Ministerie van Justitie en Veiligheid

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
28 oktober 2025

Onze referentie
6852843

nota

Wetsvoorstellen Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten

1. Aanleiding

De verslagen op het wetsvoorstel Cyberbeveiligingswet (hierna: Cbw) en het wetsvoorstel Wet weerbaarheid kritieke entiteiten (hierna: Wwke) zijn begin september uitgebracht. De nota's naar aanleiding van die verslagen zijn gereed voor verzending aan de Tweede Kamer.

Na de indiening van deze wetsvoorstellen is gebleken dat deze voorstellen op een aantal punten (primair technisch) aangepast moeten worden. Hiertoe is voor beide wetsvoorstellen een nota van wijziging opgesteld.

2. Geadviseerde besluiten

U wordt gevraagd om in te stemmen met:

- De nota naar aanleiding van het verslag op het wetsvoorstel Cbw;
- De nota naar aanleiding van het verslag op het wetsvoorstel Wwke;
- De nota van wijziging op het wetsvoorstel Cbw;
- De nota van wijziging op het wetsvoorstel Wwke;
- De verzending van deze stukken aan de Tweede Kamer middels de bijgevoegde brieven.

3. Kernpunten

In een nota naar aanleiding van het verslag reageert u op de vragen die Tweede Kamerleden in het verslag hebben gesteld over het wetsvoorstel. In de verslagen op beide wetsvoorstellen zijn geen fundamentele bezwaren geuit tegen de wetsvoorstellen. De vragen van de Kamerleden zien met name op het krijgen van aanvullende toelichtingen of verduidelijkingen over de wetsvoorstellen. Paragraaf 4.2 gaat in op de belangrijkste punten uit de verslagen en de reactie daarop.

4. Toelichting

4.1 Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten

Kern van de wetten

- De Cbw implementeert de zogeheten NIS2-richtlijn en gaat over cyberbeveiliging. De Wwke implementeert de zogeheten CER-richtlijn en gaat over de weerbaarheid van kritieke entiteiten.
- Beide wetten bevatten een zorgplicht.
    - Voor wat betreft de Cbw houdt dit in dat organisaties maatregelen moeten nemen om risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen en om ICT-incidenten te voorkomen. Voorbeelden van zulke maatregelen: het vaststellen en toepassen van

beleid over de beveiliging van genoemde systemen en beleid over risicomanagement.
    - Voor wat betreft de Wwke gaat het om het nemen van maatregelen om de weerbaarheid van essentiële diensten te waarborgen. Voorbeelden van zulke maatregelen: het plaatsen van detectieapparatuur om sabotage te voorkomen en het installeren van extra (reserve)stroomgeneratoren om te garanderen dat er ten tijde van een incident stroomvoorziening is.
- Beide wetten bevatten ook een meldplicht. Dat is de verplichting om grote incidenten te melden. Na een melding van een ICT-incident in het kader van de Cbw kan een zogeheten computer security incident response team (CSIRT) bijstand verlenen, bijvoorbeeld met advies over cybermaatregelen die een organisatie kan nemen.

Onderliggende amvb's
Gelijktijdig aan de wetsvoorstellen is gewerkt aan twee algemene maatregelen van bestuur (amvb's). Het gaat om het Cyberbeveiligingsbesluit (strekt ter uitwerking van de Cbw) en het Besluit weerbaarheid kritieke entiteiten (strekt ter uitwerking van de Wwke). Deze amvb's zijn in consultatie geweest en ter informatie aan de Tweede Kamer aangeboden. Zij zijn thans gereed om via de CBJ (ambtelijk voorportaal) en de ministerraad te worden aangeboden aan de Raad van State. De desbetreffende stukken worden in een afzonderlijke werkstroom aan u aangeboden.

