Ministerie van Justitie en Veiligheid

Aan de Minister van Justitie en Veiligheid

Directie Wetgeving en Juridische Zaken
Sector staats- en bestuursrecht

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Datum
16 mei 2025

Onze referentie
6397844

nota

Indiening wetsvoorstellen Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten bij de Tweede Kamer

1. Aanleiding

De wetsvoorstellen Cyberbeveiligingswet (hierna: Cbw) en Wet weerbaarheid kritieke entiteiten (hierna: Wwke) zijn gereed voor de indiening bij de Tweede Kamer.

2. Geadviseerde besluiten

U wordt gevraagd om:

- in te stemmen met de wetsvoorstellen en bijbehorende toelichtingen;
- in te stemmen met de nadere rapporten op de adviezen van de Afdeling advisering van de Raad van State (hierna: Raad van State) op deze wetsvoorstellen; en
- in te stemmen met de verzending van de hiervoor genoemde stukken aan het Kabinet van de Koning ten behoeve van de indiening van deze wetsvoorstellen bij de Tweede Kamer der Staten-Generaal.

3. Kernpunten

Gelet op de urgentie van deze wetsvoorstellen heeft u de Raad van State verzocht om spoedadvies. Dat verzoek is gehonoreerd. De Raad van State heeft inmiddels geadviseerd. Bij beide wetsvoorstellen gaat het om een licht dictum (dictum B). In de bijgevoegde nadere rapporten reageert u op de adviezen van de Raad van State.

De belangrijkste punten uit de adviezen van de Raad van State zien op de volgende onderwerpen, die in paragraaf 4.2 nader worden toegelicht:

1. de toepasselijkheid van de Cbw en Wwke op overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving;
2. de coördinerende taak van de Minister van Justitie en Veiligheid;
3. de in beide wetsvoorstellen opgenomen uitzondering op de Wet open overheid; en
4. bijzondere categorieën van persoonsgegevens (ziet alleen op de Cbw, de Wwke bevat geen grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens).

U wordt voorts gewezen op de in beide wetsvoorstellen naderhand opgenomen grondslag om in het kader van de zorgplicht bij of krachtens algemene maatregel van bestuur (amvb) te kunnen regelen dat aan entiteiten de verplichting wordt opgelegd om producten of diensten van specifieke leveranciers te weren. Zie hierover meer in paragraaf 4.3.

Directie Wetgeving en Juridische Zaken
Sector staats- en bestuursrecht

Datum
16 mei 2025

Onze referentie
6397844

4. Toelichting

4.1 Kern van de wetsvoorstellen

Cyberbeveiligingswet (Cbw)

- De zogeheten NIS2-richtlijn[1] gaat over cyberbeveiliging en wordt in Nederland geïmplementeerd in de Cbw. Het doel van de Cbw is het vergroten van de digitale weerbaarheid van Nederland.
- Organisaties en bedrijven[2] die onder het toepassingsbereik van de Cbw vallen – zowel overheidsinstellingen als de private sector – moeten op grond van de Cbw (cyber)maatregelen nemen, onder meer om cyberrisico's te beheersen en ICT-incidenten te voorkomen (zorgplicht). Ook moeten zij grote ICT-incidenten melden (meldplicht). Dit moeten zij doen bij hun toezichthouder en hun zogeheten computer security incident response team (CSIRT), waarna het CSIRT hen kan bijstaan (bijvoorbeeld met advies over cybermaatregelen).
- De Cbw bevat ook specifieke verplichtingen voor entiteiten uit de digitale sector.

Wet weerbaarheid kritieke entiteiten (Wwke)

- De zogeheten CER-richtlijn[3] gaat over de weerbaarheid van kritieke entiteiten en wordt in Nederland geïmplementeerd in de Wwke. Het doel van de Wwke is het verhogen van de weerbaarheid van entiteiten die een essentiële dienst verlenen in Nederland binnen de sectoren uit de CER-richtlijn. Het gaat hierbij om weerbaarheid ten aanzien van alle relevante door de natuur en door de mens veroorzaakte risico's die de verlening van essentiële dienst of diensten door een kritieke entiteit kunnen verstoren.
- Organisaties en bedrijven[4] die onder het toepassingsbereik van de Wwke komen te vallen – de private sector en de centrale overheid – moeten maatregelen nemen om voor hun weerbaarheid te zorgen (zorgplicht). Ook moeten zij incidenten melden (meldplicht). De Wwke bevat naast plichten ook het recht op ondersteuning van het betrokken vakdepartement voor het vergroten van de weerbaarheid van entiteiten.

4.2 Adviezen Raad van State en de reactie daarop

Hieronder volgt een weergave van de belangrijkste punten uit de adviezen van de Raad van State en de reactie die daarop wordt gegeven in de nadere rapporten.

1. Toepasselijkheid op overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving

In de wetsvoorstellen die aan de Raad van State ter advies zijn voorgelegd is conform de NIS2-richtlijn en de CER-richtlijn bepaald dat de Cbw en Wwke niet van toepassing zijn op overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving. Volgens de Raad van State moet uitdrukkelijk bij wet worden bepaald op welke specifieke overheidsinstanties de wet niet van toepassing is. De wetsvoorstellen zijn naar aanleiding van dit advies aangepast, zodat expliciet bij wet is bepaald dat de wetten niet van toepassing zijn op het Ministerie van Defensie, de AIVD, de MIVD, het openbaar ministerie, de politie en de veiligheidsregio's.

[1] De afkorting NIS is afgeleid van de woorden *security of network and information*, de toevoeging "2" ziet op het feit dat de NIS2-richtlijn de opvolger is van de zogeheten NIS1-richtlijn.
[2] Zij worden in de Cbw genoemd: essentiële entiteiten en belangrijke entiteiten.
[3] De afkorting CER is ontleend aan de woorden *critical entities* en *resilience* die voorkomen in de titel van de Engelstalige naam van de CER-richtlijn.
[4] Zij worden in de Wwke genoemd: kritieke entiteiten.

Directie Wetgeving en Juridische Zaken
Sector staats- en bestuursrecht

Datum
16 mei 2025

Onze referentie
6397844

2. Coördinerende taak van Minister van Justitie en Veiligheid
De Raad van State adviseert om in de toelichtingen bij de wetsvoorstellen nader in te gaan op de wijze waarop invulling wordt gegeven aan de coördinerende taak en de (mede)betrokkenheid van de Minister van Justitie en Veiligheid, en de wetsvoorstellen zo nodig op dit punt aan te passen. Naar aanleiding van dit advies is in de nadere rapporten toegelicht hoe de coördinerende rol van de Minister van Justitie en Veiligheid wordt ingevuld en zijn de toelichtingen op de wetsvoorstellen hierop aangepast. Daarnaast zijn de wetsvoorstellen op sommige punten aangepast om de rol van de Minister van Justitie en Veiligheid duidelijker naar voren te brengen.

3. Uitzondering op de Wet open overheid
In beide wetsvoorstellen is geregeld dat de Wet open overheid niet van toepassing is op vertrouwelijke gegevens die onder andere de bevoegde autoriteit en het centrale contactpunt verwerken in het kader van de uitoefening van hun taken op grond van de Cbw en Wwke.[5] De Cbw voorziet ook in een dergelijke regeling voor wat betreft het CSIRT. Deze regeling is interdepartementaal overeengekomen; alle betrokken departementen onderschrijven het belang van deze regeling.

De Raad van State geeft in haar adviezen aan dat de Wet open overheid uitzonderingen kent in verband met onder meer de veiligheid van de Staat, bedrijfs- en fabricagegegevens en de eerbiediging van de persoonlijke levenssfeer. De Raad van State adviseert om nader te motiveren waarom het noodzakelijk is om in beide wetsvoorstellen te regelen dat de Wet open overheid niet van toepassing is op gegevens die in het kader van de wetsvoorstellen worden verstrekt.

Hierop is de reactie in de nadere rapporten, kort samengevat, als volgt. De door de Afdeling genoemde uitzonderingsgronden zijn niet toereikend, omdat deze niet de garantie bieden dat alle vertrouwelijke gegevens die in het kader van de Cbw en de Wwke worden verwerkt, niet openbaar kunnen worden gemaakt op grond van de Woo. De in beide wetsvoorstellen geregelde uitzondering op de Wet open overheid biedt de garantie dat vertrouwelijke gegevens, waarvan ook veel door entiteiten zelf zijn aangeleverd en die berusten bij de bevoegde autoriteit, het CSIRT of het centrale contactpunt, niet openbaar kunnen worden gemaakt op grond van de Wet open overheid. Zowel in het geval van de bevoegde autoriteit als in het geval van het CSIRT geldt dat de vertrouwelijkheid van die gegevens moet worden geborgd om schade bij entiteiten, zoals reputatieschade, toegenomen kwetsbaarheid en benadeling van de concurrentiepositie, zo veel als mogelijk te voorkomen. In het geval van het CSIRT is daarnaast ook van belang dat als het gaat om gegevens die niet verplicht hoeven te worden gemeld, het risico bestaat dat entiteiten terughoudend worden met het delen van informatie als de vertrouwelijkheid daarvan niet zo veel mogelijk is gewaarborgd. Daardoor kan de goede taakuitoefening door het CSIRT in het geding komen.

4. Bijzondere categorieën van persoonsgegevens
De Cbw voorziet in een grondslag voor de bevoegde autoriteit en het CSIRT om bijzondere categorieën van persoonsgegevens te verwerken. In de Wwke is een dergelijke grondslag niet opgenomen, omdat het in het kader van de Wwke niet nodig is om bijzondere persoonsgegevens te kunnen verwerken.

[5] Dit is geregeld in artikel 66, tweede lid, Cbw en artikel 34, tweede lid, Wwke. Milieu-informatie is uitgezonderd van deze regeling. Dit heeft te maken met het Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden (*Trb*. 2001, 73), ook wel het Verdrag van Aarhus, en de Richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad (*PbEU* 2003, L 41).

De Raad van State adviseert in haar advies op het wetsvoorstel Cbw om de in de Cbw opgenomen grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens te beperken tot de uitoefening van taken waarvoor verwerking van bijzondere categorieën van persoonsgegevens noodzakelijk is. Ook adviseert zij om te voorzien in passende en specifieke waarborgen. Naar aanleiding van dit advies is het wetsvoorstel Cbw zodanig aangepast dat de grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens door het CSIRT alleen ziet op de expliciet genoemde taken van het CSIRT waarbij de verwerking van zulke gegevens noodzakelijk kan zijn. Over de waarborgen is in het nader rapport op het wetsvoorstel Cbw aangegeven dat deze er voldoende zijn, onder verwijzing naar de Algemene verordening gegevensbescherming, de Uitvoeringswet Algemene verordening gegevensbescherming, de eisen die de NIS2-richtlijn in artikel 11, eerste lid, stelt aan het CSIRT en de verkorting van de maximale bewaartermijn ten aanzien van bijzondere categorieën van persoonsgegevens die door het CSIRT worden verwerkt van 60 naar 12 maanden.

4.3 Weren van leveranciers

- In beide wetsvoorstellen is een grondslag opgenomen om bij of krachtens amvb regels te stellen over de maatregelen die entiteiten in het kader van de zorgplicht moeten nemen en regels over de eisen die met betrekking tot die maatregelen aan entiteiten worden gesteld. Dit wordt aangemerkt als een nadere invulling van de zorgplicht.
- Met deze grondslag zal in de amvb's onder de Cbw en de Wwke worden geregeld dat de betrokken vakminister, in overeenstemming met de Minister van Justitie en Veiligheid, aan een entiteit de verplichting kan opleggen om producten of diensten van specifieke leveranciers te weren. Van deze bevoegdheid kan gebruik worden gemaakt als dat noodzakelijk is voor het beheersen van risico's die de nationale veiligheid raken. De bevoegdheid zal alleen kunnen worden gebruikt als onder meer vaststaat dat geen andere beheersmaatregelen mogelijk en realiseerbaar zijn.
- Met de hiervoor bedoelde wettelijke grondslag in de wetsvoorstellen en de gebruikmaking daarvan in de onderliggende amvb's (zoals hiervoor omschreven) geldt dat daarmee wordt aangesloten bij met name de reeds bestaande regelgeving hierover met betrekking tot aanbieders van openbare elektronische communicatienetwerken en -diensten (Telecommunicatiewet).
- Van belang is in dit verband ook dat u naar aanleiding van een motie van het lid Rajkowski c.s. heeft toegezegd om risico's bij inkoop en aanbesteding van producten en diensten mee te nemen bij de invulling van de zorgplicht.[6]

4.4 Politiek-bestuurlijke context

- De NIS2-richtlijn en de CER-richtlijn dienden met ingang van 18 oktober 2024 te zijn omgezet in nationale wet- en regelgeving. Nederland heeft deze richtlijnen niet tijdig kunnen omzetten. Dit komt doordat de omzetting naar nationale wetgeving een omvangrijk en complex traject is, waarbij grote zorgvuldigheid is vereist. Die grote zorgvuldigheid is vereist, omdat de Cbw en Wwke aanzienlijke impact hebben op tal van Nederlandse organisaties, zowel in de publieke als in de private sector. Er zijn ten opzichte van bestaande wetgeving meer en nieuwe sectoren en significant meer organisaties die moeten voldoen aan de nieuwe wetgeving. De toepasselijkheid op vele sectoren leidt er ook toe dat afstemming met bijna alle departementen vereist is. In het licht van de vertraagde omzetting wordt ook gewezen op de keuze van Nederland om, vanwege de hiervoor genoemde impact op organisaties, de implementatiewetsvoorstellen open te stellen voor internetconsultatie, hoewel dit bij implementatiewetgeving niet verplicht is. De internetconsultatie heeft waardevolle reacties opgeleverd. Naar aanleiding daarvan zijn de implementatiewetsvoorstellen op verschillende

[6] *Kamerstukken II* 2022/23, 36200 VII, nr. 62.

onderdelen aangepast en zijn de bijbehorende toelichtingen op punten aangevuld of verduidelijkt.
- De Europese Commissie is ten aanzien van beide richtlijnen een infractieprocedure gestart tegen Nederland.
- Het is ook veel andere lidstaten niet gelukt om de richtlijnen binnen de gestelde termijn te implementeren. Inmiddels heeft de Europese Commissie besloten om ten aanzien van 19 lidstaten (waaronder Nederland) een met redenen omkleed advies te zenden vanwege de onvolledige implementatie van de NIS2-richtlijn. Ten aanzien van de CER-richtlijn is nog niet bekend of de Europese Commissie ook hiertoe overgaat en ten aanzien van hoeveel lidstaten. Wel blijkt uit de officiële website van de Europese Unie dat 17 lidstaten (waaronder Nederland) nog geen nationale wet- en regelgeving tot stand hebben gebracht ter implementatie van de CER-richtlijn.[7]
- Vanwege de inhoudelijke samenhang van de NIS2-richtlijn en de CER-richtlijn zijn de implementatiewetsvoorstellen gezamenlijk voorbereid en worden de beleidskeuzes die beide richtlijnen verlangen, integraal gemaakt in een interdepartementaal traject onder leiding van JenV. Deze implementatiewetsvoorstellen zijn door JenV (DWJZ en NCTV) voorbereid in samenwerking met BZK, DEF, EZ, FIN, IenW, KGG, LVVN, VWS (Cbw en Wwke) en OCW (alleen Cbw). Andere betrokkenen zijn: het Nationaal Cyber Security Centrum, het Digital Trust Center, sectorale CSIRT's, DG Politie en Veiligheid van JenV, de AIVD, de MIVD, toezichthouders en brancheorganisaties.

4.5 Planning en toezending amvb's aan Tweede Kamer
- Eerder is gecommuniceerd dat het streven is dat de Cbw en de Wwke in het derde kwartaal van 2025 in werking treden. Met de op voorhanden zijnde indiening van de wetsvoorstellen bij de Tweede Kamer is duidelijk dat dat niet meer realistisch is.
- De Stuurgroep VAV is overeengekomen dat het raadzaam is om de concept-amvb's onder de Cbw en de Wwke na verwerking van de consultatiereacties onverplicht toe te zenden aan de Tweede Kamer, zodat de Tweede Kamer deze amvb's kan betrekken bij de behandeling van de wetsvoorstellen. Op dit moment wordt gewerkt aan het daarvoor gereed maken van die concept-amvb's, met inbegrip van de verwerking van de consultatiereacties. Zodra deze gereed zijn voor verzending, worden deze bij afzonderlijke nota aan u voorgelegd.

4.6 Bijlagen
- Wetsvoorstel Cbw
- Memorie van toelichting Cbw
- Nader rapport Cbw
- Wetsvoorstel Wwke
- Memorie van toelichting Wwke
- Nader rapport Wwke

5. Informatie die niet openbaar gemaakt kan worden

5.1 Toelichting
De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.

[7] https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32022L2557