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)

B **VERSLAG VAN DE VASTE COMMISSIE VOOR DIGITALISERING[1] EN VOOR JUSTITIE EN VEILIGHEID[2]**
Vastgesteld 2 juni 2026

Het wetsvoorstel heeft de leden de fractie van **GroenLinks-PvdA**, mede namens de leden van de fractie van **PvdD,** en de leden van de fracties van de **VVD**, **D66**, **CDA**, **PVV**, **FVD**, **JA21**, **Volt** aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de **CDA**-fractie hebben met belangstelling kennisgenomen van de Cyberbeveiligingswet. Deze leden onderschrijven het belang van een hoog niveau van cyberweerbaarheid, maar hebben nog enkele vragen.

Deze leden constateren dat voor de NIS2-richtlijn de omzettermijn 17 oktober 2024 is overschreden en ten aanzien van deze richtlijn inmiddels een inbreukprocedure is gestart door de Europese Commissie. Deze leden onderschrijven het belang van tijdige omzetting van Europese richtlijnen in nationale regelgeving en vragen de regering te reflecteren op het niet halen van de omzettermijnen en vragen de regering om dit nader toe te lichten.

Kan de regering aan de leden van de fractie van de **VVD** bevestigen dat inwerkingtreding in het tweede kwartaal van 2026 haalbaar is, gezien de ingebrekestelling door de Europese Commissie en de benodigde amvb’s? Welke overgangstermijn hanteert de regering

[1] Samenstelling:
Baumgarten (JA21), Beukering (Fractie-Beukering), Fiers (GroenLinks-PvdA), Van Gasteren (Fractie-Van Gasteren), Goossen (BBB), Hartog (Volt), Van Hattem (PVV), Janssen (SP), Kanis (D66), Lievense (BBB), Van Meenen (D66), Musa (VVD), Nicolaï (PvdD), Van den Oetelaar (FVD), Panman (BBB) (ondervoorzitter), Petersen (VVD), Ramsodit (GroenLinks-PvdA), Recourt (GroenLinks-PvdA), Van Rooijen (50PLUS), Roovers (GroenLinks-PvdA), Van de Sanden (Fractie-Van de Sanden), Steenkamp (CDA), Talsma (ChristenUnie), Veldhoen (GroenLinks-PvdA) (voorzitter), Visseren-Hamakers (Fractie-Visseren-Hamakers), De Vries (SGP), Walenkamp (Fractie-Walenkamp)

[2] Samenstelling:
Beukering (Fractie-Beukering), Bezaan (PVV), Van Bijsterveld (JA21), Croll (D66), Dittrich (D66) (voorzitter), Doornhof (CDA), Van Gasteren (Fractie-Van Gasteren), Van der Goot (OPNL), Hartog (Volt), Janssen (SP), Kluit (GroenLinks-PvdA), Lievense (BBB), Van der Linden (VVD), Marquart Scholtz (BBB) (ondervoorzitter), Martens (GroenLinks-PvdA), Meijer (VVD), Nicolaï (PvdD), Van den Oetelaar (FVD), Ramsodit (GroenLinks-PvdA), Recourt (GroenLinks-PvdA), Van Rooijen (50PLUS), Van de Sanden (Fractie-Van de Sanden), Schalk (SGP), Talsma (ChristenUnie), Van Toorenburg (CDA), Veldhoen (GroenLinks-PvdA), Visseren-Hamakers (Fractie-Visseren-Hamakers), Vogels (VVD), Walenkamp (Fractie-Walenkamp)

voor entiteiten die nieuw onder de werkingssfeer vallen en hoe wordt voorkomen dat met name MKB-entiteiten en gemeenten overvraagd worden?

De leden van de **D66**-fractie hebben met belangstelling kennisgenomen van het voorstel voor de Cyberveiligheidswet. Deze leden onderstrepen het belang van het beschermen en bevorderen van onze fysieke en digitale veiligheid. Dit geldt al helemaal in deze roerige tijden. Wel hebben deze leden nog enkele vragen over de uitvoering van deze wet.

De leden van de **PVV**-fractie hebben met interesse kennisgenomen van de Cyberbeveiligingswet en de daarbij horende stukken. Deze leden hebben buiten het voorstel tevens kennisgenomen van het feit dat de Europese Commissie Nederland voor het Hof van Justitie van de EU daagt vanwege het uitblijven van de volledige implementatie van de CER-richtlijn. Nederland loopt ver voorop waar het gaat om digitale veiligheid en cybersecurity. Deelt de regering de zorg van deze leden dat gezwinde spoed afbreuk doet aan een kwalitatief adequate implementatie en daarmee de digitale weerbaarheid en cyberveiligheid van Nederland en is zij voornemens deze houding stellig te veroordelen? Deze leden lezen graag een gedegen onderbouwing van de beantwoording.

Kan de regering aan de leden van de fractie van **FVD** toelichten waarom ervoor wordt gekozen om onder tijdsdruk van een lopende inbreukprocedure wetgeving versneld door het parlement te loodsen? Welke gevolgen heeft dit voor de kwaliteit van de parlementaire controle? Acht de regering het wenselijk dat wetgeving op dit terrein primair wordt ingegeven door dreigende EU-sancties in plaats van inhoudelijke nationale afwegingen?

Kan de regering voor de leden van de fractie van **FVD** uiteenzetten waarom Nederland ervoor heeft gekozen om de NIS2-richtlijn grotendeels één-op-één te implementeren, in plaats van kritisch te bezien welke onderdelen daadwerkelijk noodzakelijk zijn binnen de Nederlandse context? In hoeverre is hierbij nog sprake van nationale beleidsruimte, en waarom is die ruimte wel of niet benut?

De leden van de **Volt**-fractie hebben met belangstelling kennis genomen van het voorliggende wetsvoorstel. Het geeft deze leden aanleiding tot het stellen van een aantal vragen.

2. Algemeen deel / hoofdlijnen wetsvoorstel / aanleiding

De leden van de fracties van **GroenLinks-PvdA** en **PvdD** hebben de volgende algemene vragen aan de regering.

1. Welke bewindspersoon of instantie heeft tijdens een sectoroverstijgende cybercrisis de uiteindelijke doorzettingsmacht wanneer meerdere toezichthouders of ministeries betrokken zijn?
2. Hoe wordt voorkomen dat organisaties onder tegenstrijdige instructies van verschillende toezichthouders komen te staan?
3. Kan de regering concreet uiteenzetten hoe de coördinatie tussen het Nationaal Cyber Security Centrum (NCSC), sectorale toezichthouders, veiligheidsregio’s en crisisstructuren in de praktijk verloopt tijdens een grootschalige verstoring?
4. Waarom is niet gekozen voor één centrale cyberautoriteit met bindende coördinatiebevoegdheden?
5. Kan de regering aangeven welke rol de Autoriteit Persoonsgegevens concreet krijgt bij toezicht op gegevensverwerking onder deze wet?
6. Hoe wordt voorkomen dat organisaties te maken krijgen met dubbele of overlappende rapportageverplichtingen onder de Cyberbeveiligswet en de Wet weerbaarheid kritieke entiteiten?

7. Hoe beoordeelt de regering de risico's van afhankelijkheid van Amerikaanse Cloud providers voor vitale infrastructuur? Welke gevolgen kan de Amerikaanse CLOUD Act in de optiek van de regering hebben voor Nederlandse vitale infrastructuur en overheidsdata? Deze leden lezen hier graag een analyse van.
8. Welke mogelijkheden heeft de Nederlandse regering om buitenlandse overnames van vitale digitale infrastructuur tegen te houden? Deze leden lezen hier graag een analyse van en tevens een reactie op de vraag of de regering voornemens is hier, al dan niet in Europees verband, regelgeving voor in het leven te roepen.
9. Welke geopolitieke criteria worden betrokken bij aanbestedingen van vitale digitale diensten?
10. Hoe worden klimaatrisico's zoals overstromingen, droogte en hitte structureel meegenomen in de beoordeling van kritieke infrastructuur?
11. Hoe beoordeelt de regering de weerbaarheid van vitale infrastructuur tegen gecombineerde klimaat- en cyberdreigingen?

