van bestuur is niet van toepassing op gegevens als bedoeld in het tweede lid, behalve voor zover die gegevens milieu-informatie inhouden als bedoeld in artikel 19.1a van de Wet milieubeheer.

Artikel 20 (openbaarmaking incidenten)

- Onverminderd artikel 19, vierde lid, onder b, kan de bevoegde autoriteit, na raadpleging van de betrokken aanbieder:
- a. als publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen: het publiek informeren over een gemeld incident als bedoeld in artikel 10, eerste lid, onder a;
 - b. als publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, of wanneer de openbaarmaking van het incident anderszins in het algemeen belang is: het publiek informeren over een gemeld incident als bedoeld in artikel 13, eerste lid, of vorderen dat de digitaaldienstverlener dit doet.

HOOFDSTUK 6. HANDHAVING

Artikel 21 (reikwijdte)

Dit hoofdstuk is alleen van toepassing op aanbieders van een essentiële dienst en digitaalendienstverleners.

Artikel 22 (toezichthoudende personen)

1. De door de bevoegde autoriteit aangewezen personen zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens deze wet.
2. Van een besluit als bedoeld in het eerste lid wordt mededeling gedaan door plaatsing in de Staatscourant.

Artikel 23 (beveiligingsaudit)

1. De bevoegde autoriteit kan een aanbieder van een essentiële dienst bij besluit de verplichting opleggen dat de aanbieder:
 - a. een onafhankelijke deskundige laat onderzoeken of de door de aanbieder genomen maatregelen voldoen aan de artikelen 7 en 8 en aan de nadere regels, bedoeld in artikel 9, en
 - b. de resultaten van dat onderzoek binnen een bij de aanwijzing gestelde redelijke termijn verstrekt aan de bevoegde autoriteit.
2. Het onderzoek wordt uitgevoerd op een door de bevoegde autoriteit voorgeschreven wijze.
3. Tenzij bij algemene maatregel van bestuur anders is bepaald, draagt de aanbieder de kosten van het onderzoek.
4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste en tweede lid.

Artikel 24 (bindende aanwijzing)

De bevoegde autoriteit kan degene die niet voldoet aan artikel 7 of 8 of aan de nadere regels, bedoeld in artikel 9, door middel van het geven van een aanwijzing verplichten om binnen een daarbij gestelde redelijke termijn de daarbij omschreven maatregelen te nemen.

Artikel 25 (last onder bestuursdwang)

De bevoegde autoriteit is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van:

- a. het bepaalde bij of krachtens deze wet;
- b. artikel 5:20, eerste lid, van de Algemene wet bestuursrecht.

Artikel 26 (bestuurlijke boete)

1. De bevoegde autoriteit kan aan de overtreder een bestuurlijke boete opleggen in geval van:
 - a. overtreding van het bepaalde bij of krachtens deze wet;
 - b. overtreding van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht.
2. De boete bedraagt ten hoogste:
 - a. in geval van overtreding van artikel 12 of van artikel 5:20, eerste lid, van de Algemene wet bestuursrecht: 1 miljoen euro;
 - b. in geval van een andere overtreding: 5 miljoen euro.
3. De werking van het besluit tot oplegging van de boete wordt opgeschort totdat de beroepstermijn is verstreken of, als beroep is ingesteld, op het beroep is beslist.
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, onder b.

HOOFDSTUK 7. SLOTBEPALINGEN

Artikel 27 (samenloop met wetsvoorstel Wet open overheid)

Als het bij geleidende brief van 5 juli 2012 aanhangig gemaakte voorstel van wet, houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid) (Kamerstukken 33328) tot wet is of wordt verheven ... PM

Artikel 28 (intrekking Wet gegevensverwerking en meldplicht cybersecurity)

De Wet gegevensverwerking en meldplicht cybersecurity wordt ingetrokken.

Artikel 29 (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 30 (citeertitel)

Deze wet wordt aangehaald als: Cybersecuritywet.

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.

De Staatssecretaris van Veiligheid en Justitie,
De Minister van Economische Zaken,
De Minister van Financiën,
De Minister van Infrastructuur en Milieu,
De Staatssecretaris van Infrastructuur en Milieu,
De Minister van Volksgezondheid, Welzijn en Sport,