Docnr1

From: 5.1.2.e 5.1.2.e <5.1.2.e @gmail.com>
Date: Sunday, July 5, 2026, 12:16 AM
To: postbus@eerstekamer.nl
cie.diza@tweedekamer.nl
cie.jv@tweedekamer.nl
boris.dittrich@eerstekamer.nl
5.1.2.e @eerstekamer.nl
b.kathmann@tweedekamer.nl
gala.veldhoen@eerstekamer.nl
tekke.panman@eerstekamer.nl
5.1.2.e @eerstekamer.nl
b.eerdmans@tweedekamer.nl
r.dekker@tweedekamer.nl
Subject: Inbreng Cyberbeveiligingswet (wetsvoorstel 36764) – Verzoek om versterking van governance en onafhankelijkheid via amendement of nadere uitwerking

---

Geachte leden van de Vaste commissie voor Justitie en Veiligheid en Digitale Zaken van de Tweede Kamer en de Eerste Kamer,

In verband met de plenaire behandeling van de Cyberbeveiligingswet (Cbw) in de Eerste Kamer op 6 en 7 juli 2026, wil ik u graag mijn zienswijze voorleggen.

Aanleiding De Cyberbeveiligingswet is een belangrijke stap in de versterking van de digitale weerbaarheid van Nederland. Desondanks zie ik drie structurele tekortkomingen die de effectiviteit van de wet kunnen beperken:

1. **Governance blijft onderbelicht.** Artikel 24 vereist goedkeuring van de risicobeheersingsmaatregelen door het bestuur, maar de wet bevat geen concrete eisen aan de governancestructuur zelf (rollen, verantwoordelijkheden, rapportagelijnen, escalatie en periodieke evaluatie). Dit leidt tot onvoldoende handelingsperspectief voor organisaties.
2. **Onafhankelijkheid van de CISO / security-functie is niet geborgd.** Anders dan de Functionaris Gegevensbescherming (FG) onder de AVG kent de Cbw geen wettelijke waarborgen voor een onafhankelijke security-functionaris met directe toegang tot het hoogste bestuursorgaan en bescherming tegen benadeling. Dit kan leiden tot belangenconflicten en onvoldoende escalatie van risico's.
3. **Onvoldoende verbinding met bestaande best practices.** De open norm van "passende en evenredige maatregelen" (artikel 21) verwijst niet expliciet naar erkende kaders. Dit vermindert de rechtszekerheid en maakt het lastiger om aantoonbaar compliant te zijn.

Oplossingsrichting: amendement of nadere uitwerking Ik verzoek u om in de behandeling aandacht te vragen voor de volgende concrete verbeteringen:

Amendement 1 – Versterking van governance Voeg aan artikel 24 (of een nieuw artikel) toe dat essentiële en belangrijke entiteiten verplicht zijn een governancestructuur voor cyberbeveiliging vast te stellen en te onderhouden. Hierin dienen ten minste te worden opgenomen: duidelijke rollen en verantwoordelijkheden, rapportagelijnen naar het bestuur, en een periodieke evaluatie door of namens het bestuur.

Amendement 2 – Functionaris Informatieveiligheid Voeg een bepaling toe die entiteiten verplicht een Functionaris Informatieveiligheid (of equivalente onafhankelijke security-functionaris) aan te stellen met de volgende waarborgen:

- directe rapportage aan het hoogste bestuursorgaan;
- bescherming tegen benadeling wegens de uitoefening van de functie;
- verplichting tot tijdige escalatie bij ernstige risico's of niet-naleving.

Dit sluit aan bij de systematiek van de AVG en versterkt de bestuurlijke verantwoordelijkheid die de wet beoogt.

Amendement 3 – Expliciete verwijzing naar erkende kaders Voeg aan artikel 21 toe dat bij de invulling van passende en evenredige maatregelen entiteiten zich kunnen baseren op of kunnen laten toetsen aan erkende internationale en nationale kaders, waaronder in ieder geval het NIST Cybersecurity Framework, ISO/IEC 27001, CIS Controls, COBIT en COSO ERM. Dit vergroot de rechtszekerheid en consistentie van de zorgplicht.

Indien amendementen in dit stadium niet meer haalbaar zijn, verzoek ik u de regering te vragen deze punten alsnog op te nemen in de memorie van toelichting, in nadere regelgeving (AMvB of ministeriële regeling) of in de NCSC-guidance, en om na twee jaar een evaluatie te laten uitvoeren op de governance-aspecten.

Ik dank u voor uw aandacht en sta uiteraard open voor een nadere toelichting.

Met vriendelijke groet,

5.1.2.e Informatiebeveiliging Prive tel: 5.1.2.e