Ingebrekestelling wegens te late implementatie
De NIS2-richtlijn en de CER-richtlijn moesten uiterlijk op 17 oktober 2024 zijn geïmplementeerd. Nederland heeft die deadline niet gehaald (zie hierover meer in paragraaf 4.2) en is daarom door de Europese Commissie in gebreke gesteld. Beide inbreukprocedures zitten op dit moment in de zogeheten administratieve fase. In deze fase informeert Nederland de Europese Commissie middels brieven over onder meer de stand van zaken en voortgang van de implementatie. Er is door de Europese Commissie nog geen zaak bij het Hof van Justitie geïnitieerd.

4.2 Nota's naar aanleiding van de verslagen
De belangrijkste onderwerpen uit de verslagen en de reactie daarop:

Overschrijding implementatietermijn
- In beide verslagen is gevraagd naar waarom Nederland de richtlijnen niet tijdig heeft geïmplementeerd.
- In beide nota's naar aanleiding van de verslagen legt u uit dat het tot stand brengen van de implementatiewet- en regelgeving helaas meer tijd heeft gekost, waardoor het niet is gelukt om de implementatie tijdig af te ronden. Dit komt doordat de omzetting naar nationale wetgeving een omvangrijk en complex traject is, waarbij grote zorgvuldigheid is vereist vanwege de aanzienlijke impact op vele Nederlandse organisaties. Dit was ook de belangrijkste reden om de wetsvoorstellen – anders dan bij implementatiewetgeving gebruikelijk is – open te stellen voor internetconsultatie, hetgeen waardevolle reacties heeft opgeleverd ter verbetering van de wetsvoorstellen.
- De Tweede Kamer is in brieven en debatten meermaals geïnformeerd over de niet-tijdige implementatie. Daarnaast is ook in andere communicatie, waaronder de website van de NCTV, gecommuniceerd over de niet-tijdige

Directie Wetgeving en Juridische Zaken
Sector staats- en bestuursrecht

Datum
28 oktober 2025

Onze referentie
6852843

implementatie, waarbij ook is aangegeven dat het streven is dat de implementatiewetten in het tweede kwartaal van 2026 in werking treden.

Gegevensverwerking en informatie-uitwisseling door instanties

- In het verslag op het wetsvoorstel Cbw zijn diverse vragen gesteld over de verwerking van (persoons)gegevens door instanties met taken in de Cbw en de informatie-uitwisseling van die instanties met andere instanties (bijvoorbeeld buitenlandse computercrisisteams) én de waarborgen daaromtrent.
- In de nota naar aanleiding van het verslag legt u uit dat de verwerking van gegevens door die instanties in de Cbw uitdrukkelijk is gekoppeld aan de noodzakelijkheid voor de uitvoering van de taken die aan hen in die wet zijn toegewezen. Ook voor informatie-uitwisseling met andere instanties is in de Cbw uitdrukkelijk bepaald dat het daarbij telkens moet gaan om informatie die voor de samenwerking noodzakelijk is. Bovendien moeten zij, als het specifiek gaat om de verwerking of verstrekking van persoonsgegevens, voldoen aan de in de Algemene verordening gegevensbescherming daaraan gestelde eisen. Op de naleving hiervan wordt toezicht gehouden door de Autoriteit persoonsgegevens en de functionaris gegevensbescherming.

Regelgevingsniveau

- In het verslag op het wetsvoorstel Cbw is kritiek op de opname van cyberveiligheidsmaatregelen in een amvb.
- In de nota naar aanleiding van het verslag licht u toe dat de zorgplicht uit de Cbw één van de hoofdelementen van die wet is en daarom is geregeld op wetsniveau. De uitgewerkte maatregelen die moeten worden genomen in het kader van de wettelijke zorgplicht zijn uitwerkingen van de zorgplicht. Daarom zijn de regels daarover opgenomen op het niveau van een amvb.

Onderwijsinstellingen

- In het verslag op het wetsvoorstel Cbw stellen leden van de fracties van GroenLinks-PvdA, D66, CDA en NSC vragen over het besluit van de regering om hbo- en wo-instellingen middels aanwijzing onder het toepassingsbereik van de Cbw te brengen.
- In de nota naar aanleiding van het verslag is hierover onder meer toegelicht dat dat besluit het resultaat is van een zorgvuldige afweging en in het belang is van een brede en duurzame beheersing van cyberrisico's en toenemende digitale dreigingen in de maatschappij. De onderwijskoepelorganisaties hebben in de aanloop naar het besluit bij OCW hun zorgen geuit over de tijd, inzet en middelen die de implementatie en uitvoering van de verplichtingen uit de Cbw vragen. Om die reden heeft de regering besloten tot een gefaseerde aanpak. Voor de zorgplicht is besloten dat deze voor hbo- en wo-instellingen 36 maanden na de aanwijzing ingaat, zodat zij zich hierop kunnen voorbereiden. Er is ten aanzien van de zorgplicht dan ook gedurende die periode geen sprake van toezicht in het kader van de Cbw. De andere verplichtingen uit de Cbw zijn wel direct na aanwijzing van toepassing en daarop zal direct toezicht plaatsvinden.
- De minister van OCW is akkoord met de in de nota naar aanleiding van het verslag opgenomen antwoorden over (de aanwijzing van) onderwijsinstellingen.

Directie Wetgeving en Juridische Zaken
Sector staats- en bestuursrecht

Datum
28 oktober 2025

Onze referentie
6852843

Aansluiting bij bestaande systematiek van de Aanpak vitaal

- In het verslag op het wetsvoorstel Wwke is gevraagd waarom in die wet is gekozen voor de systematiek waarin een primaire verantwoordelijkheid bij de vakminister ligt en een coördinerende verantwoordelijkheid bij de minister van Justitie en Veiligheid.
- In de nota naar aanleiding van het verslag is hierover uitgelegd dat de Wwke voor een groot deel aansluit op het huidige kader voor de bescherming van onze vitale infrastructuur: de Aanpak vitaal. De Aanpak vitaal kent een systematiek met een primaire verantwoordelijkheid bij de vakminister en een coördinerende verantwoordelijkheid bij de minister van Justitie en Veiligheid. Bij de implementatie van de CER-richtlijn is ervoor gekozen om aan te sluiten bij deze reeds bestaande systematiek. Dit omdat, zeker wat betreft de fysieke weerbaarheid, er sectoraal veel verschillen zijn die ook sectorale kennis en expertise behoeven. De vakminister staat daarnaast in nauwer contact met de "eigen" sector en heeft beter zicht op aanpalende sectorale wet- en regelgeving waar organisaties zich ook toe moeten verhouden. De sectoroverstijgende kennis wat betreft veiligheid en weerbaarheid die bij de minister van Justitie en Veiligheid ligt, wordt voldoende wettelijk geborgd door de rol die deze minister heeft bij veel onderdelen van de Wwke.

4.4 Nota's van wijziging

De bij nota van wijziging geregelde wijzigingen van de wetsvoorstellen zijn primair technisch van aard. Het gaat om de aanscherping van definities, het corrigeren van (verwijzings)fouten, het maken van verduidelijkingen (het wegnemen van onduidelijkheden in het wetsvoorstel) en het wijzigen van andere wetgeving (over het hoofd gezien ten tijde van de indiening van de wetsvoorstellen).

4.5 Politiek-bestuurlijke context

U bent primair politiek verantwoordelijk voor de implementatie van de NIS2-richtlijn en de CER-richtlijn als coördinerend bewindspersoon voor cybersecurity en de bescherming van de vitale infrastructuur. Vanwege de inhoudelijke samenhang van de richtlijnen is de implementatiewet- en regelgeving gezamenlijk voorbereid en worden de beleidskeuzes die beide richtlijnen verlangen, integraal gemaakt in een interdepartementaal traject onder leiding van uw departement.

De aan u voorgelegde stukken zijn voorbereid in samenwerking met BZK, DEF, EZ, FIN, IenW, KGG, LVVN, VWS, OCW, het Nationaal Cyber Security Centrum (NCSC) en toezichthoudende instanties.

De wetsvoorstellen worden in de Tweede Kamer behandeld door twee verschillende commissies: de Cbw wordt behandeld door de vaste commissie voor Digitale Zaken, terwijl de Wwke wordt behandeld door de vaste commissie voor Justitie en Veiligheid.

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.