



Adviescollege —  
toetsing regeldruk

Aan de minister van Klimaat en Groene Groei  
Mevrouw drs. S.Th.M. Hermans  
Postbus 20401  
2500 EK DEN HAAG

**Onze referentie**

MvH/RvZ/ATR4279/2025-U198

**Uw referentie**

**Datum**

18 december 2025

**Onderwerp**

Regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector

Geachte mevrouw Hermans,

Op 10 november 2025 is de *Regelingen cyberbeveiliging (Cbr) en weerbaarheid kritieke entiteiten (Rwke) energiesector* aan het Adviescollege toetsing regeldruk (ATR) voor advies voorgelegd. Er is voor dit voorstel 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. Deze richtlijnen bevatten maatregelen gericht op het vergroten van de digitale (NIS2) en de fysieke (CER) weerbaarheid van organisaties. Ten behoeve van deze implementatie wordt nationale wetgeving op drie verschillende niveaus opgesteld: 1) wet; 2) algemene maatregel van bestuur; 3) ministeriële regeling. Dit advies betreft de regeling. De regelingen worden per departement opgesteld, waarbij het Ministerie Klimaat en Groene Groei (KGG) specifiek regels stelt ten aanzien van energiesector.

**Inhoud van het voorstel**

De regeling cyberbeveiliging en weerbaarheid kritieke entiteiten energiesector van KGG werkt de Cyberbeveiligingswet (Cbw), het Cyberbeveiligingsbesluit (Cbb) en de Wet weerbaarheid kritieke entiteiten (Wwke) nader uit. Bij de kritieke entiteiten gaat het om de sectoren elektriciteit, gas en olie.

De regeling regelt ook verplichtingen onder de Cbw. Deze hebben betrekking op elektriciteit, stadsverwarming- en koeling, aardolie, aardgas en waterstof.

**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

De Wwke/Bwke en Cbw/Cbb grijpen op elkaar in doordat veel energiebedrijven onder beide wetten vallen. De wetten hebben echter elk een ander doel, maar hebben wel een sterke link. Kritieke entiteiten onder de Wwke worden automatisch als essentiële entiteit onder de Cbw geschaard, waarbij de Wwke breder gaat ten aanzien van dreigingen en is gekozen om de cyberdreiging in de Cbw uit te werken.

De Wwke richt zich op het waarborgen van de continuïteit van essentiële diensten in de energiesector. Zij verplicht kritieke entiteiten om incidenten te melden die een aanzienlijke verstoring van hun dienstverlening veroorzaken of kunnen veroorzaken, ongeacht of deze fysiek of digitaal is. De Wwke kent ook een zorgplicht, maar

De Cbw/Cbb richt zich specifiek op het versterken van de cyberweerbaarheid van essentiële en belangrijke entiteiten en bevat een meldplicht voor significante cyberincidenten en een veel uitgebreidere en concretere zorgplicht (onder andere beveiligingsbeleid, patchbeheer, segmentatie, BCP, kwetsbaarheidsscans). De meldcriteria zijn grotendeels geharmoniseerd om dubbele verplichtingen te voorkomen.

Het college benadrukt het belang dat het gehele wetgevingspakket inzake Cyberbeveiliging en Wet weerbaarheid kritieke entiteiten een grote inspanning van diverse sectoren vraagt met forse regeldrukgevolgen (ruim een miljard aan regeldruk). Sectoren moeten bovendien op korte termijn gaan voldoen aan de regelgeving (inwerkingtreding is in 2026 voorzien). Nut en noodzaak van veiligheid en leveringszekerheid 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.

### 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 is van toepassing op entiteiten in de energiesector die onder de Wwke of de Cbw vallen. Deze regelt de algemene zorg- en meldplichten uit de voorgenoemde regelgeving door deze te concretiseren voor de energiesector, zodat essentiële en belangrijke en kritische entiteiten precies weten welke maatregelen zij moeten nemen om risico's te beheersen. De regeling voorkomt dat organisaties zelf uiteenlopende interpretaties ontwikkelen, wat zou leiden tot inconsistent beveiligingsniveau en moeilijk uitvoerbaar toezicht. Daarom regelt de regeling wanneer een incident significant is en dus moet worden gemeld, zowel via algemene criteria (zoals ernstige verstoring of ongeoorloofde toegang) als sectorspecifieke criteria (bijvoorbeeld dremfels voor stadsverwarming en elektriciteit).

De zorgplicht verplicht energie-entiteiten om hun netwerk- en informatiesystemen structureel, aantoonbaar en risico gestuurd te beveiligen. Dit omvat het opzetten van een beheersysteem voor cybersecurity, waarin organisaties risico's analyseren, passende maatregelen vaststellen,

deze monitoren en periodiek evalueren. Daarnaast moeten zij een volledig bedrijfscontinuïteitsplan en robuuste back-upvoorzieningen hebben, inclusief herstelpunten, hersteltijden en periodieke testprocedures. In essentie verplicht de zorgplicht organisaties tot een volledig cyberbeveiligingsmanagementsysteem dat continu wordt verbeterd.

Het college ziet geen aanleiding voor opmerkingen onder nut en noodzaak.

## *2. Minder belastende alternatieven*

De meldplicht verplicht kritieke, belangrijke en essentiële entiteiten om ernstige incidenten tijdig te rapporteren zodat risico's voor de energievoorziening en -zekerheid en digitale veiligheid snel kunnen worden onderkend en beheerst. Onder de Wwke moeten kritieke entiteiten een incident dat de essentiële dienst aanzienlijk verstoort of kan verstoren, binnen 24 uur na kennisname melden, gevolgd door een uitgebreid verslag binnen één maand. Onder de Cyberbeveiligingswet geldt een meerfasige meldstructuur: een vroegtijdige waarschuwing binnen 24 uur, vervolgens een volledige melding binnen 72 uur, en aanvullende informatie zodra deze beschikbaar komt. De regeling bevat voor de energiesector specifieke drempelcriteria die bepalen wanneer sprake is van een meldplichtig incident, zoals verstoringen bij elektriciteit, gas, olie, warmte en waterstof. Hiermee moet de sector zowel fysieke verstoringen als significante cyberincidenten snel signaleren en melden, zodat op nationaal niveau tijdig kan worden ingegrepen.

In de toelichting is opgenomen dat de criteria van de meldplicht is afgestemd met de diverse energiepartijen, brancheverenigingen uit de desbetreffende sectoren en betrokken toezichthouders. Dit heeft als doel gehad om de regels goed te laten aansluiten op de praktijk en bestaande kaders, zoals de Wet beveiliging netwerk- en informatiesystemen (Wbni) en sectorale regelgeving, om de uitvoerbaarheid en handhaafbaarheid te borgen en onnodige regeldruk te beperken. 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.

De zorgplicht uit de regeling geldt voor essentiële en belangrijke entiteiten binnen de energiesector, waaronder de subsectoren elektriciteit (productie, transmissie, distributie en levering van stroom), aardgas (transport, opslag, invoer en levering van gas), aardolie (transport via leidingen, opslag, raffinage en wettelijke olievoorraden), stadsverwarming en -koeling (productie en levering van warmte en koude aan afnemers) en waterstof (productie, transport en opslag van waterstof). Deze sectoren leveren energie of energiedragers die essentieel zijn voor het functioneren van maatschappij en economie.

De zorgplicht waaraan bedrijven moeten voldoen is in de regeling nader uitgewerkt. Een belangrijk onderdeel van de zorgplicht is de verplichting voor essentiële en belangrijke entiteiten om conform de Cbw hun toeleveringsketen beveiligen. Hiervoor moet beleid schriftelijk worden vastgesteld en toegepast, waarin de omgang wordt bepaald met (afhankelijkheden van) producten en diensten van leveranciers en dienstverleners die de beveiliging van netwerk- en informatiesystemen kunnen beïnvloeden. Bovendien moet de entiteit 'periodiek toetsen of rechtstreekse leveranciers voldoen aan de eisen die de entiteiten opstellen met betrekking tot de

beveiliging van hun netwerk- en informatiesystemen. Onduidelijk is wat 'periodiek' inhoudt. In de regeling, waarin de zorgplicht nader is uitgewerkt, geeft over dit onderdeel geen uitsluitel. De toelichting gaat in op de afweging van de drempelwaarden en de wijze waarop zorgplicht is vormgegeven en besteedt geen aandacht aan mogelijke alternatieve waarden (en waarom daarvoor niet is gekozen). Omdat de drempelwaarden en de concrete verplichtingen bij de zorgplicht van invloed zijn op de proportionaliteit van de regeldruklasten en de werkbaarheid van de bepalingen acht het college deze toelichting wel noodzakelijk.

**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.**

*3. Werkbaarheid*

Uniek aan de regeling is dat het verplichtingen van twee verschillende wettelijke regimes regelt. De werkbaarheid van de zorgplicht hangt sterk af van de schaal, volwassenheid en digitaliseringsgraad van de entiteit. Voor grote energiebedrijven sluit de zorgplicht grotendeels aan op bestaande cybersecurity frameworks (zoals ISO 27001 of NIST), waardoor de extra lasten vooral liggen in het aantoonbaar maken van maatregelen en het formaliseren van processen zoals patchbeheer, back-ups en continuïteitsplanning. Voor middelgrote en kleinere entiteiten is de werkbaarheid uitdagender: de eisen zijn gedetailleerd en breed, vereisen specialistische kennis en raken vrijwel alle bedrijfsprocessen. Met name structurele documentatie, monitoring, netwerksegmentatie en periodiek testen van herstelprocedures vragen om aanvullende capaciteit en investeringen. Tegelijkertijd biedt de regeling duidelijke kaders, sluit zij aan bij bestaande best practices en is zij technisch neutraal, waardoor organisaties ruimte hebben om maatregelen proportioneel en risicogestuurd in te vullen. Hierdoor is de zorgplicht in de praktijk haalbaar, maar vraagt zij bij veel organisaties om professionalisering van cybersecurity-governance en extra organisatorische inbedding.

De toelichting gaat niet specifiek in op de vraag of de regeling werkbaar is voor de bedrijven en in hoeverre zij kunnen voldoen aan de verplichtingen en welke inspanning dit vergt. Het is verder onduidelijk hoeveel bedrijven onder de reikwijdte van deze regeling vallen en hoeveel bedrijven op dit moment al moeten voldoen aan de zorgplicht die uit deze regeling voortvloeit.

Voor de meldplicht zijn verschillende termijnen, die niet allemaal uit de regeling vallen. Onder de Wwke moet een kritieke entiteit een incident binnen 24 uur na kennisname melden, gevolgd door een uitgebreid verslag binnen één maand. De Cbw hanteert een meerfasig meldsysteem: een vroegtijdige waarschuwing binnen 24 uur, gevolgd door een volledige melding binnen 72 uur na kennisname, met eventuele aanvullende informatie zodra deze beschikbaar komt. Hiermee kent de Wwke één strikte meldtermijn, terwijl de Cbw een gedetailleerdere en meerlaagse rapportagestructuur voorschrijft.

**3.1 Het college adviseert om de werkbaarheid van de regeling nader toe te lichten en dit per sectoronderdeel uit te splitsen, daarbij na te gaan of gekozen kan worden voor het meest regeluwe alternatief van melden.**

Bij de wet heeft ATR geadviseerd om na een jaar een invoeringstoets uit te voeren. Dit adviespunt is door het Ministerie van Justitie en Veiligheid (JenV) niet opgevolgd: er zal alleen een evaluatie na 4 jaar worden uitgevoerd. Het college acht een invoeringstoets voor de zorgplicht nog steeds van toegevoegde waarde, omdat met een dergelijke toets 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 voor de sector. Niet alle knelpunten zijn immers op dit moment te voorzien of weg te nemen. Met een invoeringstoets kan ook sneller gekeken worden waar lastenvermindering mogelijk is. Een invoeringstoets acht het college tot slot ook passend gezien de snel opeenvolgende technologische ontwikkelingen.

**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 verschillende sectoren of onderdelen daarvan.**

*4. Gevolgen regeldruk*

De huidige paragraaf over regeldruk is onvolledig. Hoewel in de toelichting bij beide wetsvoorstellen de regeldruk kwantitatief is onderbouwd, biedt deze ministeriële regeling een specifiekere afbakening van de entiteiten binnen het domein van Klimaat en Groene Groei die daadwerkelijk onder de reikwijdte vallen. De regeling geeft echter geen inzicht in het aantal bedrijven dat specifiek onder deze regeling valt en ook niet van de impact op de bedrijfsvoering van deze ondernemingen.

**4.1 Het college adviseert om de regeldrukeffecten specifiek voor de ondernemers die onder deze regeling vallen concreet inzichtelijk te maken, gebruikmakend van de Rijksbrede methodiek.**

*Dictum*

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

**Niet 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