

Tweede Kamer der Staten Generaal

t.a.v. de Commissie Digitale Zaken

Betreft: Behandeling van de Cyberbeveiligingswet 23 maart 2026
Plaats: Breukelen
Datum: 10 maart 2026

NLdigital inbreng wetgevingsoverleg Cyberbeveiligingswet

De Cyberbeveiligingswet zal ingrijpen op 8.000-10.000 organisaties in Nederland via een ingewikkeld bouwwerk van de Europese richtlijn 2022/2555 & de uitvoeringsverordening 2024/2690, de Nederlandse Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en meerdere ministeriële regelingen. Deze heeft daardoor ook een zeer grote variatie in impact op deze organisaties. Door dit complexe bouwwerk beogen de eisen proportioneel en risico-gebaseerd te zijn. De keerzijde is dat er veel gevraagd wordt van organisaties om te begrijpen welke delen van welke wet- en regelgeving op hen van toepassing zijn.

NLdigital steunt de NIS2 richtlijn van harte en heeft hier in iedere stap van de wetsontwikkeling ook constructief-kritische bijdragen aan geleverd via openbare consultaties¹. Nu de wet voorligt in het parlement constateren we dat sommige zorgen (deels) weggenomen zijn, maar zijn er ook nieuwe zorgen ontstaan door met name de vergaande interventiebevoegdheid.

Deze wetgeving vraagt om grote zorgvuldigheid bij uitwerking en invoering. Voor uw wetgevingsoverleg op 23 maart 2026 leidt dit bij de digitale sector tot de volgende aandachtspunten.

1. Maak de ministeriële interventiebevoegdheid juridisch solide door haar in de wet te verankeren

Via het Cyberbeveiligingsbesluit (de AMvB) wordt de zorgplicht opgerekt tot een vergaande interventiebevoegdheid voor ministers. Een zorgplicht is de wettelijke verplichting om er alles aan te doen wat redelijkerwijs van de organisatie zelf verwacht mag worden om schade te voorkomen. Dat maakt het wezenlijk anders dan een interventiebevoegdheid door ministers. Deze oprekking zet een gevaarlijk precedent voor het sleutelen aan wetten door ministers per lagere regelgeving. Een AMvB zou geen nieuwe zelfstandige bevoegdheden moeten scheppen zonder expliciete wettelijke grondslag². Relevant daarbij is dat deze interventiebevoegdheid (artikel 18 van het Cyberbeveiligingsbesluit) pas in een laat stadium is toegevoegd, nadat twee consultatieprocedures en twee adviezen van de Raad van State al waren doorlopen.

¹ Op 2 juli 2024 [op de conceptwet](#), op 28 oktober 2024 met onze EU-koepel Digital Europe [op de uitvoeringshandelingen](#), op 31 maart 2025 [op het Cyberbeveiligingsbesluit](#) en op 1 september 2025 op [de last-minute interventiebevoegdheid toevoeging](#) aan het Cbb.

² Dit principe vindt steun in jurisprudentie: het Fluoride-arrest (HR 1973) bevestigde dat ingrijpende overheidsbevoegdheden met grote maatschappelijke impact een expliciete wettelijke grondslag vereisen en niet via lagere regelgeving kunnen worden gecreëerd.



NLdigital is niet gekant tegen een interventiebevoegdheid bij nationale veiligheidsrisico's, maar die bevoegdheid hoort in de wet zelf opgenomen te zijn. Met objectieve criteria, rechtswaarborgen en alleen als het niet anders kan (*ultimum remedium*). Zeker niet als oprekking van het zorgplichtbegrip via een zin in de Memorie van Toelichting, en alleen te wijzigen via zorgvuldige democratische besluitvorming.

Oproep aan de Tweede Kamer

- **Amendeer de Cyberbeveiligingswet om de interventiebevoegdheid op wetsniveau te verankeren**, met expliciete verankering van het ultimium-remedium-principe, duidelijke beoordelingscriteria, hoor en wederhoor, beroepsmogelijkheden en een nadeelcompensatieregeling. Dit brengt logischerwijs met zich mee dat het Cyberbeveiligingsbesluit op dit punt teruggebracht wordt tot wat in een AMvB thuishoort: de nadere uitwerking en detaillering van bevoegdheden die hun grondslag in de wet zelf hebben, niet het scheppen van zelfstandige nieuwe bevoegdheden.
- **Alternatief: Amendeer dat het Cyberbeveiligingsbesluit uitsluitend met een verplichte voorhangprocedure kan worden gewijzigd**, zodat de Kamer democratische controle behoudt (zoals we eerder hebben opgeroepen met VNO-NCW, MKB-Nederland, FME en vele anderen³).

2. Houd het web van meldplichten beheersbaar

De meldplicht in de Cyberbeveiligingswet raakt de digitale sector dubbel: als NIS2-entiteit én als IT-leverancier die klanten die onder de NIS2 vallen moet ondersteunen bij hun meldverplichtingen. Daarnaast is het niet de enige meldplicht die van toepassing is tijdens cyberincidenten. Bij een grootschalig incident betekent dit een veelvoud aan parallelle meldingen onder de Cbw (voor zowel de eigen organisatie als ondersteunen van de klanten), AVG, DORA, Wwke en CRA, bij meerdere toezichthouders en CSIRTs tegelijk. Terwijl dit de fase is waarin de volledige aandacht zou moeten uitgaan naar het afweren en beheersen van de aanval.

NLdigital verwelkomt de richting van de EU-Omnibus-simplificatievoorstellen op dit punt en ziet dit als de meest directe route om de stapeling van meldverplichtingen structureel aan te pakken. De Nederlandse overheid toonde zich echter terughoudend in eerste instantie. Wij roepen de Kamer op het kabinet hierop bij te sturen: pleit actief voor maximale harmonisatie en vereenvoudiging van meldverplichtingen, met name gedurende de initiële 72 uur waarin meerdere meldingen onder meerdere wetten verplicht worden.

Oproep aan de Tweede Kamer

- Verzoek het kabinet constructief mee te werken aan **één centraal meldloket voor alle wettelijke meldplichten bij incidenten** (Cbw, AVG, DORA, Wwke, CRA), met één gestandaardiseerd meldformulier. Dit met name voor de meldplichten gedurende de initiële fase (24 en 72 uur).
- Verzoek het kabinet actief in te zetten op **Europese harmonisatie van meldverplichtingen** door constructief mee te werken aan de Omnibus-voorstellen op dit punt.
- Verzoek het kabinet te bevorderen dat **het Cyberweerbaarheidsnetwerk gepositioneerd wordt om bij grootschalige incidenten snel als coördinatiepunt te fungeren** tussen getroffen organisaties, potentiële hulpverleners, toezichthouders en het NCSC.

³ [Verzoek tot voorhangprocedure voor de AMvB's onder de wetsvoorstellen Cbw en Wwke, brief aan de VC Digitale Zaken en Justitie en Veiligheid van de Tweede Kamer](#)

3. Risico-gebaseerde aanpak vraagt om advies & ondersteuning van toezichthouders

NLdigital steunt de risico-gebaseerde aanpak voor cybersecuritywetgeving: dit geldt in de sector als de enige juiste benadering. Dit heeft echter een inherente keerzijde: de uitwerking hiervan is voor iedere organisatie verschillend. Dat maakt het proportioneel, maar kan ook onzekerheid creëren. De toezichthouder en het NCSC hebben tot nu toe een terughoudende rol aangenomen in het duiden van standaarden en certificeringen. Wij roepen hen op dat nadrukkelijker te doen.

Het is inmiddels helder dat ISO27001 een stevige basis biedt voor grotere organisaties, en varianten daarop als de BIO2 en NEN7510 spelen nadrukkelijk een rol voor de sectoren overheid en zorg. Ook zien we dat de CYRA-methode⁴ van het CCV een sterk groeipad biedt voor organisaties voor wie een volledig ISO-traject te zwaar is. De CYRA-methode biedt deze bovendien ook aan in sectorale varianten. Advies en ondersteuning (proactief gecommuniceerd) in het doolhof van mogelijke raamwerken en standaarden maakt de risico-gebaseerde aanpak werkbaar in de praktijk, juist voor het MKB. Kijk bijvoorbeeld naar de Belgische implementatie die hun eigen CyberFundamentals framework⁵ of een ISO27001 met de juiste scope hanteren om de toezicht-last te verlichten.

Oproep aan de Tweede Kamer

- Verzoek het kabinet het NCSC en de sectorale toezichthouders te verzoeken proactief te communiceren welke standaarden, certificeringen en methoden van afdoende kwaliteit zijn om organisaties te helpen bij het invullen van de zorgplicht, uitgesplitst naar sector, organisatietype en -omvang.
- Verzoek het kabinet te bevorderen dat toezicht in de eerste periode na inwerkingtreding gericht is op advies en het stimuleren van naleving, niet op repressieve handhaving. Uiteraard met uitzondering van de organisaties die aantoonbaar niets hebben ondernomen.

4. AMvB en ministeriële regelingen: doolhof moet beheersbaar zijn

De Cyberbeveiligingswet delegeert een groot aantal cruciale details naar AMvB's en ministeriële regelingen. Dit was al een vroege zorg van NLdigital. De praktijk is minder slecht dan gevreesd: de koppeling van sectorale regelingen aan de BIO2 (overheid) en de NEN7510 (zorg) wijst in de goede richting. Toch blijft de situatie voor IT-leveranciers die aan meerdere sectoren leveren complex: zij moeten in meerdere sectorale regimes aantonen compliant te zijn voor in essentie vergelijkbare technische maatregelen.

De wet en de lagere regelgeving moeten waarborgen dat sectorale regelingen hoogstens in zwaarte afwijken van de Europese Uitvoeringsverordening 2024/2690, maar niet in richting of systematiek. Dit moet ook een prioriteit blijven bij toekomstige aanscherpingen.

Oproep aan de Tweede Kamer

- Vraag het kabinet te bevestigen dat bij de uitwerking en toekomstige aanpassing van ministeriële regelingen het uitgangspunt is dat deze aansluiten bij de terminologie en systematiek van Uitvoeringsverordening 2024/2690, en dat afwijkingen uitdrukkelijk worden toegelicht.

⁴ [Online zelfbeoordelingsinstrument voor bedrijven CYRA - Het CCV](#)

⁵ [CyberFundamentals Framework | CyFun](#)

5. Harmonisatie binnen Europa: Nederland, neem het voortouw

Een gelijk speelveld binnen de EU is een fundamentele voorwaarde voor het functioneren van de digitale interne markt. Nationale koppen op Europese cybersecurityregelgeving benadelen Nederlandse en in Nederland opererende bedrijven ten opzichte van hun EU-concurrenten en ondermijnen het vestigingsklimaat. Harmonisatie binnen Nederland is beter verlopen dan vooraf gevreesd; Europese harmonisatie blijft echter een zorgpunt.

Oproep aan de Tweede Kamer

- Verzoek het kabinet actief in Europees verband te pleiten voor maximale harmonisatie van NIS2- implementatie tussen lidstaten.