Ten aanzien van de Cyberveiligheidswet lezen de leden van de **D66**-fractie dat voor de vitaalbeoordeling en de beslissing om een entiteit aan te wijzen de vakminister alleen verplicht is om te overleggen met de minister van J&V.[3] De leden van de D66-fractie vragen de regering of dit geen afbreuk doet aan het vermogen van de minister van J&V om coördinerend op te treden. Wat betekent dit voor mogelijke rechtsongelijkheid tussen verschillende sectoren, omdat verschillende vakministers verschillend zouden kunnen optreden?

De leden van de **CDA**-fractie constateren dat de regering kiest voor een stelsel waarin meerdere vakministers optreden als bevoegde autoriteit, terwijl de minister van J&V een coördinerende rol vervult. De Afdeling advisering van de Raad van State heeft gevraagd nader uiteen te zetten op welke wijze de minister van J&V daadwerkelijk "in positie" wordt gebracht als stelselverantwoordelijke.[4]

Voorts vragen deze leden waarom niet is gekozen voor een sterkere vorm van formele medebetrokkenheid van de minister van J&V bij sectorspecifieke regelgeving en besluiten die gevolgen kunnen hebben voor het functioneren van het integrale cybersecuritystelsel.

Deze leden lezen verder dat bestaande sectorspecifieke toezichthouders, waaronder zelfstandige bestuursorganen, naast de bevoegde autoriteiten een rol blijven vervullen bij toezicht op veiligheid en cyberweerbaarheid.

3. Rechtmatigheid /rechtsbeginselen /consistentie

De leden van de fracties van **GroenLinks-PvdA** en **PvdD** vragen de regering hoe zij garandeert dat deze wetgeving enerzijds voldoende flexibel blijft om cyberdreigingen het hoofd te bieden, maar anderzijds niet leidt tot structurele onzekerheid over de juridische verplichtingen van organisaties.

1. Waarom heeft de regering ervoor gekozen essentiële normen grotendeels via lagere regelgeving uit te werken in plaats van in de wet zelf?
2. Op basis van welke concrete criteria kan een organisatie vooraf vaststellen dat zij voldoet aan de (zorgplicht) verplichting om "passende en evenredige maatregelen" te nemen? Kan de regering hierbij betrekken dat er geen sprake is van eenduidige wettelijke minimumnormen maar van uitwerking in lagere regelgeving?
3. Hoe wordt voorkomen dat pas achteraf, bij toezicht of handhaving of via jurisprudentie, duidelijk wordt of een organisatie aan haar wettelijke verplichtingen heeft voldaan? Aan de hand van welke concrete criteria wordt

[3] *Kamerstukken II* 2025/26, 36.764, nr. 8, pp. 18-19.
[4] *Kamerstukken II* 2025/26, 36.764, nr. 4.

beoordeeld of een organisatie voldoet aan de zorgplicht? Is dit op voorhand voldoende kenbaar?
4. Kan de regering exact aangeven welke minimale beveiligingseisen in de wet zelf zijn vastgelegd, los van lagere regelgeving?
5. Hoe wordt parlementaire controle gegarandeerd op normen die feitelijk pas in lagere regelgeving en toezichtpraktijk worden ingevuld?
6. Hoe voorkomt de regering dat verschillende sectorale toezichthouders de open normen verschillend interpreteren en daarmee ongelijkheid in handhaving ontstaat?
7. Welke juridische grenzen zijn gesteld aan de normstellende rol van toezichthouders via richtsnoeren en handhavingspraktijk?
8. Hoe verhoudt deze open normstelling zich tot het rechtszekerheidsbeginsel en het vereiste van voorzienbare wetgeving onder het Europees Verdrag voor de Rechten van de Mens (EVRM)?

Kan de regering aan de leden van de fractie van de **VVD** toelichten hoe de “essentiële entiteit” onder 36.764 zich tot de “kritieke entiteit” onder 36.765 verhoudt in gevallen waarin beide regimes van toepassing zijn? Kan de regering toezeggen dat er één loket en één meldlijn komt?

De leden van de fractie van **D66** constateren dat de regering hbo- en wo-instellingen als belangrijke of essentiële entiteit kwalificeert, waardoor deze instellingen onder de Cyberveiligheidswet komen te vallen. Zij geeft daarbij aan dat het geen onderscheid tussen individuele instellingen maakt, maar dat al deze instellingen als een dergelijke entiteit zullen worden aangemerkt. Deze leden vragen of dit niet kan leiden tot onwenselijke situaties. Kan de regering bijvoorbeeld uitleggen waarom wo- en hbo-instellingen belangrijkere of essentiëlere entiteiten zijn dan mbo-instellingen, zeker wanneer mbo-opleidingen duidelijke vitale functies raken, zoals ICT, transport of energie en dit bij bepaalde wo- en hbo-instellingen minder duidelijk kan zijn? Weegt in dergelijke gevallen de noodzaak van het vallen onder de Cyberveiligheidswet en daarmee het moeten voldoen aan de daaruit voortvloeiende eisen wel op tegen de daaruit voortvloeiende lasten?

De leden van de fractie van het **CDA** vragen de regering nader toe te lichten hoe in de praktijk wordt voorkomen dat verschillende bevoegde autoriteiten uiteenlopende normen, toezichtpraktijken en handhavingsstrategieën ontwikkelen. Deze leden vragen de regering daarnaast in hoeverre zij het risico aanwezig acht dat hierdoor rechtsongelijkheid ontstaat tussen sectoren of entiteiten.

De regering geeft aan dat toezichthouders in voorkomende gevallen samenwerkingsafspraken zullen maken. Deze leden vragen waarom niet is gekozen voor een meer expliciete wettelijke afbakening van bevoegdheden en verantwoordelijkheden bij samenloop van toezicht. Daarnaast vragen deze leden hoe wordt voorkomen dat entiteiten geconfronteerd worden met overlappende toezichtslasten, tegenstrijdige aanwijzingen of onduidelijkheid over welke toezichthouder leidend is. Ook zijn deze leden benieuwd naar welke rol de minister van J&V speelt bij het coördineren van deze samenwerkingen.

Deze leden hebben voorts vragen over het vereiste van operationeel onafhankelijk toezicht op overheidsinstanties als bedoeld in artikel 31, vierde lid, van de NIS2-richtlijn. De regering stelt dat de operationele onafhankelijkheid van het toezicht onder meer wordt gewaarborgd door organisatorische scheiding en de Aanwijzingen inzake de rijksinspecties. Deze leden vragen de regering nader te motiveren waarom deze

organisatorische en bestuurlijke waarborgen voldoende worden geacht om te voldoen aan het vereiste van operationele onafhankelijkheid uit de richtlijn.

Deze leden hebben eveneens een vraag over de voorgestelde uitzondering op de toepasselijkheid van de Wet open overheid (Woo). De regering motiveert deze uitzondering mede met het belang dat entiteiten erop moeten kunnen vertrouwen dat verstrekte informatie niet openbaar wordt gemaakt. Deze leden vragen de regering nader toe te lichten waarom de reeds bestaande uitzonderingsgronden binnen de Woo onvoldoende worden geacht om gevoelige bedrijfs- en veiligheidsinformatie te beschermen.

4. Doeltreffendheid / doelmatigheid

Kan de regering aan de leden van de fractie van de **VVD** toelichten hoe de meldplicht “betekenisvol incident” geoperationaliseerd en voorkomen dat entiteiten uit voorzorg alles melden, met overbelasting van meldpunten tot gevolg?

5. Uitvoerbaarheid/handhaafbaarheid

In juni 2024 heeft de Eerste Kamer motie-Fiers c.s. aangenomen met daarin een aantal voorwaarden voor de behandeling van digitaliseringswetgeving.[5] In deze motie wordt een drietal zaken gevraagd:

1. bij de toekomstige wetsbehandeling van digitaliseringswetgeving (zowel nationale wetgeving als implementatiewetgeving van de Europese richtlijnen) inzicht te bieden in de samenhang van het voorliggende wetsvoorstel met bestaande en te verwachten digitaliseringswetten, zodat de Kamer een wetsvoorstel in de juridische context kan beoordelen;
2. bij toekomstige voorstellen voor digitaliseringswetgeving altijd vooraf een Uitvoeringstoets Decentrale Overheden (UDO) te laten uitvoeren, waarbij de samenhang met bestaande en te verwachten digitaliseringswetgeving wordt meegenomen en getoetst op uitvoerbaarheid, waarmee rekening wordt gehouden met juridische, organisatorische en technische implicaties, zodat de Kamer deze kan betrekken bij de beoordeling van voorstellen van digitaliseringswetgeving;
3. bij voorstellen voor toekomstige digitaliseringswetgeving een helder, met de medeoverheden afgestemd, implementatiepad aan te geven (onder andere AMvB's, KB's), met een haalbare implementatietermijn en met inschatting van de kosten voor invoering, zodat de Kamer dit kan betrekken bij de beoordeling om te komen tot zorgvuldige implementatie volgens de bedoeling van de wet.

Aan deze drie vereisten is niet voldaan. De leden van de fracties van **GroenLinks-PvdA** en **PvdD** verzoeken de regering om hier alsnog aan te voldoen.

De Eerste Kamer heeft op 7 oktober 2025 per brief aan de regering te kennen gegeven dat uitvoerbaarheidstoetsen belangrijk zijn om de uitvoerbaarheid van wetgeving goed te kunnen beoordelen.[6] In deze Kamerbrief wordt vervolgens ook ingegaan op een aantal kwalitatieve eisen waaraan een uitvoerbaarheidstoets moet voldoen. Bij deze voorliggende wet zijn consultatiereacties van enkele belangrijke uitvoerende instanties en overheden gevoegd, maar deze consultatiereacties, op de concept-wetgeving, geven geen zicht op de uitvoerbaarheid van de uiteindelijke wet die voorligt. Daarom verzoeken de leden van de fracties van **GroenLinks-PvdA** en **PvdD** aan de regering om de Eerste Kamer alsnog te voorzien van uitvoerbaarheidstoetsen op de voorliggende, geamendeerde, wet van de betrokken organisaties/instanties.

[5] *Kamerstukken I 2025/26,* 36.382, D.
[6] *Kamerstukken I* 2025/26, 31.731 / 29.362, X.

Daarnaast vragen deze leden welke ondersteuning middelgrote organisaties krijgen die niet beschikken over eigen cybersecurityafdelingen? Hoe wordt voorkomen dat kleinere organisaties disproportioneel zwaar worden belast?

Kan de regering de leden van de fractie van de **VVD** een totaaloverzicht geven van alle toezichthoudende instanties en hoe coördinatie (one-stop-shop) wordt geborgd?

Kan de regering deze leden toelichten hoe de persoonlijke aansprakelijkheid van bestuurders zich verhoudt tot bestaande privaat- en bestuursrechtelijke aansprakelijkheidsregimes? Bestaat het risico op over-compliance en defensief bestuur?

De leden van de fractie van **D66** lezen dat de regering aangeeft dat afhankelijkheid van bepaalde leveranciers een te groot risico kan vormen ten aanzien van de beveiliging van digitale systemen. Dit zou kunnen volgen uit de risicobeoordelingen die belangrijke en essentiële entiteiten moeten doen. Het afbouwen van dergelijke afhankelijkheid zou de Nederlandse strategische autonomie ten goede kunnen komen. Kan de regering voorbeelden noemen van gevallen waarin de afhankelijkheid als zodanig groot kan worden gezien, dat het wenselijk is om te stoppen met bepaalde leveranciers? Moet er een concrete aanleiding zijn, zoals een incident ten aanzien van de entiteit zelf, waardoor entiteiten kunnen waarnemen dat de afhankelijkheid te groot is, of kan de macht van een leverancier op zichzelf al reden genoeg zijn?

Daarnaast heeft de regering in de nota naar aanleiding van het verslag aangegeven dat er geen verkenning heeft plaatsgevonden ten aanzien van de vraag of er genoeg materiaal en genoeg cursussen beschikbaar zijn om bestuursleden op te leiden over cyberveiligheid.[7] Daarbij heeft de regering te kennen gegeven dat dit niet is gebeurd, omdat bekend zou zijn dat er voldoende aanbieders van cursussen zijn. Waar baseert de regering dit op, wanneer er geen verkenning heeft plaatsgevonden? Deze leden merken op dat genoeg aanbieders niet noodzakelijkerwijs betekent dat de kwaliteit van de cursussen goed is. Ook is onduidelijk wat voor soort materiaal er beschikbaar is. Is de regering voornemens om hier een verkenning naar uit te voeren? Zo nee, waarom niet?

De regering maakt melding van een verwacht aantal meldingen per jaar.[8] Ten aanzien van de Computer Security Incident Response Teams geeft zij aan dat deze teams op dit moment voorbereidingen treffen om hier in de toekomst mee om te kunnen gaan. Kan de regering aan deze leden toelichten om wat voor voorbereidingen het hier gaat? Daarnaast laat de regering weten dat het cyberlandschap snel verandert. Voorziet de regering steeds meer meldingen? Wat betekent het aantal meldingen en een mogelijke stijging van het aantal meldingen over tijd voor de werklast en operationele capaciteit van de teams? Daarnaast hebben deze leden nog een vraag ten aanzien van de samenstelling van de teams. Hoeveel technische medewerkers zullen ongeveer nodig zijn om alle teams van de wenselijke operationele capaciteit te voorzien? Hoe is de regering van plan om een mogelijk grote hoeveelheid aan vacatures in te vullen, gelet op het grote tekort in Nederland aan beschikbaar personeel in deze sector?

Deze leden lezen dat er duidelijke inschattingen zijn over het aantal organisaties dat aan de verplichtingen in de wet moet voldoen. Tegelijkertijd geeft de regering aan dat

[7] *Kamerstukken II* 2025/26, 36.764, nr. 8.
[8] *Kamerstukken II* 2025/26, 36.764, nr. 8.

in de meeste gevallen de organisaties zelf moeten nagaan of ze een entiteit zijn in de zin van de wet en daarom aan de verplichtingen moeten voldoen. Waarom heeft de regering er niet voor gekozen om organisaties ervan op de hoogte te stellen dat ze onder de wet zouden kunnen gaan vallen, zeker gelet op dat er al wel onderzocht is om welke organisaties het zou gaan?

De leden van de fractie van het **CDA** constateren dat de Vereniging Nederlandse Gemeenten (VNG) en de Unie van Waterschappen zorgen hebben geuit over de uitvoerbaarheid van de Cyberbeveiligingswet voor decentrale overheden. Daarbij wordt onder andere gewezen op financiële en organisatorische consequenties die uitvoering van de Cyberbeveiligingswet met zich brengt. Deze leden vragen de regering toe te lichten hoe deze zorgen worden ondervangen.

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 reeds 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 zien graag 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?

Uit een recent artikel van Het Financieele Dagblad blijkt dat grote bedrijven per jaar tot circa 6700 arbeidsuren en middelgrote bedrijven circa 3500 uur verwachten te moeten investeren in de voorbereidingen op de implementatie van de Cyberbeveiligingswet.[9] Kan de regering aan de leden van de fractie van **JA21** inzichtelijk maken wat de verwachte arbeidsdruk voor het implementeren en naleven van de wet voor kleine bedrijven is? Kan de regering daarnaast aangeven in hoeverre zij het realistisch acht dat kleine, middelgrote en grote bedrijven tijdig aan de verplichtingen uit de Cyberbeveiligingswet kunnen voldoen?

Door de verwevenheid en complexiteit van beide wetsvoorstellen bestaat het risico dat kleine en middelgrote bedrijven in de praktijk vaak beschikken over onvoldoende capaciteit om te voldoen aan de uitgebreide administratieve verplichtingen. Kan de

[9] Cyberbeveiligingswet komt eraan, maar bedrijven lopen mijlenver achter, Het Financieele Dagblad, 7 mei 2026.

regering aan deze leden toelichten op welke wijze wordt voorkomen dat de administratieve en bureaucratische druk voor deze bedrijven onevenredig zwaar wordt?

Deze leden constateren dat op grond van artikel 24 van de Cyberbeveiligingswet ieder lid van het bestuur van een essentiële of belangrijke entiteit verplicht behoort te beschikken over aantoonbare kennis en vaardigheden op het gebied van cyberbeveiliging, inclusief certificering en het actueel houden daarvan. Artikel 93 voorziet daarnaast in de mogelijkheid om individuele bestuurders bestuurlijk te sanctioneren indien niet aan deze verplichtingen wordt voldaan.

1. Hoe voorkomt de regering dat persoonlijke sancties moeilijk of niet verzekerbaar blijken voor bestuurders van essentiële en belangrijke entiteiten?
2. Kan de regering nader toelichten op welke categorieën van private organisaties en bestuursorganen deze verplichtingen van toepassing zijn? Geldt dit bijvoorbeeld voor bestuurders van veiligheidsregio’s, provincies, gemeenten, waterschappen?
3. Kan de regering daarnaast toelichten in hoeverre voldoende trainings- en certificeringscapaciteit beschikbaar is om deze bestuurders binnen de gestelde termijn aan deze verplichtingen te laten voldoen? In hoeverre zijn er uitzonderingsmogelijkheden gewaarborgd?
4. Hoe beoordeelt de regering de proportionaliteit van het opleggen van persoonlijke sancties aan politieke en publieke ambtsdragers wegens het niet voldoen aan verplichtingen die uit de functie voortvloeien?
5. Herkent de regering het risico dat het opleggen van dergelijke persoonlijke sancties een negatieve invloed kan hebben op de bereidheid om bestuurlijke functies binnen decentrale overheden te vervullen en ertoe kan leiden dat zowel publieke als private bestuursfuncties langdurig vacant blijven?
6. Is de regering van mening dat het persoonlijk sanctioneren van openbare bestuurders een ongewenst precedent kan scheppen?
7. Kan de regering nader toelichten hoe artikel 24, lid 3 wordt toegepast op bestuurders die bijvoorbeeld slechts voor één tot twee jaar bestuurder zijn geweest van een essentiële of belangrijke entiteit? Geldt die verplichting ook voor hen en zouden zij in aanmerking kunnen komen voor een persoonlijke sanctie indien zij binnen die periode de benodigde training niet hebben volbracht?

De invoering van de wet heeft gevolgen voor provincies en gemeenten, in het bijzonder gemeenten die grote infrastructurele projecten beheren zoals havens en luchthavens. Kan de regering aan de leden van de fractie van **Volt** toelichten welk overleg zij met de mede-overheden hierover gevoerd heeft? Op welke wijze worden de mede-overheden ondersteund? Op welke wijze wordt gewerkt aan gezamenlijke maatregelen ter uitvoering van de richtlijn? Hoe zit dit met grensoverstijgende samenwerking, bijvoorbeeld tussen de havens van Rotterdam en Antwerpen?

6. Kostenaspect

Kan de regering aan de leden van de fractie van de **VVD** uiteenzetten wat de geactualiseerde raming van de structurele lasten voor bedrijfsleven is en overheid en welke compensatie is voorzien voor gemeenten? Op welke wijze wordt voorkomen dat decentrale overheden – die geen keuze hebben om niet onder de wet te vallen – worden geconfronteerd met onevenredige lasten?

Kan de regering aan de leden van de fractie van **FVD** toelichten hoe wordt geborgd dat de nieuwe verplichtingen voor kritieke entiteiten niet leiden tot onevenredige administratieve lasten en kostenstijgingen voor essentiële sectoren zoals zorg, energie en drinkwatervoorziening? Kan de regering concreet onderbouwen dat de proportionaliteit van de maatregelen systematisch is getoetst? Zo ja, op basis van welke criteria?

De vaste commissies voor Digitalisering en Justitie & Veiligheid zien met belangstelling uit naar de nota naar aanleiding van het verslag en ontvangt deze graag binnen **vier weken** na vaststelling van dit verslag.

De voorzitter van de vaste commissie voor Digitalisering,
Veldhoen

Voorzitter van de vaste commissie voor Justitie en Veiligheid,
Mr. B.O. Dittrich

De griffier voor het verslag,
Van Dooren