Adviescollege toetsing regeldruk

Aan de minister van Economische Zaken
De heer V.P.G. Karremans LL.M., MSc
Postbus 20401
2500 EK DEN HAAG

Onze referentie
MvH/RvZ/ATR4306/2025-U201

Uw referentie

Datum
19 december 2025

Onderwerp
Regeling cyberbeveiliging EZ

Geachte heer Karremans,

Op 10 november 2025 is het *Cyberbeveiligingsregeling (Cbr) EZ* aan het Adviescollege toetsing regeldruk (ATR) voor advies voorgelegd. Er is voor dit ook een internetconsultatie van start gegaan. De reactietermijn en de adviestermijn van ATR eindigen op 21 december 2025

Context

Nederland dient de Europese richtlijnen *Network and Information Security Directive* (NIS2-richtlijn) en de *Critical Entities Resilience Directive* (CER-richtlijn) in Nederlandse wet- en regelgeving te implementeren. De NIS2 richtlijn introduceert maatregelen om de digitale veiligheid van belangrijke systemen te vergroten, terwijl de CER-richtlijn maatregelen betreft om de weerbaarheid te vergroten ten aanzien van andere risico's, zoals fysieke sabotage en natuurrampen. Voor de nationale implementatie van de NIS2-richtlijn zijn eerder de Cyberbeveiligingswet (Cbw) en het Cyberbeveiligingsbesluit (Cbb) door ATR van advies voorzien (in combinatie met de Wet weerbaarheid kritieke entiteiten (Wwke) en Besluit weerbaarheid kritieke entiteiten (Bkke) ten behoeve van implementatie van de CER-richtlijn).[1]

De NIS2-richtlijn, de Cbw en Cbb werken diverse verplichtingen uit voor zogenaamde essentiële en belangrijke entiteiten tot het nemen van maatregelen om de risico’s voor hun netwerk- en informatiesystemen te beheersen. De regelgeving heeft betrekking op entiteiten die op basis van een aantal (in de richtlijn bepaalde) criteria over dienstverlening, schaalgrootte of organisatietype worden onderscheiden. Te nemen maatregelen richten zich op digitale (cyber)risico’s

[1] Zie https://www.adviescollegeregeldruk.nl/documenten/2024/07/01/atr-advies-wetsvoorstellen-cyberbeveiligingswet-cbw-en-de-wet-weerbaarheid-kritieke-entiteiten-wwke en https://www.adviescollegeregeldruk.nl/documenten/2025/04/04/atr-advies-cyberbeveiligingsbesluit-en-besluit-weerbaarheid-kritieke-entiteiten.

Contact:
Postbus 16228
2500 BE DEN HAAG
Bezoekadres: Rijnstraat 50
2515 XP DEN HAAG
info@atr-regeldruk.nl
www.adviescollegeregeldruk.nl
Tel: 070-310 86 66

voor netwerk- en informatiesystemen, zoals het internet en het betalingsverkeer. De verplichtingen omvatten onder meer een zorgplicht en een meldplicht.

De reikwijdte van de bovenliggende wetten en besluiten is sectoroverstijgend. In de Cbw en het Cbb worden generieke regels gesteld die gelden voor alle sectoren die onder deze wetgeving vallen. In de Cbw en het Cbb zijn delegatiegrondslagen opgenomen om in een ministeriële regeling nadere sectorale uitwerking te geven aan de zorgplicht en meldplicht. De voorliggende ministeriële regeling bevat deze sectorspecifieke bepalingen voor economische zaken. De verschillende sectorale regelingen zijn waar relevant door het college in samenhang bezien. Daarbij acht het college het van belang om te benadrukken dat het gehele wetgevingspakket inzake Cyberbeveiliging een grote inspanning van diverse sectoren vraagt met forse regeldrukgevolgen (ruim één miljard aan regeldruk). Sectoren moeten bovendien op korte termijn gaan voldoen aan de regelgeving (inwerkingtreding is in 2026 voorzien). Nut en noodzaak van cyberbeveiliging staan niet ter discussie. De sectorale regelingen en de toelichtingen dienen wel de abstracte, juridische kaders zodanig te concretiseren dat deze kenbaar, werkbaar en haalbaar zijn voor de betreffende entiteiten. Het college constateert in de diverse adviezen dat de verschillende sectorale regelingen deze mate van concretisering nog niet bevatten. Het risico bestaat hiermee dat beleidsdoelen niet worden verwezenlijkt.

In de voorliggende ministeriele regeling werkt het ministerie werkt het Ministerie van Economische Zaken verder uit.

Inhoud van het voorstel

De Regeling cyberbeveiliging EZ werkt de Cbw en het Cbb nader uit voor de sectoren die onder verantwoordelijkheid vallen van de minister van Economische Zaken, waaronder:

1. digitale infrastructuur[2],
2. ruimtevaart,
3. post- en koeriersdiensten,
4. vervaardiging Bij de sector vervaardiging gaat het om de subsectoren a) vervaardiging van informaticaproducten en van elektronische en optische producten, b) vervaardiging van elektrische apparatuur, c) vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd, d) vervaardiging van motorvoertuigen, aanhangers en opleggers, en e) vervaardiging van andere transportmiddelen.
5. delen van de onderzoeksector.

De regeling concretiseert de zorgplicht door aanvullende eisen te stellen aan beleid, risicobeheer, beveiliging van systemen, bedrijfscontinuïteit, back-ups, softwareontwikkeling, toegangsbeheer en monitoring. Daarnaast specificeert zij per sector de criteria voor het bepalen wanneer een cyberincident als significant moet worden gemeld — bijvoorbeeld op basis van impact op dienstverlening, veiligheid, integriteit van gegevens, industriële processen of gebruikersaantallen.

[2] Betreft specifiek aanbieders van openbare elektronische communicatiediensten- en netwerken en internetknooppunten. Voor de rest van de digitale infrastructuur geldt een Europese uitvoeringsverordening en deze partijen zijn als gevolg hiervan uitgezonder van de meld- en zorgplicht uit deze regeling.

Toetsingskader

ATR beoordeelt de regeldrukgevolgen aan de hand van het volgende toetsingskader:

1. Nuloptie (nut en noodzaak): is er een taak voor de overheid en is wetgeving het meest aangewezen instrument?
2. Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een uitvoeringswijze die werkbaar is voor de doelgroepen die de wetgeving moeten naleven?
4. Zijn de gevolgen voor de regeldruk volledig en juist in beeld gebracht?

1. Nut en noodzaak

De *Regeling cyberbeveiliging EZ* geeft invulling aan de algemene zorg- en meldplichten uit de Cbw en het Cbb door deze te concretiseren voor de EZ-sectoren, zodat essentiële en belangrijke entiteiten precies weten welke maatregelen zij moeten nemen om cyberrisico's te beheersen. De regeling voorkomt dat organisaties zelf uiteenlopende interpretaties ontwikkelen, wat zou leiden tot inconsistent beveiligingsniveau en moeilijk uitvoerbaar toezicht. Daarom werkt de regeling de zorgplicht uit in concrete activiteiten, zoals het opstellen en uitvoeren van een beveiligingsbeleid en managementsystematiek, het borgen van bedrijfscontinuïteit, het uitvoeren van back-up- en herstelprocessen, het testen en beveiligen van softwareontwikkeling, het beheer van kwetsbaarheden, het segmenteren van netwerken, het toepassen van adequaat toegangs- en accountbeheer (waaronder beheer van bevoorrechte accounts) en het monitoren van systemen en activiteiten. Daarnaast regelt de regeling wanneer een cyberincident significant is en dus moet worden gemeld, zowel via algemene criteria (zoals ernstige verstoring of ongeoorloofde toegang) als sectorspecifieke criteria (bijvoorbeeld drempels voor telecom, post, ruimtevaart, industrie en onderzoek). Ook bevat de regeling regels voor samenwerking en informatie-uitwisseling tussen toezichthouders om toezicht effectief en uniform uit te voeren. Daarmee vormt de regeling een noodzakelijke schakel om de cyberweerbaarheid binnen kritieke ketens te verhogen en de praktische werking van de Cbw mogelijk te maken.

Het college ziet geen aanleiding voor een adviespunt onder nut en noodzaak.

2. Minder belastende alternatieven

De meldplicht verplicht essentiële en belangrijke entiteiten binnen de sectoren om significante cyberincidenten tijdig te rapporteren, zodat risico's voor digitale communicatie, logistieke ketens, productieprocessen, ruimtevaartdiensten en onderzoeksactiviteiten snel kunnen worden onderkend en beheerst. Onder de Cbw geldt daarvoor een meerfasige meldstructuur: een vroegtijdige waarschuwing binnen 24 uur na ontdekking van een mogelijk significant incident, gevolgd door een volledige melding binnen 72 uur en het aanleveren van aanvullende informatie zodra deze beschikbaar komt.

De regeling werkt deze meldplicht verder uit door sectorspecifieke drempelcriteria vast te stellen voor elektronische communicatienetwerken en -diensten, internetknooppunten, grondfaciliteiten in de ruimtevaartsector, post- en koeriersdiensten, industriële vervaardiging en onderzoeksorganisaties. Deze criteria concretiseren wanneer sprake is van een significant incident, bijvoorbeeld grootschalige verstoringen in telecommunicatie, uitval van besturings- of veiligheidsfuncties in industriële processen, verlies van communicatie met ruimtevoorwerpen of ern-

stige aantasting van gegevensintegriteit. Daarmee wordt geborgd dat incidenten met potentieel grote maatschappelijke of economische impact snel worden gesignaleerd en gemeld, zodat toezicht en respons tijdig kunnen worden ingezet. Echter kunnen lage drempelwaarden leiden tot hoge aantallen meldingen waarvan de behandeling veel capaciteit vergt, terwijl dit mogelijk niet in alle gevallen nuttig en proportioneel is. Om deze reden is in de voorbereiding van de regelingen naar een balans gezocht. De toelichting bij de regeling bevat echter geen onderbouwing hoe deze drempelwaarden tot stand zijn gekomen en of daarbij mogelijk minder belastende alternatieven zijn overwogen.

Onderdeel van de regeling is ook de zorgplicht, waaraan bedrijven moeten voldoen. Een belangrijk onderdeel van de zorgplicht is ook dat entiteiten maatregelen treffen om leveranciersrisico's te beperken. Bij deze maatregelen gaat het bijvoorbeeld om cybersecurity-eisen in contacten. De zorgplicht vereist verder dat organisaties kunnen aantonen dat de leveranciersrisico's zijn beheerst. Dat betekent dat zij periodiek moeten controleren of leveranciers voldoen aan de afgesproken beveiligingsmaatregelen, bijvoorbeeld via audits, bewijsdocumentatie of technische verificaties. Dit vraagt de nodige inspanningen van deze organisaties.

Het college merkt op dat de specifieke grenzen voor het verplicht melden te zijn vastgesteld, waarbij in de toelichting ontbreekt waarop deze keuzes zijn gebaseerd. Gelet op de regeldrukgevolgen die deze grenzen hebben, behoeven de grenzen nadere onderbouwing.

2.1 Het college adviseert te onderbouwen hoe de drempelwaarden en de uitwerking van de zorgplicht tot stand zijn gekomen, in welke mate bij de drempelwaarden de samenleving wordt ontwricht, welke mogelijk minder belastende alternatieven zijn overwogen en waarom die alternatieven niet zijn gekozen.

Binnen de betreffende sectoren zijn multinationals actief. Incidenten kunnen derhalve niet alleen in Nederland spelen, maar cyberincidenten kunnen de activiteiten raken van activiteiten in andere lidstaten. Voor bedrijven in de digitale sector, zoals clouddienstverleners en datacenters geldt sowieso een zogeheten "one jurisdiction regime", waarbij een entiteit onder het toepassingsbereik van 1 lidstaat valt en alleen in de lidstaat van zijn hoofdvestiging een melding van incidenten hoeft te doen, dus ook bij cross border effecten. Hiervoor volstaat het melden via het landelijke meldpunt.

3. Werkbaarheid

Voor een aantal wettelijke regimes bestaat een duidelijke inhoudelijke en operationele samenhang met de Cbw. Entiteiten die onder de reikwijdte van de Cbw vallen, zijn in meerdere gevallen ook onderworpen aan sectorspecifieke verplichtingen uit onder meer de Wet ruimtevaartactiviteiten, Verordening (EU) 2019/881, Verordening (EU) 2024/2847 en de Telecommunicatiewet. Deze wet- en regelgeving kent deels overlappende toezichtarrangementen met betrekking tot digitale infrastructuur, veiligheid en betrouwbaarheid van netwerk- en informatiesystemen. Om te waarborgen dat het toezicht op dergelijke entiteiten doelmatig, samenhangend en zonder dubbele lasten wordt uitgevoerd, voorziet artikel 51 van de Cbw in de mogelijkheid om bij ministeriële regeling autoriteiten aan te wijzen waarmee de Cbw-instanties — te weten de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt — samenwerken en informatie uitwisselen. De Regeling cyberbeveiliging EZ geeft aan deze bevoegdheid uitvoering door de ge-

noemde autoriteiten formeel aan te wijzen. Deze aanwijzing vormt de juridische basis die noodzakelijk is voor het rechtmatig delen van informatie die onder verschillende vertrouwelijkheids- en geheimhoudingsregimes valt. De toelichting geeft aan dat dit verzekert dat toezichthouders op sectorspecifieke regelgeving "effectief kunnen samenwerken en informatie kunnen uitwisselen met de Cbw-instanties" met het oog op doelmatig en samenhangend toezicht en het beperken van toezichtslasten voor bedrijven.
Door de aanwijzing valt informatie-uitwisseling binnen het toepassingsbereik van de Cbw. Daarmee wordt voorkomen dat toezichtprocessen gefragmenteerd raken of dat relevante incident- en risico-informatie niet kan worden gedeeld vanwege wettelijke beperkingen in andere toezichtkaders. De aanwijzing van autoriteiten onder artikel 14 van de regeling voorkomt dubbeltellingen, overlappende handhavingsacties en inconsistenties in risico-inschattingen. De regeling ondersteunt zo de doelstelling van de Cbw om te komen tot een hoog en uniform niveau van cyberweerbaarheid, terwijl tegelijkertijd de uitvoerbaarheid en proportionaliteit van het toezicht worden geborgd.

Voor de sector vervaardiging is op dit moment onduidelijk in hoeverre de nieuwe regeling uitvoerbaar is. Er is onvoldoende inzicht in de mate waarin de verplichtingen aansluiten bij de feitelijke bedrijfsvoering van ondernemingen in deze sector en in hoeverre de betreffende ondernemers zich bewust zijn van de nieuwe verplichtingen en de concrete gevolgen daarvan voor hun organisatie. Daarnaast is geeft de toelichting niet aan hoeveel en welke bedrijven onder de reikwijdte van deze regeling vallen. Hierdoor kan niet worden vastgesteld of de regeling voor deze doelgroep realistisch, proportioneel en handhaafbaar is. Het is daarmee ook niet duidelijk of de regeling in de praktijk werkbaar is voor bedrijven in de vervaardigingssector. Zonder consultatie kan niet worden vastgesteld of de regeling aansluit bij de operationele realiteit en mogelijkheden van deze bedrijven.

3.1 Het college adviseert om de werkbaarheid van de regeling nader toe te lichtingen en dit per sector uit te splitsen, vanwege de aard en activiteiten van de verschillende sectoren die onder de reikwijdte van deze regeling vallen.

Bij de wet heeft ATR geadviseerd om na een jaar een invoeringstoets uit te voeren. Dit adviespunt is door het ministerie niet opgevolgd: er zal alleen een evaluatie na 4 jaar worden uitgevoerd. Het college acht echter een invoeringstoets nog steeds nuttig, met name voor wat betreft de zorgplicht, omdat met een dergelijke invoeringstoets sneller kan worden ingespeeld op mogelijke knelpunten en tijdig kan worden bepaald of de criteria voor significante incidenten en de uitwerking van de zorgplicht passend en werkbaar zijn. Niet alle knelpunten zijn immers op dit moment te voorzien of weg te nemen. Een invoeringstoets kan ook een beeld geven in hoeverre en op welke wijze lastenvermindering mogelijk is.

3.2 Het college adviseert na een jaar een invoeringstoets te doen zodat tijdig kan worden bepaald of de invulling van de zorgplicht en criteria voor significante incidenten en de meldplicht passend en werkbaar zijn voor de bedrijven.

4. Gevolgen regeldruk

De huidige paragraaf over regeldruk is onvolledig. Hoewel in de toelichting bij Cbw en het Cbb de regeldruk reeds kwantitatief is onderbouwd, biedt deze ministeriële regeling een specifiekere afbakening van de entiteiten binnen het domein van Economische Zaken die daadwerkelijk onder de reikwijdte vallen. Daarmee is het van belang om beter inzicht te geven in de regeldrukeffecten die uit déze regeling voortvloeien. Het gaat daarbij nadrukkelijk niet om het kwantificeren van additionele regeldruk bovenop wat in de bovenliggende regelgeving al is vastgesteld; de verplichtingen worden met deze regeling slechts nader geconcretiseerd. Juist door deze concretisering is het wenselijk en noodzakelijk om in de toelichting expliciet te maken hoeveel bedrijven door deze regeling worden geraakt en welke regeldrukeffecten voor deze bedrijven gelden op basis van de reeds bepaalde verplichtingen. Dit concrete inzicht ontbreekt nu, waardoor onduidelijk blijft wat de daadwerkelijke gevolgen zijn voor de bedrijfsvoering van de ondernemingen die specifiek onder deze regeling vallen. Een nadere uitsplitsing draagt bij aan transparantie, voorspelbaarheid en een beter begrip van de impact van deze regeling op de betreffende sectoren.

4.1 Het college adviseert om de regeldrukeffecten voor de ondernemers die onder deze regeling vallen inzichtelijk te maken, conform de Rijksbrede methodiek.

Dictum

Gelet op bovengenoemde bevindingen is het eindoordeel ten aanzien van dit voorstel:

Niet indienen / vaststellen tenzij met de adviespunten rekening wordt gehouden.

Het college vertrouwt erop u hiermee voldoende te hebben geïnformeerd over de uitkomsten van de toetsing. Indien u het voorstel verder in procedure brengt, gaat ATR ervanuit dat de toelichting per adviespunt duidelijk maakt op welke wijze rekening is gehouden met het ATR-advies. Aanvullend verzoekt het college u deze gewijzigde versie van het voorstel aan ATR voor te leggen, zodat wij kunnen bepalen of een Aanvullende zienswijze opportuun is.

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris