Adviescollege toetsing regeldruk

> **Retouradres** Postbus 16228 2500 BE Den Haag

Aan de minister van Justitie en Veiligheid
Mevrouw drs. D. Yeşilgöz-Zegerius
Postbus 20301
2500 EH DEN HAAG

ATR, Adviescollege toetsing regeldruk
Rijnstraat 50
2515 XP Den Haag

Postbus 16228
2500 BE Den Haag

T 070 310 86 66
E info@atr-regeldruk.nl
www.atr-regeldruk.nl

Onze referentie MvH/RvZ/PS/JH/ls/ATR2896/2024-U057
Uw referentie

Datum 1 juli 2024
Betreft Wetsvoorstellen Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke)

Geachte mevrouw Yeşilgöz-Zegerius,

Op 21 mei 2024 zijn aan het Adviescollege toetsing regeldruk (ATR) ter toetsing voorgelegd het concept wetsvoorstel Cyberbeveiligingswet (Cbw) en het wetsvoorstel Weerbaarheid kritieke entiteiten (Wwke). De adviestermijn van ATR loopt tot 2 juli 2024.

Context en aanleiding

De Cbw implementeert de *Critical Entities Resilience Directive (CER-richtlijn)*. Deze richt zich op *digitale* (cyber) risico's voor netwerk- en informatiesystemen, zoals het internet en het betalingsverkeer. Vergeleken met de NIS1-richtlijn komen meer organisaties onder de werking van de richtlijn te vallen en worden nieuwe verplichtingen opgelegd. Deze omvatten onder meer een zorgplicht, een meldplicht en een informatieplicht.
De Wwke implementeert de *Network and Information Security Directive (NIS2-richtlijn*). Deze richt zich op de bescherming van organisaties tegen *fysieke* dreigingen, zoals (terroristische) misdrijven, sabotage en natuurrampen. De NIS2-richtlijn kent vergelijkbare verplichtingen als de CER-richtlijn.
Beide richtlijnen moeten uiterlijk 17 oktober 2024 zijn geïmplementeerd.

Inhoud

De Cbw en Wwke stellen inhoudelijke eisen op hoofdlijnen, zoals de zorgplicht en de meldplicht. Deze worden in AMvB's nog nader uitgewerkt. De delegatiegrondslagen bieden daarbij de mogelijkheid om met sectorspecifieke regels te komen, zoals sectorspecifieke drempelwaarden voor het bepalen van incidenten die meldplichtig zijn. De wetsvoorstellen bieden verder de mogelijkheid om in lagere regelgeving sommige organisaties vrij te stellen van verplichtingen als de zorgplicht en de meldplicht, voor zover de richtlijnen bepaalde organisaties al niet hebben uitgezonderd.

Cyberbeveiligingswet (Cbw)

De Cbw maakt onderscheid naar essentiële organisaties en belangrijke organisaties. Criteria voor dat onderscheid zijn onder andere de sector en de omvang van de organisatie. Het onderscheid is met name van belang als het gaat om de vraag welk toezichtsregime op de organisatie van toepassing is.

De Cbw bevat een zorgplicht, een meldplicht en een registratieplicht:

- Zorgplicht: De betreffende organisaties moeten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Zij kunnen zelf bepalen wat passend en evenredig is. Ook moeten zij maatregelen nemen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten te beperken. Klanten en andere ontvangers van de diensten van de organisatie moeten worden geïnformeerd over significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. Ook deelt de organisatie alle maatregelen of voorzieningen die de ontvanger van de dienst ter beschikking staan om de risico's die uit een cyberdreiging voortvloeien te beperken. Het wetsvoorstel bevat verder bepalingen met betrekking tot de governance, het opstellen van een cybersecurity plan en gegevensuitwisseling tussen betrokken overheidsorganisatie, waaronder de "computer security incident response teams" (CSIRT).
- Meldplicht: Deze houdt in dat organisaties de melding doen bij zowel hun CSIRT als de toezichthoudende instantie (de zogenoemde dubbele meldplicht).
- Registratieplicht: De Cbw verplicht organisaties zich te registreren in het organisatieregister en om de betreffende registratie actueel te houden. Dit moet zorgen voor een Europees breed beeld van het aantal organisaties onder de NIS2.

Het toezicht zal door sectorale toezichthouders worden uitgeoefend. Het handhavingsinstrumentarium omvat diverse opties, waaronder een verplichte beveiligingsscan, beveiligingsaudit, openbaarmaking van een overtreding en het opleggen van een aanwijzing, een last onder bestuursdwang of een bestuurlijke boete. Het instrumentarium verschilt voor essentiële en belangrijke organisaties en ook voor organisaties die domeinnaamregistraties verlenen. Zo kan voor essentiële organisaties ook een controlefunctionaris aangewezen worden of een tijdelijke opschorting van een certificering opgelegd worden.

Wet weerbaarheid kritieke entiteiten (Wwke)

De Wwke richt zich op zogeheten kritieke entiteiten. Dat zijn organisaties, die in bepaalde sectoren een essentiële dienst verlenen die onmisbaar is voor de uitvoering van maatschappelijke functies en/of economische activiteiten. Lidstaten kunnen op nationaal niveau aanvullende sectoren vaststellen waarbinnen kritieke organisaties aangewezen kunnen worden.

De Wwke kent ten dele vergelijkbare verplichtingen als de Cbw:

- Zorgplicht: Kritieke organisaties moeten tenminste om de 4 jaar een risicobeoordeling uitvoeren en passende en evenredige technische, beveiligings- en organisatorische maatregelen nemen om de dienstverlening zoveel mogelijk te beschermen tegen fysieke risico's en dreigingen. De maatregelen worden nog geconcretiseerd in

een AMvB. Daarbij wordt de mogelijkheid geboden om het weerbaarheidsniveau te verhogen.

- Meldplicht: Organisaties moeten bij de bevoegde autoriteit melden als er een incident plaatsvindt dat de verlening van de essentiële dienst aanzienlijk verstoort of kan verstoren. Die melding bestaat uit twee fases: een eerste melding binnen 24 uur en een gedetailleerd verslag binnen een maand na de eerste melding. Ook moeten ze melden als ze essentiële diensten aan of in zes of meer lidstaten verlenen. Ze moeten hierbij vermelden om welke essentiële diensten en om welke lidstaten het gaat.
- Toezicht: De toezichthouders in de Wwke hebben als mogelijkheid om de kritieke organisatie te verplichten tot het uitvoeren van een audit of een aanwijzing op te leggen. Verder kan een toezichthouder een last onder bestuursdwang of een bestuurlijke boete opleggen.

Toetsingskader

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

1. Nut en noodzaak: is er een taak voor de overheid en is regelgeving 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

Het doel van de beide richtlijnen (en de implementatie ervan) is om de continuïteit van de levering van essentiële diensten zo veel mogelijk te borgen. Daartoe nemen zij onder meer de verschillen tussen Lidstaten op het gebied van fysieke en digitale veiligheids- en beveiligingseisen weg. Deze maatregelen worden genomen in de context van toegenomen dreigingen voor de vitale infrastructuur respectievelijk de digitaal veilige samenleving. De toelichting maakt echter niet duidelijk in welke zin en in welke mate de bestaande wetgeving daarvoor tekort schiet.

1.1 Het college adviseert om het nut en noodzaak in de toelichtingen bij de voorstellen beter te onderbouwen door te verduidelijken waar en in welke mate de bestaande wetgeving tekort schiet op het punt van toegenomen dreigingen.

2. Minder belastende alternatieven

De richtlijnen stellen minimumeisen aan de organisaties die belangrijk, essentieel of kritiek zijn. Lidstaten kunnen zelf hogere eisen opleggen als zij dat noodzakelijk vinden. Volgens de toelichting bij de Cbw zal in de AMvB daar naar verwachting gebruik van worden gemaakt om een hoger cyberbeveiligingsniveau te waarborgen. De toelichting gaat niet in op de redenen hiervoor. Verder wordt de mogelijkheid genoemd dat op Europees of nationaal niveau in bepaalde sectoren verplichte certificeringen zullen worden opgelegd en dat via Ministeriële regelingen sectorale regels (kunnen) worden opgelegd. Deze sectorspecifieke regels kunnen bijvoorbeeld zien op de toepassing van bepaalde

NEN-normen. Ook kunnen de regels zien op (sectorale) normen van internationale, Europese of nationale standaardisatieorganisaties.

Het college constateert dat deze aanvullende vereisten (kunnen) leiden tot een nationale kop (goldplating), waarvan de onderbouwing extra aandacht verdient.

2.1 Het college adviseert om in de toelichting van de implementatiewetgeving te verduidelijken of, en zo ja, waar en waarom wordt gekozen voor zwaardere eisen dan de minimumeisen van de richtlijnen.

Het college constateert verder dat op andere punten wel aandacht is besteed aan een lastenluwe invulling van de verplichtingen. Zo is voor een deel van de entiteiten de omvang van een organisatie één van de criteria op basis waarvan bepaald wordt of het een essentiële organisatie of belangrijke organisatie betreft. Bij de zorgplichten kunnen organisaties zelf nagaan (op basis van een eigen normenkader) wat in hun geval de risico's te zijn en daar zelf passende maatregelen voor nemen. Het toezicht op "belangrijke organisaties" zal uitsluitend achteraf plaatsvinden. Het kan worden "geactiveerd" wanneer de bevoegde autoriteiten op de hoogte zijn gekomen van mogelijke inbreuken op de verplichtingen. Deze differentiatie moet zorgen voor een evenwicht tussen op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds. Verder is het uitgangspunt om de meldplicht op een lastenluwe manier in te richten. Er wordt naar gestreefd de dubbele meldplicht zo in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt. Tenslotte meldt de toelichting dat het NCSC een gebruiksvriendelijke registratie zal inrichten, zodat organisaties de informatie laagdrempelig kunnen aanleveren en beheren.

3. Werkbaarheid

Het college constateert dat veel verplichtingen nog door middel van een AMvB of ministeriële regeling zullen worden uitgewerkt. Volgens de toelichting wordt bij het opstellen van beveiligingseisen in de AMvB onder de Wwke aangesloten bij wat gangbaar en gewenst is in een sector. In de toelichting op de Cbw ontbreekt een soortgelijke passage, terwijl het ook daar voor de hand ligt om na te gaan of beoogde regels voor (met name kleine) bedrijven werkbaar zijn. Bovendien bevatten de richtlijnen en implementatiewetgeving veel subjectieve begrippen, die voor onduidelijkheid kunnen zorgen, ondanks een uitwerking in lagere wetgeving. Hierdoor ontstaat het risico dat de betrokken organisaties veel tijd moeten steken in het doorgronden van alle verplichtingen en mogelijk zelfs externe expertise daarvoor moeten inhuren.

3.1 Het college adviseert om een MKB-toets uit te laten voeren voor de lagere regelgeving waarmee de verplichtingen nader worden uitgewerkt.

3.2 Het college adviseert te waarborgen dat organisaties weten wat de verplichtingen precies inhouden en hoe die nageleefd moeten worden.

Verder wijst het college op de mogelijkheid om een jaar na invoering van de implementatiewetgeving en toelichtingen daarop te toetsen of deze voldoende werkbaar zijn. Hiervoor kan een invoeringstoets worden uitgevoerd.

3.3 Het college adviseert om een jaar na inwerkingtreding van de implementatiewetgeving een invoeringstoets uit te voeren.

4. Gevolgen regeldruk

De toelichtingen bij de wetsvoorstellen bevatten een gedeeltelijke inschatting van de regeldrukkosten. Zo wordt een schatting vermeld van ongeveer 8.100 organisaties, die onder de Cbw komen te vallen en 500 waar de Wwke betrekking op zal hebben. Er is echter geen indicatie van welk deel op dit moment al onder de Wbni c.q. de sectorale wetten op het terrein van vitale dienstverlening valt. Organisaties die al veel maatregelen hebben genomen, zullen minder regeldruk ervaren.

De toelichting vermeldt dat de regeldruk als gevolg van de zorgplicht in zowel de Cbw als de Wwke in beeld zal worden gebracht bij de daarvoor nog op te stellen AMvB's. De toelichting op de Cbw geeft aan dat in de Impact Assessment van de Europese Commissie geschat wordt dat nieuwe organisaties een toename van maximaal 22% aan ICT-beveiligingskosten benodigd hebben om aan de eisen te voldoen. Voor organisaties die al onder de huidige wetgeving vallen, is de schatting maximaal een toename van 12%. De toelichting op de Wwke bevat een dergelijke schatting niet. Het college merkt op dat de Rijksbrede methodiek voor het berekenen van regeldruk in dergelijke gevallen voorschrijft om een globale indicatie van de orde van grootte van de regeldruk te geven, zodat de wetgever deze kan meewegen in de besluitvorming. Een dergelijke indicatie kan worden verkregen met behulp van scenario's en bandbreedtes.

4.1 Het college adviseert om inzicht te geven in de orde van grootte van de regeldrukgevolgen van die zaken die nog bij AMvB worden geregeld.

De toelichtingen bij beide voorstellen geven inzicht in een deel van de regeldrukgevolgen. De regeldrukkosten van de meldplicht in de Cbw worden geschat op structureel € 450.000,-. De regeldrukkosten van de registratieplicht zijn eenmalig € 972.000,- en structureel € 30.000,-. De eenmalige kennisnamekosten van de Cbw worden geschat op € 960,- per organisatie. De toelichting vermenigvuldigt dit bedrag echter niet met het aantal betrokken organisaties (8.100),- zodat niet duidelijk wordt dat de totale eenmalige kennisnamekosten € 7.776.000,- bedragen.
Voor de Wwke bedragen de kosten van de meldingsplicht structureel € 7.500,- per jaar. De Wwke zal verder € 480.000,- tot eenmalige kennisnamekosten leiden.

Verder ontbreken enkele andere omvangrijke regeldrukcomponenten in de berekeningen. Zo kan de toezichthouder in het kader van de Wwke een organisatie verplichten om beveiligingsaudit uit te laten voeren door een onafhankelijke deskundige. Ook kan de toezichthouder de organisatie onderwerpen aan (steekproefsgewijze) inspecties en ad-hoc audits. De toezichthouder kan bovendien verzoeken om informatie, gegevens, do-

cumenten en bewijzen van uitvoering van het beveiligingsbeleid. De toezichthouder kan in het kader van de Cbw kan onder andere een beveiligingsscan of een beveiligingsaudit opleggen. Verder leiden de vrijwillige meldingen met als oogmerk om ondersteuning van het NCSC te krijgen tot regeldrukkosten die niet gekwantificeerd zijn.

4.2 Het college adviseert om de beschrijving en de berekening van de regeldrukgevolgen aan te vullen met de nog ontbrekende elementen, conform de Rijksbrede methodiek.

Dictum

Gezien het voorgaande is het dictum:

De wetsvoorstellen niet indienen, tenzij met de adviespunten rekening wordt gehouden.

Het college vertrouwt erop u hiermee voldoende te hebben geïnformeerd en verneemt graag van u op welke wijze u met onze adviespunten rekening houdt. Het college verzoekt u om een eventueel aangepast voorstel toe te sturen, opdat het kan beoordelen of een aanvullende zienswijze noodzakelijk is.

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris