Adviescollege toetsing regeldruk

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties
De heer F. Rijkaart
Postbus 20011
2500 EA DEN HAAG

**Onze referentie**
MvH/RvZ/ATR4336/2025-U199

**Uw referentie**

**Datum**
18 december 2025

**Onderwerp**
Cyberbeveiligingsregeling Sector Overheid

Geachte heer Rijkaart,

Op 26 november 2025 is het *Cyberbeveiligingsregeling (Cbr) Sector Overheid* aan het Adviescollege toetsing regeldruk (ATR) voor advies voorgelegd. De adviestermijn van ATR verloopt op De adviestermijn van ATR verloopt op 23 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 voor netwerk- en informatiesystemen, zoals het internet en het betalingsverkeer. De verplichtingen omvatten onder meer een zorgplicht en een meldplicht.

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

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 overheden. Deze regeling bevat geen directe regeldrukgevolgen, maar de indirecte gevolgen kunnen erg groot zijn. 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 een 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.

### Inhoud van het voorstel

De regeling bevat vier hoofdonderdelen:

a. Verplichte beveiligingsmaatregelen: Overheidsorganisaties moeten hun informatiebeveiliging inrichten conform ISO 27001 (ISMS-verplichting), ISO 27002 (toepassing of motivering van beveiligingsmaatregelen) en BIO2, die deze normen vertaalt naar de overheidscontext en aanvullende eisen stelt voor onder andere audit en risicobeoordeling. Organisaties moeten kunnen aantonen dat maatregelen ook in de praktijk werken, wat structurele capaciteit, documentatie en interne controles vereist.

b. Identificatie van essentiële diensten: Overheden moeten via een impactanalyse vaststellen welke diensten essentieel zijn als incidenten kunnen leiden tot ernstige politieke, maatschappelijke, veiligheids- of financiële schade. Voor het Rijk geldt impactniveau 3; voor decentrale overheden impactniveau hoog. Deze classificatie is nieuw en bepaalt welke diensten onder zwaardere meldplichten vallen.

c. Meldplicht significante incidenten: Incidenten op essentiële diensten worden altijd als significant aangemerkt en moeten worden gemeld aan het CSIRT en/of de toezichthouder. Voor niet-essentiële diensten gelden afzonderlijke drempels (onder andere langdurige uitval, ernstige schade, lekken van gerubriceerde informatie). De verplichting om álle incidenten op essentiële diensten te melden kan tot een groot aantal meldingen leiden.

d. Ketenverantwoordelijkheid: Overheden moeten risico’s in de keten beoordelen en beheersen, wat ertoe leidt dat leveranciers (zoals cloud- en ICT-dienstverleners) meer informatie, documentatie en audits moeten aanleveren. Daardoor raken de verplichtingen ook private partijen, hoewel de regeling formeel alleen overheden adresseert.

## 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 noodzakelijk voor de implementatie van Europese verplichtingen en voor het uniformeren van beveiligingsmaatregelen binnen de overheid. Nut en noodzaak zijn in beginsel helder en worden door het stafbureau onderschreven.

Het college ziet daarom geen aanleiding voor opmerkingen onder deze toetsvraag.

### *2. Minder belastende alternatieven*

Doordat overheidsorganisaties verplicht worden om beveiligingsrisico's in hun keten te analyseren, ontstaat een nieuwe structurele informatie- en verificatieverplichting richting leveranciers. Die leveranciers moeten beveiligingsdocumentatie aanleveren (ISO-certificaten, pentestresultaten, auditrapportages). Verder moeten ze hun bedrijfsprocessen aanpassen (logging, monitoring, incidentregistratie). En in sommige gevallen moeten ze aanvullende beveiligingsmaatregelen implementeren.

De toelichting maakt niet inzichtelijk welke alternatieven zijn overwogen bij de vormgeving van de verplichtingen en procedures. Het gaat daarbij onder meer over de vraag of lichtere of gefaseerde maatregelen mogelijk zijn voor kleinere overheidsorganisaties, of differentiatie mogelijk is tussen categorieën diensten of risico's, of bestaande structuren voor informatie-uitwisseling (zoals sectorale CERTs) al voldoende mogelijkheden boden en daarom beter hadden kunnen worden ingezet, en of een minder gedetailleerde of uniformere verplichting werkbaar zou zijn geweest.

## Nationale koppen

Niet duidelijk is welke onderdelen van de regeling dwingend voortvloeien uit NIS2 en welke keuzes nationaal zijn gemaakt. Het college kan daardoor niet beoordelen of de regeling verder gaat dan het Europese minimum. Gezien de potentiële gevolgen voor ketenafhankelijkheden en indirecte lasten is dit inzicht noodzakelijk.

De toelichting maakt nu niet duidelijk welke informatie overheden precies mogen of zullen uitvragen. Ook is niet duidelijk of hierbij een gestandaardiseerd format wordt gehanteerd, of en zo ja welke alternatieven zijn onderzocht (bijvoorbeeld aansluiten op bestaande certificeringsschema's) en of varianten met lagere lasten zijn overwogen. Zonder inzicht hierin is niet vast te stellen of de regeling de minst belastende variant bevat.

**2.1 Het college adviseert toe te lichten welke onderdelen rechtstreeks uit Europese verplichtingen komen en welke nationaal zijn ingevuld. Daarbij dient gemotiveerd te worden dat geen sprake is van nationale koppen.**

**2.2 Het college adviseert de afweging van beleidsalternatieven inzichtelijk te maken, waaronder varianten met minder gedetailleerde verplichtingen, differentiatie naar risico of omvang en benutting van bestaande structuren.**

### *3. Werkbaarheid*

De werkbaarheid voor ketenleveranciers hangt sterk af van de bereidheid en mogelijkheden van leveranciers om aan de informatie-uitvraag te voldoen. De regeling veronderstelt dat leveranciers structureel beveiligingsrapportages, audits en technische gegevens beschikbaar stellen. De toelichting maakt niet inzichtelijk of dit realistisch is voor alle typen leveranciers (MKB, SaaS-partijen, cloudproviders, niche-leveranciers). Evenmin is duidelijk of leveranciers geconfronteerd worden met versnipperde eisen van verschillende overheidsorganisaties, of centrale guidance beschikbaar komt, en of de verplichtingen proportioneel zijn voor leveranciers van niet-kritieke systemen. Zonder deze informatie is onzeker of de ketenleveranciers aan hun (indirecte) wettelijke verplichtingen daadwerkelijk kunnen voldoen.

**3.1 Het college adviseert te verduidelijken hoe de informatie-uitvraag aan leveranciers wordt ingericht, hoe uniformiteit wordt geborgd en welke organisatorische en technische lasten hierbij voor leveranciers wordt verwacht.**

### *4. Gevolgen regeldruk*

De regeling legt formeel geen verplichtingen op aan burgers en bedrijven, maar leidt indirect tot regeldruk voor bedrijven die als ketenleverancier aan overheidsorganisaties verbonden zijn. Deze regeldruk is mogelijk substantieel. De indirecte lasten bestaan onder meer uit de kosten die voortvloeien uit extra documentatie- en rapportageverplichtingen, audits en certificeringen, aanpassingen in technische beveiligingsmaatregelen, periodieke updates en monitoring, investeringen in compliance-capaciteit.

Leveranciers bedienen vaak meerdere overheidsorganisaties. Zij kunnen daardoor worden geconfronteerd met verschillende eisen, formats en termijnen. Dit kan de lasten cumulatief vergroten. De toelichting bij het voorstel biedt geen inzicht in de aard van de informatie-uitvraag, de verwachte kosten voor leveranciers, de proportionaliteit van deze lasten proportioneel, en hoe onnodige variatie tussen overheden wordt voorkomen.

**4.1 Het college adviseert de regeldruk in kaart te brengen volgens de Rijksbrede methodiek.**

## Dictum

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

**Vaststellen nadat met de adviespunten rekening is gehouden.**

In de verwachting u hiermee voldoende te hebben geïnformeerd,

Hoogachtend,

*w.g.*

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris