Ministerie van Justitie en Veiligheid
Minister van Justitie en Veiligheid
Dhr. D.M. van Weel
Postbus 20301
2500 EH DEN HAAG

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

Datum
2 juli 2024
Ons kenmerk
U202400361
Uw kenmerk
.
Telefoon
.
Bijlage(n)
1. Uitvoeringsanalyse Digital Decade Wetten beveiliging Netwerk- en Informatiesystemen
2. Memo begrip bestuursorgaan Hooghiemstra en Partners

Geachte heer Van Weel,

In mei zijn de consultaties op de Cyberbeveiligingswet (Cbw) en Wet weerbaarheid kritieke entiteiten (Wwke) gestart. De VNG heeft met belangstelling kennisgenomen van de consultatiewetteksten en deze met onze leden gedeeld. Uiteraard onderschrijven de gemeenten van Nederland het doel van deze wetten. Namens hen delen wij deze reactie met u.

Het is goed dat de conceptwetteksten nu beschikbaar zijn. Echter, doen deze nog onvoldoende recht aan de diversiteit van taken van de Nederlandse gemeenten, en hun samenwerkingsverbanden, of aan onderlinge verschillen in schaalgrootte en organisatorische slagkracht.

Om een digitaal veilige en weerbare overheid te worden, is het van cruciaal belang dat wij de nieuwe wetten op lokaal niveau kunnen uitvoeren. De haalbaarheid, betaalbaarheid en uitvoerbaarheid staan hierbij centraal.

Daarom brengen wij een aantal punten onder uw aandacht:

- Zorgplicht
    - Gemeenten moeten worden gecompenseerd voor de implementatiekosten.
    - Gemeenten implementeren de zorgplicht van de Cbw risico-gebaseerd, met een balans tussen effectiviteit en kosten.
- Governance
    - De Cbw moet geen individuele functionarissen sanctioneren, maar bestuursorganen (volgens de definitie van de Algemene wet bestuursrecht).

Vereniging van Nederlandse Gemeenten
Nassaulaan 12 Den Haag | Postbus 30435 | 2500 GK Den Haag
070 - 373 83 93 | info@vng.nl

    - De verplichte training uit de Cbw past bij de behoefte van het bestuur.
- Meldplicht
    - De gemeenten kunnen alleen aan de meldplicht voldoen als de Cbw en Wwke duidelijk maken wat meldplichtig is.
    - De Cbw en Wwke moeten duidelijk maken bij welke instanties gemeenten melden.
- Toezicht
    - De auditlasten en kosten voor de controlefunctionaris moeten betaalbaar zijn voor gemeenten.
    - Het toezichtsstelsel wordt geharmoniseerd om de auditlasten te verlagen.
- Sancties
    - Gemeenten krijgen eerst de kans om aan de nieuwe wetgeving te voldoen, voordat boetes worden opgelegd.
- Definitie overheidsinstantie
    - De definitie van een overheidsinstantie moet in de Cbw worden verduidelijkt, zodanig dat gemeenschappelijke regelingen hier standaard onder vallen, tenzij de bevoegde autoriteit anders bepaalt.
- Samenloop sectoren en gemeentetaken
    - De Cbw en Wwke dienen voldoende rekening te houden met de diverse taken van gemeenten.
- Wet weerbaarheid kritieke entiteiten
    - De normen- en toetsingskaders van de Cbw en Wwke moeten op elkaar worden afgestemd.
    - De nadere regelgeving moet uitvoerbaar, haalbaar en betaalbaar zijn.
- Uitvoerbaarheidstoets Decentrale Overheden (UDO) en voorhangprocedure
    - Op de nadere regelgeving van de Cbw en Wwke komt een UDO en een voorhangprocedure, om ervoor te zorgen dat de regels zorgvuldig worden overwogen.

Zorgplicht

Gemeenten worden gecompenseerd voor de implementatiekosten.

Wij zijn bezorgd over de kosten die gemeenten 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 van de nieuwe regelgeving voor het beveiligen van netwerk- en informatiesystemen. Zie ook bijlage 1: Uitvoeringsanalyse Digital Decade Wetten beveiliging Netwerk- en Informatiesystemen.

In de Memorie van Toelichting (MvT) van de Cbw op pagina 54 dat nieuwe entiteiten onder de NIS2 een toename van maximaal 22% aan ICT-beveiligingskosten nodig hebben om aan de eisen van de Cbw te voldoen. Wij merken op dat de MvT niet specificeert wat deze extra 22% aan kosten precies omvat. Wij verzoeken u deze details aan de MvT toe te voegen.

Gemeenten momenteel bezig met de implementatie van de BIO, die een zelfverplichtend karakter kent en geen wettelijke verankering. Dit zal veranderen met de Cbw. De Cbw betekent een taakverzwaring op het gebied van zorgplicht, governance, registratieplicht en meldplicht. Waarbij opgemerkt moet worden dat gemeenten niet alleen steeds meer worstelen met de

uitvoeringskosten van de drie decentralisaties van 2015, maar hier ook een informatiehuishouding aan overgehouden hebben met inherent hogere risico's voor de samenleving, die langs deze weg nog kostbaarder worden dan ooit voorzien. Volgens artikel 2 van de Financiële-verhoudingswet dient de rijksoverheid de kosten die medeoverheden maken door nieuwe taken of extra werkzaamheden (zoals de wettelijke zorgplicht, meldplicht en registratieplicht, en de fysieke beveiliging van systemen) te vergoeden om te voorkomen dat deze medeoverheden in financiële problemen komen.

We willen u erop wijzen dat een compensatie per inwoner voor gemeenten niet voldoende zou zijn om de verplichtingen van de Cbw te implementeren, omdat kleine gemeenten dezelfde processen gebruiken en beheren als grote gemeenten waardoor ze dezelfde kosten en inspanningen hebben, ongeacht hun grootte. De vergoeding moet recht doen aan de feitelijke situatie van gemeenten. We zien dit graag verder uitgewerkt in de uitvoerbaarheidstoetsen, als onderdeel van het UDO-proces (Uitvoerbaarheidstoets Decentrale Overheden).

Gemeenten implementeren de zorgplicht van de Cbw risico-gebaseerd, met een balans tussen effectiviteit en kosten.

In artikel 23 lid 1 van de Cbw staat dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheersen. Hierbij wordt rekening gehouden met de stand van de techniek, uitvoeringskosten, EU- en internationale normen, de mate van blootstelling aan risico's, de omvang van de entiteit, de kans en ernst van incidenten, inclusief de maatschappelijke en economische gevolgen.

In de MvT op pagina 20 staat dat een beperkte financiële capaciteit of een beperkte omvang van een entiteit geen reden kan zijn om de weerbaarheid niet op orde te hebben. Hier kunnen wij ons niet in vinden. Niet alleen staat dit haaks op wat de NIS2-richtlijn beoogt met evenredigheid, de Cbw houdt hier ook geen rekening met de uitwerking van de nieuwe financieringssystematiek voor gemeenten voor de periode na 2025. In 2026 eindigt het huidige financiële systeem voor gemeenten, wat leidt tot financiële onzekerheid en een geschat tekort van ongeveer 3 miljard euro. Dit kan de financiering van onmisbare diensten zoals jeugdzorg, woningbouw en armoedebeleid in gevaar brengen. De herstructurering van het Gemeentefonds is nog niet afgerond en moet door het kabinet worden opgepakt.

We stellen voor dat gemeenten risico-gebaseerd de zorgplicht van de Cbw en de BIO2.0 zullen implementeren, met een balans tussen effectiviteit en kosten. Hiervoor is een meerjarig organisatieontwikkelingstraject voor gemeenten nodig, met aandacht voor de uitvoerbaarheid door zowel grote als kleine gemeenten. Daarnaast dient de Cbw een groeipad aan te bieden voor essentiële en belangrijke entiteiten om aan de Cbw te voldoen en dat gemeenten gecompenseerd worden voor de financiële gevolgen. Hier volgt een korte beschrijving.

Governance

De Cbw moet geen individuele functionarissen sanctioneren, maar bestuursorganen (volgens de definitie van de Algemene wet bestuursrecht).

In artikel 26 lid 7 lezen wij dat indien het bestuur van een essentiële entiteit een gemeente is (want een rechtspersoon naar publiek recht), het gemeentebestuur hoofdelijk aansprakelijk is voor de naleving van deze wet door desbetreffende essentiële entiteit. Aangezien het veelvuldig voorkomt dat gemeenten als rechtspersoon zitting hebben in het bestuur van samenwerkingsverbanden en uitvoeringsinstanties is dit onwenselijk.

In lid 8 van artikel 26 van de Cbw wordt gesteld dat voor de toepassing van het bepaalde in de leden twee tot en met zes van artikel 26, de leden van het bestuur van een ministerie, provincie, gemeente, waterschap of gemeenschappelijke regeling worden beschouwd als leden van de ambtelijke leiding.

Wij verzoeken u dringend om de term 'bestuur' in lijn te brengen met de bestaande wettelijke definities zoals gehanteerd in de Gemeentewet. Om de rechtszekerheid en de coherente toepassing van wetgeving binnen de gemeentelijke en andere overheidsorganisaties te garanderen is het essentieel dat de term 'bestuur' duidelijk en consistent wordt gebruikt en geïnterpreteerd. Een afwijkende interpretatie van de term 'bestuur' in de Cbw kan leiden tot verwarring en misverstanden omtrent verantwoordelijkheden en bevoegdheden binnen gemeenten en andere overheidsinstanties. Dit kan op zijn beurt de effectieve uitvoering van de Cbw en de algehele cyberbeveiliging negatief beïnvloeden.

De redenen waarom u het bestuur als de ambtelijke leiding beschouwt, worden genoemd in de MvT:

- Zij zijn verantwoordelijk voor dagelijkse werkzaamheden.
- De verplichtingen passen beter bij hen dan bij politiek benoemde ambtsdragers.
- Bovendien past het sanctioneren niet bij de aard van de benoeming van politiek benoemde ambtsdragers (p.23, MvT).

Het argument dat sanctioneren niet past bij de aard van politiek benoemde ambtsdragers is niet valide, aangezien de NIS2-richtlijn ruimte laat aan het nationale recht af te wijken voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen. Hiermee blijven er slechts twee argumenten over om het bestuur als de ambtelijke leiding aan te merken. Door het bestuur als ambtelijke leiding in te vullen, lijkt de Cbw in de praktijk nieuwe maatregelen zoals boetes, voorafgaand toezicht en een meldingsplicht in te voeren, zonder dat dit onderwerp op de agenda van het hoogste bestuursniveau (college van burgemeester en wethouders, gemeenteraad) komt te staan. Gezien de doelstellingen van de richtlijn, zoals opgenomen in overweging 137 van de NIS2-richtlijn, zou het echter logisch zijn om onder bestuursorganen ook het gemeentebestuur (dus het college van burgemeester en wethouders) te verstaan. Deze overweging luidt:

137. Deze richtlijn moet gericht zijn op het waarborgen van een hoge mate van verantwoordelijkheid voor de risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging op het niveau van de essentiële en belangrijke entiteiten. Daarom moeten de bestuursorganen van de essentiële en belangrijke entiteiten de risicobeheersmaatregelen op het gebied van cyberbeveiliging goedkeuren en toezicht houden op de uitvoering ervan.

De NIS2-richtlijn richt zich op het vermogen van de 'hoogste leiding' van een organisatie om de risicobeheersing met betrekking tot informatiebeveiliging effectief aan te sturen. Dit betekent dat zowel het college van burgemeester en wethouders als de gemeentesecretaris in staat moeten zijn

om goedkeuring te verlenen aan voorgestelde maatregelen, toezicht daarop te houden, en de benodigde scholing hiervoor te ontvangen. Zie ook bijlage 2: Memo begrip bestuursorgaan Hooghiemstra en Partners.

Daarnaast sluit het sanctioneren van een individuele functionaris van de ambtelijke leiding niet aan bij de manier waarop besluitvorming binnen gemeenten plaatsvindt. In gemeenten is er sprake van collectieve besluitvorming door het college van B&W, wat conflicteert met persoonlijke sancties voor een ambtelijke leidinggevende of bestuurder. Als de gemeentesecretaris, verantwoordelijk voor de beveiliging van netwerk- en informatiesystemen, vindt dat er extra geïnvesteerd moet worden in informatiebeveiliging, kan het college besluiten dit niet te doen en de middelen aan andere prioriteiten te besteden (bijvoorbeeld jeugdzorg of de bibliotheek). Dit kan tot vreemde situaties leiden als de gemeentesecretaris vervolgens wel persoonlijk gesanctioneerd kan worden. Daarom stellen wij voor om niet individuele functionarissen te sanctioneren, maar bestuursorganen volgens de Algemene wet bestuursrecht.

De verplichte training uit de Cbw past bij de behoefte van het bestuur.

In de consultatieversie van de Cbw heeft het traditionele bestuur, in het geval van gemeenten het college van Burgemeester en Wethouders en de gemeenteraad, de verantwoordelijkheid om goedkeuring te verlenen aan de maatregelen en houdt zij toezicht op de uitvoering daarvan volgens lid 1 van artikel 26. Het betekent ook dat het traditionele bestuur is uitgezonderd van de verplichte training. Echter, op pagina 23 van de MvT staat dat het bestuur over voldoende kennis en vaardigheden moet beschikken om een goed oordeel te kunnen geven over risicobeheersmaatregelen en de uitvoering daarvan. Dit omvat het kunnen identificeren van beveiligingsrisico’s voor de netwerk- en informatiesystemen van de entiteit, het beoordelen van risicobeheersmaatregelen, en het inschatten van de gevolgen van deze maatregelen voor de door de entiteit aangeboden diensten. Hier lijkt sprake te zijn van een tegenstrijdigheid, aangezien in lid 1 van artikel 26 het traditionele bestuur verantwoordelijk wordt gesteld voor goedkeuring en toezicht, terwijl ditzelfde bestuur is uitgezonderd van de verplichte opleiding volgens lid 8 van artikel 26. Wij stellen voor om in artikel 26 geen onderscheid te maken tussen de verantwoordelijkheden en verplichtingen van het bestuur en die van de ambtelijke leiding.

In artikel 26 van de Cbw staat dat ieder lid van het bestuur kennis en vaardigheden moet hebben om beveiligingsrisico's te identificeren, cyberbeveiligingsmaatregelen te beoordelen, en de gevolgen voor de diensten te kunnen inschatten. Deze kennis en vaardigheden dienen bestuurders via een training op te doen. In lid 6 van artikel 26 stelt u dat er in de algemene maatregel van bestuur (AMvB) nadere regels worden vastgesteld over de training, waaronder de duur en het niveau. Wij stellen voor om de verplichte training goed af te stemmen op de specifieke rollen van zowel bestuurders als de ambtelijke leiding en te onderzoeken wat de trainingsbehoeften van de verschillende groepen bestuurders bij gemeenten zijn alvorens een concrete verplichting voor het volgen van opleidingen vast te leggen in de Cbw. Dit betekent dat er verschillende trainingen moeten worden ontwikkeld. Uit de nadere regelgeving moet ook nog blijken of het niveau gaat om diepgaande kennis van cybersecurity, die doorgaans pas na 5 tot 10 jaar ervaring door professionals wordt bereikt. Om die reden zou het wenselijk zijn dat de eisen in lid 2 en 3 van artikel 26 ook de rol van zowel een bestuurder als de ambtelijke leiding in overweging neemt. Een bestuurder moet zich namelijk richten op het besturen en hoeft niet te worden opgeleid tot informatiebeveiligingsprofessional.

Voor bestuurders zou de training zich moeten richten op:

- Het begrijpen van risico-gebaseerd werken
- Het begrijpen van de PDCA-cyclus

Voor de ambtelijke leiding moet de training zich richten op de professionele uitvoering van de onderwerpen genoemd in lid 2.a, 2.b, en 2.c. Hierbij gaat het dus om:

- Inzicht hebben in wat een Information Security Management Systeem (ISMS) is.
- Toezien op een competente invulling van de informatiebeveiligingsorganisatie, waaronder de CISO-, TISO-, en ISO-rol
- Jaarlijks laten analyseren van risico's en het opstellen van een beveiligingsplan.
- De voortgang van dat plan inhoudelijk volgen.
- Organiseren dat periodiek een externe beoordeling wordt gedaan

Een training die de bovengenoemde punten behandelt hoeft niet lang te duren. Met de invoering van de NIS2-richtlijn zien we veel particuliere aanbieders die trainingen voor bestuurders aanbieden, variërend in duur, niveau en kosten. De Cbw moet zich richten op het vergroten van het risicobewustzijn en ervoor zorgen dat de markt niet verandert in een onoverzichtelijk aanbod van uiteenlopende trainingsbureaus die willekeurige trainingen aanbieden. We vragen ons af hoe u de coördinatie van deze verschillende trainingen zult aanpakken. We zien graag in de AMvB meer duidelijkheid over de accreditatie van de training en de erkenning van het certificaat van deelname, en denken hierover graag mee.

Een mogelijke aanpak is dat de bevoegde autoriteit van de overheidssector en de toezichthoudende instantie een module op stellen waar VNG aan meewerkt waarin de verplichte onderwerpen en leerdoelen voor bestuurders en de ambtelijke leiding worden behandeld. Deze module moet openbaar beschikbaar worden gesteld, zodat ook (gemeentelijke) CISO's hiermee een training kunnen ontwikkelen en intern aan hun bestuurders kunnen geven. Door intern casussen of vragen te behandelen, besparen gemeenten niet alleen kosten, maar ervaren zij ook de voordelen van bet bespreken van relevante en actuele discussies binnen hun eigen organisatie. Hierdoor kunnen goede gesprekken plaatsvinden die specifiek gericht zijn op hun eigen situaties en uitdagingen, en kunnen deze direct worden aangepakt binnen de eigen organisatie.

Meldplicht

De gemeenten kunnen alleen aan de meldplicht voldoen als de Cbw en Wwke duidelijk maken wat meldplichtig is.

Lid 2 van artikel 27 van de Cbw geeft de definitie van een significant incident:

> a. een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of
> b. andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

De MvT Cbw schrijft op pagina 24 dat de meldplicht alleen voor significante incidenten geldt.

Artikel 18 van de Wwke spreekt van een aanzienlijke verstoring:

> 3. Bij het bepalen of een verstoring aanzienlijk is, wordt in elk geval in aanmerking genomen:
> a. het aantal door de verstoring getroffen gebruikers en hun aandeel daarin;
> b. de duur van de verstoring;

c. het door de verstoring getroffen geografische gebied, rekening houdend met de vraag of het gebied geografisch geïsoleerd is.

En in lid 1. De kritieke entiteit meldt een incident dat de verlening van haar essentiële dienst aanzienlijk verstoort of kan verstoren binnen 24 uur of, indien dat operationeel niet mogelijk is, zo snel mogelijk nadat zij kennis heeft genomen van dat incident bij de bevoegde autoriteit.

De omschrijving van “significant” of “aanzienlijk” is ruim, waardoor allerlei incidenten hieronder vallen.
Wij stellen daarom voor dat u een concrete definitie van een significant incident en aanzienlijke verstoring opstelt, zoals gedaan werd voor de herijking van de vitale infrastructuur in 2015[1].

Tevens begint de klok voor de 24-uren- en 72-uren-termijnen pas te lopen vanaf het moment dat wordt vastgesteld dat het incident significant is. In artikel 28 en 29 stelt u dat essentiële en belangrijke entiteiten binnen 24 uur een vroegtijdige waarschuwing moeten geven aan hun CSIRT en de bevoegde autoriteit, en na 72 uur een update, initiële beoordeling en indicatoren voor aantasting moeten verstrekken. Het kan enige tijd duren voordat de exacte reikwijdte van een incident is vastgesteld.

Het is aan de wetgever om een duidelijke definitie te formuleren van wat een significant incident of een aanzienlijke verstoring inhoudt. Daarnaast ontbreken ook heldere definities voor de andere categorieën zoals incident, bijna-incident en cyberdreiging (lid 1 artikel 35 Cbw) en worden deze volgens de conceptwettekst vrijwillig gemeld bij het CSIRT, wat willekeur in de hand werkt. De wetgever moet deze begrippen duidelijk definiëren en specificeren wat meldplichtig is.

De Cbw en Wwke moeten duidelijk maken bij welke instanties gemeenten melden.

In artikel 31 van de Cbw staat dat entiteiten hun melding moeten doen bij hun CSIRT en de bevoegde autoriteit. In de MvT (p.24) staat dat entiteiten moeten melden bij hun CSIRT en de toezichthoudende instantie. De Wwke stelt in artikel 18 lid 1 dat de kritieke entiteit een aanzienlijk verstorend incident meldt bij de bevoegde autoriteit.

Om verwarring te voorkomen en de uitvoerbaarheid van de wet te waarborgen, verzoeken wij u om consistent te zijn in het gebruik van terminologie in beide wetteksten alsook in de MvTen, zodat duidelijk is bij welke instanties meldingen gedaan moeten worden. Wij verwachten dat significante incidenten gepaard kunnen gaan met een datalek volgens de AVG. Hierdoor zijn mogelijk meer meldplichten. Hierbij dient ook rekening gehouden te worden met het feit dat gemeenten taken uitvoeren in verschillende sectoren die onder de Cbw vallen. Het is nu nog onduidelijk wanneer gemeld moet worden aan Z-CERT, CERT-WM, het NCSC en de Informatiebeveiligingsdienst (IBD). Omwille van die duidelijkheid vragen wij u om in de MvT op te nemen dat gemeenten altijd melden bij de IBD en de toezichthoudende instantie.

Toezicht

De auditlasten en kosten voor de controlefunctionaris moeten betaalbaar zijn voor gemeenten.

[1] https://zoek.officielebekendmakingen.nl/kst-30821-23.html

In lid 2 van artikel 69 van de Cbw staat dat de bevoegde autoriteit de kosten draagt van de beveiligingsscan, tenzij een bij AMvB omschreven geval zich voordoet waarin deze kosten moeten worden gedragen door de betrokken entiteit. Verderop, in lid 4 van artikel 70, staat dat de essentiële entiteit de kosten draagt van een gerichte beveiligingsaudit, tenzij een bij AMvB omschreven geval zich voordoet waarin deze kosten niet door de betrokken entiteit worden gedragen. Ook staat in artikel 68 lid 3 van de Cbw dat de entiteit de kosten van de controlefunctionaris, die door de bevoegde autoriteit is aangewezen, draagt, tenzij de AMvB anders bepaald.

In artikel 35 lid 3 van de Wwke staat, dat de kritieke entiteit de kosten draagt van het onderzoek, tenzij een bij algemene maatregel van bestuur omschreven geval zich voordoet waarin de betrokken entiteit deze kosten niet hoeft te dragen.

Gemeenten verantwoorden zich jaarlijks via de ENSIA-methodiek. Als de Cbw en de Wwke meer verantwoordingsmomenten en handhavingsmethoden introduceren, moet dit haalbaar, betaalbaar en uitvoerbaar zijn voor gemeenten. Het is onduidelijk waarom en wanneer een essentiële of kritieke entiteit kosten draagt voor de beveiligingsaudit en waarom er onderscheid wordt gemaakt tussen de kostendrager van een beveiligingsscan en een gerichte beveiligingsaudit.

Het toezichtsstelsel wordt geharmoniseerd om de auditlasten te verlagen.

Na de consultatie van de Cbw en de Wwke worden in de nadere regelgeving door verschillende vakministers mogelijk nog meer kaders toegevoegd. Het is voor gemeenten van belang dat de wetstellers zich in spannen om de wetgeving en normenkaders goed op elkaar af te stemmen en te harmoniseren, zodat daarmee de auditlast voor gemeenten omlaag gaat.

De Cbw en de Wwke betekent wat betreft toezicht (vooraf) een taakverzwaring voor de medeoverheden. Ook hier dient de wetgever rekening te houden met artikel 2 van de Financiële-verhoudingswet, en we zien dit graag verder uitgewerkt in de uitvoerbaarheidstoets.

Sancties

Gemeenten krijgen eerst de kans om aan de nieuwe wetgeving te voldoen, voordat boetes worden opgelegd.

In artikel 77 staat dat de bevoegde autoriteit bij overtreding van de Cbw een bestuurlijke boete kan opleggen aan een essentiële entiteit. Bij inbreuken op de zorgplicht en meldplicht is de boete maximaal 10 miljoen euro. Bij inbreuken op de registratieplicht is de boete maximaal 1 miljoen euro. Bij het niet verlenen van medewerking aan de toezichthouder is de boete maximaal 5150 euro. In artikel 93 staat dat de Cbw ingaat op een datum die later door de koning (of de regering) wordt bepaald, waarbij sommige delen van de wet op verschillende momenten ingaan.

Eerder hebben wij onder zorgplicht de noodzaak van een meerjarig organisatieontwikkelingstraject aangegeven om de Cbw bij gemeenten te implementeren. Gemeenten moeten een realistische termijn krijgen om aan de eisen van de wetgeving te voldoen. Tijdens deze overgangsperiode stellen wij voor dat artikel 77 van de Cbw wordt opgeschort en pas van kracht gaat wanneer gemeenten over de nodige middelen en capaciteit beschikken om aan de Cbw te kunnen voldoen. Hiervoor dient een uitvoerbaarheidstoets te worden uitgevoerd op zowel de AMvB als de

ministeriële regelingen, die ook duidelijkheid moeten geven over de totale implementatiekosten en -termijn, en de vorm van uitkering. Daarnaast verzoeken wij u om verduidelijking te geven over welk bestuursorgaan de boete ontvangt, zoals voor gemeenten het college van B&W of de Raad.

Definitie overheidsinstantie

De definitie van een overheidsinstantie moet in de Cbw worden verduidelijkt, zodanig dat gemeenschappelijke regelingen hier standaard onder vallen, tenzij de bevoegde autoriteit anders bepaalt.

In artikel 16 van de Cbw en in de MvT op pagina 15 staat dat gemeenschappelijke regelingen aangewezen worden als essentiële entiteit, mits zij kwalificeren als overheidsinstantie en als entiteit genoemd in bijlage 1 of 2 van de NIS2-richtlijn. Op pagina 13 van de MvT staat dat een overheidsinstantie wordt gedefinieerd als een entiteit die overeenkomstig het nationale recht als zodanig in de lidstaat is erkend en die aan de volgende criteria voldoet:

a. zij is opgericht om te voorzien in behoeften van algemeen belang en heeft geen industrieel of commercieel karakter;
b. zij heeft rechtspersoonlijkheid of mag volgens de wet namens een andere entiteit met rechtspersoonlijkheid optreden;
c. zij wordt grotendeels gefinancierd door de staat, regionale autoriteiten of andere publiekrechtelijke organen, is onderworpen aan beheerstoezicht door die autoriteiten of organen, of heeft een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, regionale autoriteiten of andere publiekrechtelijke organen worden benoemd; en
d. zij heeft de bevoegdheid om ten aanzien van natuurlijke of rechtspersonen administratieve of regelgevende besluiten te nemen die van invloed zijn op hun rechten op het grensoverschrijdende verkeer van personen, goederen, diensten of kapitaal.

In Nederland bestaat er geen officiële definitie van het begrip 'overheidsinstantie', maar er is wel een definitie van bestuursorgaan in de zin van artikel 1:1 van de Algemene wet bestuursrecht. Het begrip overheidsinstantie zou dezelfde betekenis moeten hebben als bestuursorgaan. Daarnaast willen we u erop wijzen dat er meer gemeenschappelijke regelingen (>400) zijn in Nederland dan gemeenten (342). Met de huidige criteria wordt het merendeel van deze gemeenschappelijke regelingen niet als overheidsinstantie aangemerkt, terwijl een van de grootste risico’s voor een ransomware-aanval voortkomt uit het feit dat gevaren in ketens en samenwerkingsverbanden vaak onopgemerkt blijven. Tevens maakt u het met deze criteria mogelijk dat overheidstaken worden georganiseerd en uitgevoerd door gemeenschappelijke regelingen, waardoor deze niet onder de Cbw vallen.

Wij stellen voor, omwille van duidelijkheid, dat gemeenschappelijke regelingen standaard onder de Cbw vallen en dat u individuele gemeenschappelijke regelingen die niet onder de Cbw hoeven te vallen aanwijst, met een duidelijke motivatie. Daarnaast missen wij in de MvT een uitleg waarom andere samenwerkingsverbanden, die geen gemeenschappelijke regeling zijn, zoals een Zorg- en Veiligheidshuis, veiligheidsregio’s of het RIEC, niet worden genoemd of niet onder de Cbw vallen. Wij vragen u uit te werken wat de Cbw betekent voor de verschillende type samenwerkingsverbanden waarbinnen gemeenten opereren.

Samenloop sectoren en gemeentetaken

De Cbw en Wwke dienen voldoende rekening te houden met de diverse taken van gemeenten.

De consultatieversies van de Cbw en Wwke doen in de beleving van VNG geen recht aan het feit dat gemeenten ook taken uitvoeren in de andere sectoren van bijlage 1 Cbw en bijlage 1 van Wwke. Gemeenten vervullen namelijk ook taken in zorg, wegenbeheer, netwerkbeheer, drinkwatervoorziening-, afvalwaterbeheer en afvalstoffenbeheer. Gemeenten hebben dus te maken met een breed scala aan wetgeving.

Dit leidt in de context van de implementatie van de Cbw en Wwke tot de volgende vraagstukken:

- Wat is de bevoegde autoriteit voor gemeentelijke organisaties of organisatieonderdelen van gemeenten waar genoemde taken uitgevoerd worden, respectievelijk organisaties die in opdracht van gemeenten deze taken uitvoeren?
- Wat is of zijn de CSIRT(s) voor entiteiten die namens de gemeente een overheidstaak uitvoeren? Zie ook onze reactie op de meldplicht (specifiek het meldpunt).
- In diverse artikelen van de Cbw wordt gerefereerd aan een onafhankelijke deskundige, al dan niet in de rol van controlefunctionaris. Ons is niet duidelijk geworden of de onafhankelijke deskundige altijd de controlefunctionaris moet zijn en/of deze toe te rekenen valt aan de essentiële entiteit, het CSIRT of de bevoegde autoriteit danwel daadwerkelijk onafhankelijk is. In het laatste geval roept dit vervolgvragen op over de waarborgen waarmee deze rol of rollen omkleed worden, met name op het gebied van aansprakelijkheid jegens de essentiële entiteit, de verwerkingsgrondslag in de zin van de AVG als de onafhankelijke deskundige toegang krijgt tot (bijzondere) persoonsgegevens, de geheimhouding en de beveiliging die deze dient te betrachten ten aanzien van gegevens van de essentiële entiteit waar toegang tot verschaft wordt.

Wet weerbaarheid kritieke entiteiten

De huidige consultatiewettekst van de Wwke laat nog onduidelijkheid bestaan over de aanwijzing van (sommige) gemeenten als kritieke entiteiten. Volgens artikel 7 lid 6 van de Wwke moet de bevoegde autoriteit uiterlijk op 17 juli 2026, op basis van een risicobeoordeling, de eerste aanwijzingen van entiteiten als kritieke entiteiten hebben gedaan. De eerste risicobeoordeling moet uiterlijk op 17 januari 2026 plaatsvinden (artikel 9 lid 5 Wwke).

De normen- en toetsingskaders van de Cbw en Wwke moeten op elkaar worden afgestemd.

Wij voorzien de mogelijkheid dat bepaalde gemeenten of gemeentelijke organisaties als kritieke entiteiten worden aangewezen. Daarnaast kan het zijn dat in de ministeriële regelingen verschillende normenkaders en toetsingskaders voor de Wwke en de Cbw worden gehanteerd. Voor de Wwke wordt verwacht dat het normenkader voor de sector overheid de CSIR 3.0 is, terwijl voor de Cbw de BIO 2.0 geldt. Verder merken we op dat de NIS2-richtlijn voortbouwt op het bestaande NIS1-toetsingskader en dat de CER-richtlijn voortbouwt op het bestaande DORA-toetsingskader. Dit leidt niet alleen tot taakverzwaring maar ook tot verwarring. Wij verzoeken u daarom de normenkaders en toetsingskaders goed op elkaar af te stemmen in de nadere regelgeving en medeoverheden in de benodigde middelen te voorzien om deze taken uit te voeren.

Wij verzoeken u dit te doen via het UDO-proces voor het Wwke en benadrukken het belang van een uitvoerbaarheidstoets op de nadere regelgeving.

De nadere regelgeving moet uitvoerbaar, haalbaar en betaalbaar zijn.

Zoals eerder vermeld onder "samenloop sectoren en gemeenten," voeren gemeenten taken uit in verschillende sectoren die genoemd worden in bijlage 1 van de Wwke. Daarom achten wij de kans groot dat sommige gemeenten als kritieke entiteiten zullen worden aangemerkt onder de Wwke. Dit brengt met zich mee dat gemeenten een meldplicht, zorgplicht en toezicht zullen hebben volgens de Wwke. Gemeenten en andere medeoverheden voorzien grote gevolgen van deze mogelijke classificatie en zijn onzeker over de benodigde maatregelen.

We willen benadrukken dat de CSIR 3.0 te zwaar is voor kleine OT (Operationele Technologie) objecten en kleine gemeenten. Dit geldt ook voor de waterschappen. Daarom stellen wij voor dat u via het UDO-proces laat onderzoeken of een tussenvariant van de CSIR en de BIACS noodzakelijk is, voordat een norm wordt vastgesteld in de nadere wetgeving.

Voorhangprocedure en UDO

Op de nadere regelgeving van de Cbw en Wwke komt een UDO en een voorhangprocedure, om ervoor te zorgen dat de regels zorgvuldig worden overwogen.

We constateren dat de consultatietekst van de Cbw en de Wwke nog veel onduidelijkheden bevat en dat verdere invulling door de wetgever zal plaatsvinden via Algemene Maatregelen van Bestuur en Ministeriële regelingen. Deze AMvB en ministeriële regelingen zijn op dit moment nog onbekend en zullen pas later dit jaar ter consultatie worden voorgelegd. Onder deze omstandigheden is er nog veel onduidelijkheid over de uitvoerbaarheid, haalbaarheid en betaalbaarheid van de Cbw en Wwke voor gemeenten en andere medeoverheden.

Wij benadrukken dat de UDO ook op de nadere regelgeving moet worden toegepast en dat gemeenten onder dat voorbehoud pas met de aangepaste/definitieve wet akkoord gaan. Daarnaast stellen wij voor om een controlemechanisme in de vorm van een voorhangprocedure in te bouwen waarbij belangrijke regels eerst door het parlement moeten worden goedgekeurd voordat ze definitief worden. Dit versterkt de democratische controle en zorgt ervoor dat de regels zorgvuldig worden overwogen. Deze procedure zou als volgt kunnen zijn:

- Voordat een AMvB kan worden vastgesteld op basis van de artikelen van de Cbw en Wwke, moet het ontwerp eerst vier weken voorgelegd worden aan de Eerste en Tweede Kamer.
- Als een van deze Kamers besluit niet akkoord te gaan met het ontwerp, dan kan de maatregel niet worden vastgesteld.
- In dat geval moet er ten minste zes weken gewacht worden voordat een nieuw ontwerp aan beide Kamers kan worden voorgelegd.

Vertrouwen

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

Afgelopen jaar 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.

Tot slot, wensen wij u alle goeds en succes in uw nieuwe functie.

Met vriendelijke groet,

mr L.K. (Leonard) Geluk

Algemeen Directeur