Ministerie van Justitie en Veiligheid
Minister van Justitie en Veiligheid
Dhr. D.M. van Weel
Postbus 20301
2500 EH 'S-GRAVENHAGE

CC: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
De staatssecretaris voor Digitalisering en Koninkrijkrelaties Dhr. F.Z. Szabó
Postbus 20011
2500 EA DEN HAAG

Datum
27 maart 2025
Kenmerk
TPW/U202500150
Telefoon
06 18575782
Bijlage(n)
-

Onderwerp: Consultatiereactie VNG op het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten

Geachte heer Van Weel,

In februari is de internetconsultatie gestart voor de Algemene Maatregelen van Bestuur (AMvB) behorende bij de Cyberbeveiligingswet (Cbw) en de Wet weerbaarheid kritieke entiteiten (Wwke). De VNG heeft met belangstelling kennisgenomen van de consultatiewetteksten en deze met onze leden gedeeld. Namens 342 Nederlandse gemeenten delen wij onze reactie met u.

Wij waarderen het dat de teksten van de twee AMvB's beschikbaar zijn gesteld. Om gemeenten en andere medeoverheden goed voor te bereiden op de invoering van de Cbw en Wwke en de impact op hun organisatie helder te krijgen, vragen wij echter om verduidelijking op enkele specifieke punten. Wij zijn bekend met de consultatiereacties van het IPO en de UvW en ondersteunen deze volledig. Onze aandachtspunten betreffen de zorgplicht, training, governance en de meldplicht:

- Zorgplicht
    - Risicogebaseerde informatiebeveiliging vereist risicogebaseerd toezicht.
    - Toezicht moet specifiek, meetbaar, acceptabel, realistisch en tijdgebonden zijn.
    - Gemeenten kampen met personeels- en financiële uitdagingen; het Rijk biedt ondersteuning.
    - De Uitvoerbaarheidstoets Decentrale Overheden moet de implementatiekosten van de Cbw inzichtelijk maken.
- Training en governance
    - Het Cyberbeveiligingsbesluit (Cbb) bepaalt wanneer een trainer gekwalificeerd is.
    - Gemeenten kunnen zelf de training organiseren.

    - CIO Rijk ontwikkelt een trainingssyllabus met input van medeoverheden.
    - De Cbw behoudt de bestaande aansprakelijkheidsregels voor overheidsinstanties.

- Meldplicht
    - Criteria voor significante incidenten en verstoringen volgen het primaire doel van de NIS2 en CER-richtlijn zonder overbelasting bij de entiteiten.
    - Proportionele drempelwaarden voor meldplicht worden in de ministeriële regeling vastgesteld.
    - De impact bepaalt of een incident meldingswaardig is.
    - Gemeenten krijgen voldoende tijd voor implementatie, aangezien de criteria nog onbekend zijn.

Zorgplicht

In hoofdstuk 4 ‘Zorgplicht’, van het Cbb wordt benadrukt dat de beschreven technische, operationele en organisatorische maatregelen op een risicogebaseerde manier toegepast moeten worden. Gezien het verscherpte toezicht op informatiebeveiliging, verwachten wij daarom ook dat het toezicht risicogebaseerd zal zijn. Gemeenten willen dat het risicogebaseerde toezicht onder de Cyberbeveiligingswet zo wordt ingericht dat het specifiek, meetbaar, acceptabel, realistisch en tijdgebonden is, om zo effectief mogelijk te kunnen werken aan verbeteringen in cyberbeveiliging en helder verantwoording af te leggen.

Het Cbb beschrijft in dit hoofdstuk welke maatregelen door beleid ondersteund moeten worden. Hoewel gemeenten en andere medeoverheden graag bereid zijn dit beleid te ontwikkelen en te implementeren, ligt de uitdaging voornamelijk bij het beschikken over voldoende personeel en middelen. Dit geldt ook voor het Besluit weerbaarheid kritieke entiteiten (Bwke).

Daarnaast benadrukken we dat de uitdagingen niet puur financieel zijn, maar ook te maken hebben met de krapte op de arbeidsmarkt. Het is voor gemeenten bijzonder lastig om gekwalificeerd personeel te vinden voor het op peil houden van de informatiebeveiliging.

In de Nota van Toelichtingen zijn voor bedrijven zowel de eenmalige als de structurele implementatiekosten van de Cyberbeveiligingswet uiteengezet. Gemeenten verzoeken om deze informatie ook specifiek voor hen gedetailleerd uit te werken en daarbij de Uitvoerbaarheidstoets voor Decentrale Overheden te gebruiken. Verder is het voor gemeenten van belang om te weten welke gemeenschappelijke regelingen onder de Cbw vallen, aangezien de huidige criteria voor overheidsinstanties tot veel discussies en onzekerheden leiden.

Training en governance

Hoofdstuk 5 ‘Training van het Cbb’ behandelt de onderwerpen die verplicht zijn in de training voor bestuurders. Deze training wordt door een onafhankelijke en gekwalificeerde trainer gegeven. Artikel 24, lid 5 van de Cyberbeveiligingswet vereist dat elk bestuurslid van een essentiële of belangrijke entiteit een certificaat van deelname van een dergelijke training moet hebben. De markt ziet hierin kansen, wat nu al heeft geleid tot een uitgebreid aanbod van zogenaamde NIS2-trainingen. Bij sommige trainers is onduidelijk of ze voldoende gekwalificeerd zijn. Gemeenten verzoeken u om in het Cbb expliciet te maken hoe trainers kunnen aantonen dat zij voldoen aan de gestelde eisen in artikel 22.

Gemeenten willen dat zij zelf deze training kunnen organiseren. De Rijksoverheid kan ondersteuning bieden betreft de inhoud, zodat de kennis en vaardigheden van overheidsbestuurders op dit vlak uniform zijn en toegespitst op de bestuurlijke context. Op deze wijze hebben wij er dan ook vertrouwen in dat het certificaat de juiste waarde vertegenwoordigt.

In dit kader steunen we ook het voorstel voor een uniforme trainingsyllabus voor alle bestuurders van overheidsorganisaties, die door het Rijk wordt samengesteld en bekostigd. We hebben begrepen dat de CIO Rijk bezig is met het opstellen van de inhoud voor deze verplichte training. Wij willen graag betrokken worden en onze input leveren om te verzekeren dat de training aansluit bij de specifieke werkomgeving en maatschappelijke context van gemeenten, provincies en waterschappen, en om de kwaliteit te waarborgen. Bovendien willen gemeenten graag meedenken over de praktische invulling van de training en de verschillende vormen die deze kan aannemen, zoals e-learning.

Governance
Potentiële overheidsbestuurders zouden niet moeten worden afgeschrikt door het risico op bestuurlijke boetes als ze deze training en andere verplichtingen uit de Cbw niet volgen. We willen u er namelijk op wijzen dat artikel 24 lid 12d van de Cbw expliciet het college van burgemeester en wethouders als normadressaat van de wetgeving aanduidt. Volgens de Memorie van Toelichting (MvT) van de Cbw moet elk bestuurslid over voldoende kennis en vaardigheden beschikken en hiervoor een training volgen, waarbij zij ook verantwoordelijk zijn voor de goedkeuring van de genomen maatregelen (Cbw, artikel 24 lid 1). In de MvT bij de Cbw wordt benadrukt dat volgens de NIS2-richtlijn, zoals vastgelegd in artikel 20, lid 2, deze richtlijn geen afbreuk doet aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen.

De laatste zin is correct in de context dat de NIS2-richtlijn geen inbreuk maakt op het nationale recht betreffende overheidsinstanties en de aansprakelijkheid van ambtenaren en gekozen of benoemde overheidsfunctionarissen. Echter, het huidige ontwerp van de Cbw lijkt hier wel inbreuk op te maken. Voor een correcte implementatie van de NIS2-richtlijn in de nationale wetgeving, zonder afbreuk te doen aan bestaande nationale aansprakelijkheidsregels, is meer nodig dan slechts een toelichtende opmerking in de memorie van toelichting over de vereisten van de NIS2-richtlijn.

Wij stellen de volgende aanpassingen in de Cbw voor:

In artikel 24 onder vernummering van het huidige lid 13 naar 14 een nieuw lid 13 invoegen:

> Ongeacht de toebedeling van de verplichtingen aan het bestuur het twaalfde lid is een bestuurdersaansprakelijkheid van overheidsinstanties als bedoeld in artikel 20, eerste lid, eerste volzin, en artikel 32, zesde lid, van de NIS2-richtlijn, uitgesloten voor de besturen van ministeries, provincies, gemeenten, waterschappen of gemeenschappelijke regelingen. Deze uitsluiting van bestuurdersaansprakelijkheid laat het regresrecht van overheidsinstanties jegens hun besturen conform artikel 170, derde lid, van Boek 6 van het Burgerlijk Wetboek onverlet.

Of:

> In artikel 24 in lid 12 de eerste volzin vervangen door:
> "Indien de essentiële entiteit een overheidsinstantie is, wordt voor de toepassing van dit artikel als het bestuur, in de hoedanigheid van vertegenwoordigersvan de essentiële entiteit, aangemerkt:"

Meldplicht

Hoofdstuk 6 van het Cbb en hoofdstuk 5 van de Bwke behandelen de meldplicht. Hierin staat dat de criteria voor een significant incident en aanzienlijke verstoring worden bepaald in ministeriële regelingen. Gemeenten willen graag een zorgvuldige benadering die recht doet aan het primaire doel van de meldplicht volgens de Network and Informationsecurity (NIS2)- en de Critical Entities Resilience (CER)-richtlijnen: het verbeteren van de digitale weerbaarheid binnen de Europese Unie door vroegtijdig inzicht te krijgen in incidenten en dreigingen en continuïteit van essentiële diensten te waarborgen. De Nederlandse implementatiewetgeving van deze richtlijnen moet helpen om relevante incidenten adequaat te identificeren en te rapporteren zonder overbelasting van zowel de entiteiten onder de Cbw en Wwke als de toezichthoudende instanties met onnodige meldingen.

Daarnaast verwachten gemeenten in de ministeriële regelingen proportionele drempelwaarde voor meldingen, zodat alleen die incidenten gemeld worden met een daadwerkelijk risico voor de digitale veiligheid. Vanwege de aanzienlijke bestuurlijke boetes die kunnen oplopen tot € 10 miljoen voor het niet naleven van de meldplicht, moet worden voorkomen dat de meldplicht ertoe leidt dat entiteiten uit voorzorg onnodige meldingen doen om financiële sancties te vermijden.

De impact moet bepalen of een incident meldingswaardig is. Gemeenten verzoeken de wetgever om criteria die zich richten op de gebeurtenis te herformuleren naar de impact ervan. Neem daarnaast meetbare criteria op in de ministeriële regelingen voor significante incidenten, toegespitst op de specifieke context van gemeenten, provincies en waterschappen. We stellen voor om twee jaar na de invoering van de Cbw, Cbb, Wwke en Bwke de inhoud van de meldplicht te evalueren om zowel de administratieve lasten als de voordelen ervan opnieuw te beoordelen.

Omdat de drempelwaarden pas in de ministeriële regelingen worden vastgesteld, die momenteel nog niet beschikbaar zijn, kunnen gemeenten hun bestaande meldprocessen niet aanpassen aan de nog te definiëren criteria voor significante incidenten. Gemeenten verzoeken de wetgever hiermee rekening te houden en hen voldoende tijd te geven om, na de bekendmaking van de ministeriële regeling, hun meldprocessen aan te passen aan de vastgestelde criteria.

Financiering

De VNG is bezorgd over de kosten die gemeenten en andere medeoverheden moeten maken voor de implementatie. Om te kunnen voldoen aan de Cbw is een eerste randvoorwaarde dat, in overeenstemming met artikel 2 van de Financiële-verhoudingswet, de rijksoverheid zorgt voor adequate financiële dekking van de extra uitvoeringskosten die gemeenten moeten maken voor de naleving. De VNG is hierover nog in gesprek met het rijk.

Samenwerking

Namens de medeoverheden vertrouwen wij erop dat u onze punten meeneemt in de definitieve versie van de Cbw, Cbb, Bwke en de bijbehorende Memories van Toelichting en Nota van toelichting. Waar verdere toelichting nodig is zullen we deze uiteraard verstrekken.

Sinds begin 2023 werkten wij samen met uw ambtenaren om tot een goede implementatie van de NIS2- en CER-richtlijn voor lokale overheden te komen. Wij zetten deze samenwerking graag voort om zo tot een digitaal veilige en weerbare overheid te komen.

Met vriendelijke groet,

Vereniging van Nederlandse Gemeenten

mr L.K. Geluk
Algemeen directeur