20240710_168_0002

Herengracht 23
2511 EG Den Haag
telefoon (070) 888 12 12
www.ipo.nl

Ministerie van Justitie en Veiligheid
T.a.v. de heer
Postbus 20301
2500 EH 's-GRAVENHAGE

Interprovinciaal Overleg

uw brief van	uw kenmerk	ons kenmerk	datum
-	-		8 juli 2024

onderwerp
Consultatiereactie IPO Cyberbeveiligingswet

Geachte ,

U heeft een consultatie geopend waarin de provincies zijn uitgenodigd om op uw conceptwetsvoorstel voor de Cyberbeveiligingswet (Cbw) te reageren. Het IPO geeft in deze brief reactie op dat concept.

De provincies vinden cyberbeveiliging essentieel voor moderne weerbaarheid van maatschappij en overheid tegen allerlei dreiging. Wij juichen daarom ook toe dat u de NIS2-richtlijn met de beoogde Cbw vertaald wordt in Nederlandse wetgeving.

Wij denken echter dat uw conceptwetsvoorstel voor de beoogde Cbw op punten verbeterd kan worden. In de consultatiereactie benoemen wij die verbeterpunten en stellen wij concrete aanpassingen van uw conceptwetsvoorstel voor die de verbeterpunten mogelijk kunnen verhelpen. Deze concrete aanpassingen zijn opgenomen in bijlage [1] *voorgestelde aanpassingen*.

De hoofdpunten zijn:

- Het doel van de NIS2-richtlijn zou niet voorbij geschoten moeten worden. Om de focus te houden op het daadwerkelijk beveiligen, roepen de provincies de wetgever op om de regeldruk te beperken.
- Neem de uitkomsten van de impactanalyse die de provincies uitvoeren als onderdeel van het UDO traject mee in het vervolg van uw wetgevingstraject. Houd hierbij rekening met de door de provincies benodigde financiële middelen bij het aanstellen van nieuwe en/of extra taken (zoals de wettelijke zorgplicht, meldplicht en registratieplicht, en de fysieke beveiliging van systemen).
- De Wet weerbaarheid kritieke entiteiten (Wwke) is gelijktijdig met de Cbw in consultatie gegaan. De provincies signaleren dat het normenkader en toetsingskader van de NIS2-richtlijn zijn anders dan het normenkader en toetsingskader van de CER, waardoor de provincies in de praktijk twee verschillende normenkaders en toetsingskaders moeten volgen.

Inlichtingen bij :
Email :
Bijlagen : 0

- Provincies vinden het 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 provincies omlaag gaat.
- Maak van de Cbw kernwetgeving en vermeld expliciet dat cyberbeveiliging een taak van algemeen nut is.
- Zorg dat de Cbw niet ingrijpt op de interne organisatiestructuur door taken bij cyberbeveiliging die de NIS2-richtlijn in essentie identificeert als taken van bestuur, niet neer te leggen bij 'de ambtelijke leiding' bij entiteiten zoals provincie.
- De provincies stellen voor om taal in de Cbw over gegevensverwerking – oftewel over uitwisseling en andere verwerking van informatie en gegevens (bijv. persoonsgegevens) – consistenter te laten zijn met taal daarover in vergelijkbare wetgeving.
- De provincies zien graag dat de Cbw expliciete grondslagen en kaders gaat omvatten voor gegevensverwerking bij die cyberbeveiliging. Waaronder voor uitwisseling van informatie tussen entiteiten zoals provincies onderling.
- Tot slot bepleiten wij dat daar waar de Cbw maakt dat 'bevoegde autoriteiten' entiteiten zoals provincies boetes kunnen geven bij niet-naleving van regels in de Cbw, de Cbw ook bepaalt dat zulke entiteiten niet voor dezelfde feiten boetes kunnen krijgen van meerdere autoriteiten tegelijk.

De provinciale consultatiereactie is als volgt opgebouwd:

1. Algemene reactie
2. Inhoudelijke reactie op het conceptwetsvoorstel en de memorie van toelichting
3. Bijlage [1] voorgestelde aanpassingen

1. Algemene reactie

1.1 Doel van de Cyberbeveiligingswet

In de Cbw wordt de Richtlijn (EU) 2016/1148 geïmplementeerd. Deze richtlijn wordt hierna aangeduid als de NIS2-richtlijn. De NIS2-richtlijn heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren. Deze richtlijn beoogt dit doel te bereiken door de verschillen weg te nemen die tussen lidstaten bestaan op het gebied van de cyberbeveiligingseisen die worden gesteld aan entiteiten die economisch belangrijke activiteiten of diensten verrichten.

Het conceptwetsvoorstel van de Cbw die nu voorligt, laat echter veel ruimte om nadere regels te stellen aanvullend aan de Cbw. Er wordt in de tekst uitvoerig verwezen naar lagere regelgeving die aanvullend door u wordt opgesteld. De vraag is of aanscherping van de huidige regels het gewenste doel gaat bereiken. Er lijkt vooral veel nadruk te liggen op het realiseren van controle, toezicht en handhaving, wat ten koste gaat van het daadwerkelijk beveiligen. Daarnaast worden de verschillen tussen de lidstaten op het gebied van cyberbeveiligingseisen door de beoogde Cbw niet weggenomen, maar juist versterkt door de nadere regels die gesteld kunnen worden in de lagere regelgeving. Deze nadere regels zorgen er tevens voor dat de regeldruk op provincies toeneemt, waardoor de focus op het voldoen aan de gestelde wet- en regelgeving komt te liggen in plaats van op het daadwerkelijke beveiligen.

De provincies verzoeken u om het opstellen van nadere regels in lagere regelgeving zoveel mogelijk te beperken. De focus zou moeten liggen op het daadwerkelijk beveiligen.

1.2 Uitvoerbaarheid Cbw (nog) onbekend

Doordat de uitwerking van de NIS2-richtlijn grotendeels in aanvullende lagere regelgeving plaats vindt, is er op dit moment nog veel onduidelijk over de impact die de Cbw gaat hebben op de provincies. Vanuit het traject Uitvoerbaarheidstoets Decentrale Overheden (UDO) laat het IPO een impactanalyse uitvoeren op de NIS2 richtlijn, en de doorwerking van deze in de nationale wetgeving. Omdat de invulling van de lagere regelgeving nog niet bekend is, worden er binnen de impactanalyse verschillende scenario's uitgewerkt.

Het ontbreken van de lagere regelgeving, waarin vooral de impact op provincies duidelijk wordt, maakt het tevens voor deze consultatiereactie ingewikkeld om de uitvoerbaarheid van de Cbw te toetsen. In het conceptwetsvoorstel wordt er veelvoudig verwezen naar verschillende aanvullende lagere regelgeving waarin nadere regels gesteld worden of kunnen worden. De provincies verzoeken u om ons tijdig op de hoogte te houden van de ontwikkelingen van de aanvullende lagere regelgeving, en ons hierbij ook zo snel mogelijk bij te betrekken.

Uit de impactanalyse die wij nu laten uitvoeren zal ook de voor de provincies benodigde financiële middelen duidelijk worden om aan de Cbw te kunnen voldoen. Wij gaan er vanuit dat de benodigde financiële middelen in het vervolg van dit wetgevingstraject worden meegenomen. En de kosten die de provincies zullen maken door het uitvoeren van nieuwe en/of extra taken (zoals de wettelijke zorgplicht, meldplicht en registratieplicht, en de fysieke beveiliging van systemen) vergoed zullen worden zoals in artikel 2 van de Financiële-verhoudingswet staat vermeld. Dit om te voorkomen dat provincies, en de andere medeoverheden, in financiële problemen komen. We zien dit graag verder uitgewerkt in het UDO-traject.

1.3 Samenhang met Europese wet- en regelgeving

Gelijktijdig aan de NIS2-richtlijn is de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad vastgesteld. De CER-richtlijn wordt in Nederland

2024/10-168-0005

geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (Wwke). Gezien de onderlinge verbanden tussen cyberbeveiliging en de weerbaarheid van entiteiten, bevatten de NIS2-richtlijn en de CER-richtlijn waarborgen om te zorgen voor een coherente samenhang tussen de richtlijnen. Daartoe regelt de NIS2-richtlijn dat entiteiten die uit hoofde van de CER-richtlijn worden aangewezen als kritieke entiteit, ook onder het toepassingsbereik van de NIS2-richtlijn vallen en automatisch als essentiële entiteit in de zin van de NIS2-richtlijn kwalificeren.

Wat de impact van de Wwke op de provincies gaat zijn, is op dit moment niet bekend. Er is vanuit het Rijk geen Uitvoerbaarheidstoets Decentrale Overheden (UDO) traject gestart, waardoor er geen impactanalyse uitgevoerd is. Als gevolg hiervan kunnen de provincies niet goed op de consultatie van de Wwke reageren. Wel signaleren de provincies het volgende probleem: het normenkader en toetsingskader van de NIS2-richtlijn zijn anders dan het normenkader en toetsingskader van de CER, waardoor de provincies in de praktijk twee verschillende normenkaders en toetsingskaders moeten volgen. Als normenkader wordt de BIO 2.0 gebruikt en geborgd in de Zorgplicht. De CER-richtlijn borduurt voort op het reeds bestaande DORA toetsingskader, waarbij IenW en ILT in de lead zijn. Als normenkader wordt de CSIR 3.0 gebruikt. Als we dit vertalen naar de provinciale situatie levert dit verwarring op over de reikwijdte van de wetten en een onnodig ingewikkelde implementatie. Provincies streven naar één integraal kwaliteitssysteem (voor ISMS/ CSMS) zoals ISO certificering met hooguit verschillende controls en maatregelen, door de uiteenlopende keuze voor normenkader en toetsingskader wordt het onnodig ingewikkeld gemaakt. Provincies vinden het 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 provincies 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 het UDO traject.

De NIS2-richtlijn is onderdeel van een set van wet- en regelgeving van de Europese Commissie om de digitale wereld, inclusief cyberbeveiliging, in een breed scala van kritieke sectoren te versterken. Naast de NIS2-richtlijn zijn er meerdere wetten en richtlijnen die vanuit de Europese Commissie in de Europese lidstaten van kracht zijn/worden of geïmplementeerd dienen te worden zoals: DORA, de AI Act, de Cyber Solidarity Act etc. Al deze wet- en regelgeving vertonen de nodige overlap.

De provincies roepen u op om aandacht te houden voor de complexiteit van de digitale transformatie en de ambitieuze plannen van Europa hierin. De regeldruk is voor provincies al ontzettend hoog en deze lijkt alleen maar verder toe te nemen, terwijl de provincies beperkte (personele) capaciteit hebben. Wij roepen de wetgever op om te vermijden dat de regeldruk toeneemt, en als deze toeneemt kritisch te kijken naar de (personele) capaciteit van de provincies en ons hierbij te ondersteunen. Belangrijk is hierbij dat de wetten (waar nodig) integraal worden opgepakt en samenhang wordt gezocht. Nu wordt er nog te veel gebruik gemaakt van verschillende begripsbepalingen, ambities etc. Dit is ook in lijn met de motie die recentelijk in de Eerste Kamer is aangenomen[1].

