Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2025-2026

36 764 Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet)

E **NOTA NAAR AANLEIDING VAN HET TWEEDE VERSLAG**

Ontvangen 29 juni 2026

Hierbij bied ik u de nota naar aanleiding van het tweede verslag op het voorstel van wet ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333) (Cyberbeveiligingswet, *Kamerstukken* 36764) aan.

De vaste commissies voor Digitalisering en Justitie & Veiligheid hebben een tweede verslag uitgebracht op het wetsvoorstel voor de Cyberbeveiligingswet (hierna: Cbw). Dit wetsvoorstel strekt tot de uitvoering van de zogeheten NIS2-richtlijn.[1] Het tweede verslag is hieronder opgenomen in cursieve tekst en de beantwoording van de vragen uit het tweede verslag in gewone typografie.

1. Inleiding

De leden van de fractie van de PVV hebben met interesse kennisgenomen van de nota naar aanleiding van het verslag over de Cyberbeveiligingswet.[2] Deze leden hebben nog een vraag open staan welke in de nota naar aanleiding van verslag onbeantwoord is gebleven. De leden van de fracties van fractie-Walenkamp en fractie-Van Gasteren sluiten zich bij de vraag van de leden van de fractie van de PVV aan.

Bij het opstellen van de nota naar aanleiding van het (eerste) verslag op de Cbw is, te midden van de beantwoording van alle andere vragen, helaas over het hoofd gezien dat het antwoord op een vraag van de leden van de PVV-fractie niet is opgenomen in de nota. De regering betreurt het ontbreken van dat antwoord. Hieronder volgt het antwoord en de regering hoopt de vraag genoegzaam te hebben beantwoord.

2. Uitvoerbaarheid

[1] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333).
[2] *Kamerstukken I 2025/26, 36.764, C.*

Een veelgehoorde zorg bij de Cyberbeveiligingswet ziet toe op de regeldruk. De leden van de PVV-fractie vinden dit een terechte zorg en vrezen dat er vanuit de EU bij de totstandkoming van de Cyberbeveiligingswet onvoldoende aandacht is geweest voor de reeds aanwezige controlemechanieken en protocollen die in het kader van de ketenafhankelijkheid al sinds jaar en dag toezien op, onder meer, cyberveiligheid. Te denken valt aan de Corporate Sustainability Reporting Directive (CSRD) die bedrijven verplicht om duidelijk te laten zien wat de impact is van hun bedrijfsactiviteiten, waarbij het gaat om effecten op mens, milieu en klimaat over de hele waardeketen en die moet voldoen aan de European Sustainability Reporting Standards (ESRS). Vele bedrijven zijn aangesloten bij platforms en beoordelingsbureaus die gespecialiseerd zijn in zogenaamde Environmental, Social en Governance (ESG)-ratings en het controleren van duurzaamheid in wereldwijde toeleveringsketens. De ketenpartners van deze bedrijven worden overstelpt met verplichte questionnaires die onderbouwd moeten worden met bewijslast, zoals certificaten, rapportages, diploma's, verklaringen, et cetera. Voor ieder platform en beoordelingsbureau dient dit nét anders te worden onderbouwd. Kleinere ketenpartners lopen steeds verder uit de pas vanwege onvoldoende beschikbare capaciteit.

Deze leden vragen nogmaals om een inventarisatie van de regering van de beschikbare platforms en beoordelingsbureaus en hun aangeboden pakketten die reeds voldoen aan de Cyberbeveiligingswet. Tevens willen deze leden van de regering weten wat zij concreet gaat doen om dergelijke repetitieve handelingen terug te dringen en te voorkomen dat de uitvoering van de Cyberbeveiligingswet er ook een wordt?

De regering begrijpt de zorg van de leden van de PVV-fractie over de stapeling van verantwoordingsvereisten voor organisaties in toeleveringsketens. Zij merkt echter op dat de vraag berust op een misverstand over de aard van de Cbw en de door de leden genoemde ESG-instrumenten. De *Corporate Sustainability Reporting Directive* (CSRD) en de bijbehorende *European Sustainability Reporting Standards* (ESRS) zijn rapportagestandaarden gericht op niet-financiële informatieverstrekking over duurzaamheid, waaronder sociale impact en milieu-impact. De Cbw implementeert de NIS2-richtlijn en richt zich op geheel andere verplichtingen, waaronder de verplichting tot het treffen van technische, operationele en organisatorische maatregelen om risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Het gaat dus om instrumenten met een fundamenteel verschillende doelstelling, reikwijdte en handhavingsstructuur.

ESG-ratingplatforms en -beoordelingsbureaus toetsen niet aan de verplichtingen van de Cbw. Zij hanteren eigen, private methodologieën gericht op duurzaamheidsprestaties en *supply chain governance*. Een inventarisatie van zulke platforms in relatie tot de Cbw is dan ook niet zinvol. Voor zover er voor organisaties in toeleveringsketens sprake is van overlapping — bijvoorbeeld omdat sommige ESG-vragenlijsten ook vragen bevatten over informatiebeveiligingsbeleid — erkent de regering dat dit organisaties voor dubbel werk kan stellen. Dit is echter een gevolg van private marktpraktijken, niet van de Cbw zelf.

De Cbw zorgt voor nieuwe wet- en regelgeving met gevolgen voor de bedrijven en organisaties die onder het toepassingsbereik daarvan vallen, en als gevolg daarvan mogelijk ook voor organisaties in de toeleveringsketen van die entiteiten. Deze wet is belangrijk, omdat het zorgt voor het vergroten van de digitale weerbaarheid van bedrijven en organisaties in Nederland.

Bij de zorgplicht uit de Cbw is gekozen voor een risicogebaseerde aanpak. Dit houdt in dat essentiële entiteiten en belangrijke entiteiten als bedoeld in de Cbw de ruimte hebben om op basis van een door hen zelf uit te voeren risicoanalyse, een eigen invulling te geven aan de in het kader

van die zorgplicht verplicht te nemen maatregelen. Daarmee kan de exacte invulling van de zorgplichtmaatregelen dus per entiteit verschillen. Het is aan de toezichthouders om voor elke entiteit te beoordelen of – mede gelet op de specifiek door die entiteit uitgevoerde risicoanalyse – in voldoende mate invulling wordt gegeven aan de zorgplicht.

Mede vanwege de geopolitieke situatie is het nemen van maatregelen om de weerbaarheid van Nederland en Europa te verhogen, noodzakelijk.
De regering tracht door middel van heldere toelichting, handreiking en communicatie de implementatie van de Cbw, waaronder de daarin opgenomen zorgplicht, zo eenvoudig mogelijk te maken. Daar is vanuit het bedrijfsleven ook behoefte aan. Bij de beoordeling welke specifieke maatregelen in het kader van de zorgplicht uit de Cbw genomen moeten worden, kunnen entiteiten gebruik maken van bestaande normenkaders, zoals ISO27001. Vanuit de rijksoverheid zijn voorts diverse tools en kennisproducten opgesteld die kunnen helpen bij het voldoen aan de zorgplicht uit de Cbw. Hieronder volgt een overzicht daarvan:

- Op de website van het Nationaal Cyber Security Centrum zijn meerdere infosheets te vinden over de zorgplicht uit de Cbw. Hierin wordt stap voor stap uitgelegd wat een entiteit kan doen om invulling te geven aan die verplichting. Ook worden er met enige regelmaat Q&A's hierover op de website van het Nationaal Cyber Security Centrum geplaatst.
- De Rijksinspectie Digitale Infrastructuur heeft een quickscan ontwikkeld waarmee entiteiten aan de hand van 40 vragen kunnen beoordelen hoe het met hun cyberbeveiliging ervoor staat.[3]
- De Auditdienst Rijk (ADR) en NOREA, de beroepsorganisatie van IT-auditors in Nederland, hebben in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een *NIS2 Control Framework* ontwikkeld. Dit is bedoeld als praktisch hulpmiddel voor organisaties en IT-auditors om inzicht te krijgen in onder andere hun aanpak voor het voldoen aan de zorgplicht uit de Cbw.

Op grond van artikel 21, derde lid, onderdeel d, Cbw moeten essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht ook maatregelen met betrekking tot de beveiliging van hun toeleveringsketen nemen. Ter uitwerking hiervan is in artikel 10 van het concept van het Cyberbeveiligingsbesluit opgenomen dat deze entiteiten beleid hierover moeten vaststellen en toepassen. Ook moeten zij toetsen of hun rechtstreekse leveranciers en rechtstreekse dienstverleners voldoen aan de beveiligingseisen die de entiteiten op basis van de door hen te verrichten risicoanalyse hebben bepaald. Daarbij is niet voorgeschreven op welke wijze entiteiten die toets moeten verrichten en is dus niet als vereiste gesteld dat partijen in de toeleveringsketen bijvoorbeeld specifieke certificaten, rapportages, diploma's of verklaringen dienen te overleggen. Op de website van het Nationaal Cyber Security Centrum is wel informatie te vinden over de wijze waarop essentiële entiteiten en belangrijke entiteiten in de zin van de Cbw de beveiliging van partijen in hun toeleveringsketen kunnen toetsen. Blijkens die informatie kunnen partijen in de toeleveringsketen hun digitale weerbaarheid bijvoorbeeld aantonen door te voldoen aan bepaalde normen of standaarden, zoals ISO27001 en SOC (*Service Organization Control*) 2. Deze beschikbare informatie is voor partijen in de toeleveringsketen een hulpmiddel waarmee de regeldruk ook voor partijen in de toeleveringsketen, als het gaat om de in artikel 10 Cyberbeveiligingsbesluit bedoelde toets op hun beveiliging, wordt beperkt.

Bij het uitwerken van de Cbw binnen de kaders van de NIS2-richtlijn was één van de uitgangspunten een zo laag mogelijke regeldruk voor bedrijven. Dit is ook binnen Europese verbanden een leidend

[3] Deze quickscan is te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/.

principe. Ook met betrekking tot de toeleveringsketen heeft ook de Europese Commissie aandacht voor de regeldruk die de NIS2-richtlijn in alle lidstaten oplevert. In het recent gepubliceerde voorstel voor de simplificatie van de NIS2-richtlijn wordt dit als een belangrijk punt meegenomen. Meer in het bijzonder wordt hierbij verwezen naar het daarin opgenomen voorstel om *guidelines* te ontwikkelen met aanbevelingen over een passend detailniveau en formats over het door entiteiten met het oog op hun zorgplicht opvragen van informatie bij partijen in de toeleveringsketen.

Met deze voorgestelde *guidelines* beoogt de Europese Commissie de lasten voor de leveranciers en dienstverleners te verlichten en een consistente en efficiënte aanpak voor de beveiliging van de toeleveringsketen te bevorderen. Nederland heeft dit voorstel van de Europese Commissie om *guidelines* te ontwikkelen positief beoordeeld in haar BNC-fiche (Beoordeling Nieuwe Commissievoorstellen), omdat hiermee de lasten voor die leveranciers en dienstverleners worden verlicht en hiermee wordt gezorgd voor een consistente, proportionele en efficiënte beoordeling van de beveiliging van de toeleveringsketen.[4] Ook wordt hiermee beoogd zo veel mogelijk te voorkomen dat de toepasselijkheid van de zorgplicht op entiteiten voor partijen in hun toeleveringsketen onnodige lasten oplevert bij de uitvraag van die entiteiten.

De Minister van Justitie en Veiligheid,

D.M. van Weel

[4] *Kamerstukken II* 2025/26, 22112, nr. 4284.