[1] Motie-Fiers (GroenLinks-PvdA) c.s. over diverse voorwaarden voor toetsing bij toekomstige digitaliseringswetgeving door de Eerste Kamer (36.382, D) - Eerste Kamer der Staten-Generaal

2024071016:0006

2. Inhoudelijke reactie op het conceptvoorstel en memorie van toelichting

2.1 Inrichting als kernwetgeving

Onder de beoogde Cbw worden bepaalde entiteiten, waaronder provincies, aangewezen als essentiële en belangrijke entiteiten. De Cbw gaat die entiteiten verplichten tot het realiseren van cyberbeveiliging, oftewel netwerk- en informatiebeveiliging, bij hun organisaties.

In de huidige nationale wetgeving bestaat er al wetgeving met regels over zulke netwerk- en informatiebeveiliging. Zoals de Wet digitale overheid (Wdo) en de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv). Deze bestaande wetgeving is echter verbrokkeld en omvat nog geen kernwetgeving. Het lijkt ons daarom verstandig dat de Cbw die kernwetgeving wordt. En dus (net als bijv. de Wdo) grondslagen gaat bieden voor het voorschrijven van bepaalde standaarden of generieke digitale infrastructuur. Zo creëert de beoogde Cbw in feite een stelsel van entiteiten die van centraal contactpunt, bevoegde autoriteiten, CSIRTS's en essentiële of belangrijke entiteiten zijn. Standaarden en generieke infrastructuur voor gegevensuitwisseling in dat stelsel kunnen veiligheid en betrouwbaarheid van die uitwisseling verbeteren.

Uw conceptwetsvoorstel voorziet echter nog niet in bepalingen om van de Cbw zulke kernwetgeving te maken. Daarom geven wij u in overweging om in uw conceptwetsvoorstel de aanpassingen te verwerken die wij vermelden in onderdeel één van de bijlage.

2.2 Cyberbeveiliging als taak

Hiervoor is al vermeld dat de beoogde Cbw een plicht tot cyberbeveiliging gaat omvatten voor entiteiten zoals provincies. Uit achtergronden bij de NIS2-richtlijn en de beoogde Cbw, is echter af te leiden dat die beveiliging ook duidelijk algemeen nut dient. Zo verlenen essentiële entiteiten, zoals provincies (zie ook hiervoor), maatschappelijk essentiële diensten. En beschermt cyberbeveiliging bij deze entiteiten niet alleen die entiteiten zelf, maar ook de continuïteit van die dienstverlening en dus de maatschappij als geheel.

Daarmee is cyberbeveiliging door entiteiten zoals provincies ook als taak van algemeen nut te duiden. En wij menen dat een expliciete vermelding hiervan in de Cbw zaken zal verbeteren zoals transparantie en privacyrechtelijke inpasbaarheid van gegevensverwerking bij de beveiliging. Zo zal het betekenen dat die verwerking ook duidelijk is te herleiden tot de zogeheten e-grond in artikel 6, eerste lid, van de Algemene Verordening Gegevensbescherming (AVG). En laat het zien dat cyberbeveiliging veel meer in taak is en niet slechts iets wat erbij wordt gedaan.

Daarom stellen wij voor dat u uw conceptwetsvoorstel aanpast door middel van de aanpassing die wij vermelden bij onderdeel twee van bijlage.

2.3 Governance

De NIS2-richtlijn bedoelt dat entiteiten zoals provincies cyberbeveiliging realiseren met (o.a.) allerlei 'beheermaatregelen'. Conform de richtlijn, bepaalt uw conceptwetsvoorstel dat besturen van deze entiteiten daarbij taken hebben. Namelijk het bepalen van de beheermaatregelen voor cyberbeveiliging die nodig zijn bij hun entiteiten (door 'goedkeuring van die maatregelen). En het controleren op concrete uitvoering van die beheermaatregelen (door 'toe te zien' op die uitvoering). Het idee bij dit type taken, zoals weergegeven in de NIS2-richtlijn, is (o.a.) dat cyberbeveiliging ook 'Chefsache' is. En dus ook bemoeienis noodzaakt van organen die organisaties besturen.

In systematiek bij de Provinciewet, besturen het (formele) provinciebestuur en organen daarvan een provinciale organisatie. En dit besturen van de organisatie door die organen (en dus door de leden van zulke organen) vindt ook plaats in de dagelijkse praktijk. Wij wensen dus dat de bepaling over taken voor besturen (zie hiervoor) ook geldt voor provincies. Uw conceptwetsvoorstel omvat echter

2024071-1888-0007

een bepaling waarmee u de betreffende taken weghaalt bij het provinciebestuur. Namelijk een bepaling (artikel 26, lid 8) waarmee u beoogt om die taken te laten aan ambtenaren die leiding geven in een provinciale organisatie ('ambtelijke leiding').

N.B.: in uw concept-Memorie van Toelichting bij de beoogde Cbw legt u uit waarom u, ook voor overheidsinstanties zoals provincies, de hiervoor bedoelde ambtelijke leiding-bepaling heeft opgenomen. Die uitleg komt erop neer dat u om meerdere redenen aanneemt dat niet past dat gekozen bestuurders van zulke overheidsinstanties de hiervoor bedoelde bemoeienis hebben met cyberbeveiliging. Wij vinden die redenen en aanname echter onjuist, om meerdere redenen. Ook omdat de NIS2-richtlijn lijkt te bedoelen dat zulke bemoeienis – kort gezegd – gewoon wordt in het licht van (toenemende) belangen bij cyberbeveiliging.

Daarnaast sluit het sanctioneren van een individuele functionaris van de ambtelijke leiding niet aan bij de manier waarop besluitvorming binnen provincies plaatsvindt. In provincies is er sprake van besluitvorming door de gedeputeerde staten en provinciale staten, wat conflicteert met persoonlijke sancties voor een ambtelijke leidinggevende of bestuurder. Daarom stellen wij voor om niet individuele functionarissen te sanctioneren, maar bestuursorganen volgens de Algemene wet bestuursrecht.

Wij verzoeken u dringend om de term 'bestuur' in lijn te brengen met de bestaande wettelijke definities zoals gehanteerd in de Provinciewet. In de systematiek van de Provinciewet is bepaald dat het (formele) provinciebestuur en organen daarvan een provinciale organisatie besturen. Dit vindt ook plaats in de dagelijkse praktijk. In onderdeel drie van de bijlage doen we hiervoor een concreet voorstel.

N.B.: De NIS2-richtlijn vereist niet dat de Cbw reguleert welke precieze organen die entiteiten besturen beheermaatregelen voor cyberbeveiliging bepalen en controleren. En uw conceptwetsvoorstel reguleert dit ook niet voor entiteiten zoals bedrijven. De eerste optie die wij schetsen komt erop neer dat u dit (dus) ook niet reguleert voor entiteiten die overheidsinstanties zoals provincies zijn. Zodat in de praktijk systematiek uit wetgeving zoals de Provinciewet leidend is bij toebedeling van de betreffende taken van bestuur aan concrete organen.

2.4 Consistent taalgebruik

Wij rekenen de beoogde Cbw tot weerbaarheidswetgeving. Waarmee wij doelen op wetgeving met grondslagen en kaders voor activiteiten op het vlak van weerbaarheid van overheid en maatschappij tegen allerlei dreiging. Die activiteiten omvatten ook gegevensverwerking. Oftewel verwerkingen van allerlei informatie en gegevens, zoals persoonsgegevens. Het is onpraktisch als wetten onnodig verschillen in taalgebruik over zulke zaken vertonen.

Het lijkt ons verstandig dat taalgebruik in de Cbw over uitwisseling en andere verwerking van informatie en gegevens, consistent gaat zijn met taalgebruik daarover in andere recente weerbaarheidswetgeving. Zoals met het taalgebruik daarover in de Wet coördinatie terrorismebestrijding en nationale veiligheid (Wctvn) en in de beoogde Wet gegevensverwerking door samenwerkingsverbanden (Wgs). In onderdeel vier van de bijlage doen we hiervoor concrete tekstvoorstellen.

N.B.: de aanpassingen betekenen wel dat taalgebruik in de beoogde Cbw gedeeltelijk gaat afwijken van taalgebruik in de NIS2-richtlijn. Wij menen echter dat Unierecht over implementatie van EU-richtlijnen (zoals de NIS2-richtlijn) hiervoor ruimte laat.

20240710_1800_0008

2.5 Gegevensverwerking bij cyberbeveiliging
Bij de verplichte cyberbeveiliging door entiteiten zoals provincies (zie hiervoor) kan gegevensverwerking nodig zijn. Bovendien kunnen dit indringende verwerkingen zijn. Hiermee bedoelen wij verwerkingen die, door de aard van de verwerking of verwerkte gegevens, relatief ver indringen in digitaal maatschappelijk verkeer of privacy.

Het lijkt ons daarom verstandig dat de Cbw bepalingen gaat omvatten met expliciete grondslagen en kaders voor gegevensverwerking bij cyberbeveiliging. Waarbij wij daarvoor als voorbeeld zien de bepalingen in de beoogde Wgs (zie hiervoor) over gegevensverwerkingen onder die wet. Ook omdat wij menen dat dergelijke (uitgebreide, precieze) bepalingen kunnen zorgen voor (betere) transparantie, maatschappelijk draagvlak, privacyrechtelijke inpasbaarheid en praktische handvatten bij indringende gegevensverwerking. In onderdeel vijf van de bijlage doen stellen we een aanpassing voor om dit in uw conceptwetsvoorstel aan te passen.

2.6 Horizontale uitwisseling
De beoogde Cbw bepaalt dat entiteiten die verplicht zijn tot realisatie van cyberbeveiliging (zoals provincies, zie hiervoor), die beveiliging een hoog niveau moeten geven. Bij de NIS2-richtlijn is bedoeld dat zulke entiteiten dit niveau ook bereiken door horizontale gegevensuitwisseling. Hiermee wordt bedoeld dat dergelijke entiteiten elkaar gegevens verstrekken over cyberbeveiliging. Zulke gegevensverstrekking kan worden aangemerkt als een vorm van indringende gegevensverwerking (zie hiervoor).
Uit de NIS2-richtlijn volgt dat voor die horizontale gegevensuitwisseling voorwaarde is dat entiteiten eerst met elkaar regelingen over zulke gegevensuitwisseling aangaan (in de richtlijn: informatie-uitwisselingsregelingen). Wij menen dat het de privacyrechtelijke inpasbaarheid van die regelingen en dergelijke gegevensuitwisseling vergroot als de Cbw nadrukkelijke grondslagen en kaders voor die regelingen omvat.

Het lijkt ons verstandig dat de Cbw ook bepalingen gaat omvatten met nadrukkelijke grondslagen en kaders voor de betreffende horizontale gegevensuitwisseling en regelingen daarover. Mede omdat de NIS2-richtlijn (art. 29) vereist dat lidstaten zulke horizontale gegevensuitwisselingen en regelingen concreet mogelijk maken. In onderdeel zes van de bijlage hebben wij hiervoor een voorstel gedaan.

2.7 Coördinatie boetes
De beoogde Cbw geldt voor entiteiten in allerlei sectoren in de maatschappij. En de beoogde Cbw geeft elke sector een eigen 'bevoegde autoriteit' die (o.a.) zorgt voor handhaving van regels uit de Cbw voor entiteiten zoals provincies. Waaronder voor het opleggen van de (grote) boetes die de beoogde Cbw mogelijk maakt. De provincie valt echter onder twee bevoegde autoriteiten. Namelijk als overheid onder de bevoegde autoriteit voor de sector Overheid. En als 'wegenautoriteit' onder de bevoegde autoriteit voor de sector Vervoer.

De bevoegde autoriteit voor de sector Overheid kan op haar beurt ook nog verschillen. In het kader van de AVG hebben de provincies namelijk met het toezicht van de Autoriteit Persoonsgegevens te maken, en in het kader van de NIS2 zijn de provincies onderhevig aan het (nog in te vullen) toezicht van de RDI. Dit leidt tot de vraag hoe de toezichthouders zich tot elkaar verhouden als er een cyberincident plaats vindt waarbij persoonsgegevens betrokken zijn.

Daarom wensen wij dat de beoogde Cbw een bepaling omvat die maakt dat een entiteit zoals een provincie niet voor dezelfde feiten zowel een boete ontvangt van de ene bevoegde autoriteit, als een boete van de andere bevoegde autoriteit. In onderdeel zeven van de bijlage doen wij hier een concreet tekstvoorstel die opgenomen kan worden in de conceptwetstekst.

2024071198 0009

2.8 Significante incidenten
De beoogde Cbw geeft weer dat entiteiten incidenten dienen te melden die een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of aanzienlijke materiële of immateriële schade veroorzaakt dat andere natuurlijke of rechtspersonen heeft getroffen of kan treffen. Het is echter onduidelijk wanneer een incident aan de vereisten van een significante incident voldoet. Wij verzoeken u om het nader te specificeren wat u onder significante incidenten verstaat door een betere maatstaf toe te voegen over wat een significant incident betreft.

De melding van incidenten gebeurt op twee punten, namelijk bij de toezichthouder en het CSIRT. De Cbw geeft aan dat deze dubbele meldplicht technisch zo ingericht wordt dat verspreiden van de nodige informatie door de entiteiten maar één handeling bedraagt. In de Memorie van Toelichting is er een berekening van toename van lastendruk, waarin uren en kosten zijn uitgewerkt, toegevoegd. Wij verzoeken u om toe te lichten waarop deze berekening is gebaseerd en of hierbij ook de lastendruk van de 24/7 piketdiensten zijn meegenomen.

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.

Bij onderdeel acht van de bijlage bij deze brief geven wij u een aanpassing in overweging mee.

2.9 Informatieverstrekking ten behoeve van nationale register
De beoogde Cbw stelt dat een essentiële of belangrijke entiteit en een entiteit die domeinnaamregistratiediensten verleent verstrekt ten behoeve van het in artikel 22 bedoelde nationale register, aan u de in artikel 45 bevraagde informatie dient te verstrekken.

Echter, zijn deze gegevens allemaal bij u bekend en zouden deze uit bestaande registraties gehaald kunnen worden. Dit zorgt voor lagere administratielasten voor de provincies en verlicht de regeldruk. PBLQ heeft voor Forum Standaardisatie onderzoek uitgevoerd *naar identificerende nummers voor organisaties* en geeft in haar aanbevelingen aan dat het zoveel mogelijk vermeden dient te worden dat gegevens op meerdere plekken worden opgeslagen. Registreer dus zo weinig mogelijk gegevens dubbel[2].

Tevens wekt dit vragen op voor gemeenschappelijke regelingen en samenwerkingsverbanden. Wie moet de gegevens aanleveren en wie is hiervoor verantwoordelijk?

Daarom geven wij u in overweging om in uw conceptwetsvoorstel de aanpassing te verwerken die wij vermelden bij onderdeel negen van de bijlage.

[2] FS-20240417.4A-Rapport-Verkenning-identificerende-nummers-voor-organisaties.pdf (forumstandaardisatie.nl)

20240710.1638-0010

Namens de provincies vertrouwen we erop dat u onze punten meeneemt in de definitieve versie van de Cbw en u onze zorgpunten betreffende de Wwke ter harte neemt.

Met vriendelijke groet,
INTERPROVINCIAAL OVERLEG

Algemeen Directeur

Bijlage [1] Voorgestelde aanpassingen

N.B.: tenzij anders vermeld, wordt met de vermelding van artikelnummers in de voorgestelde aanpassingen, gedoeld op de artikelnummering in uw conceptwetsvoorstel.

1. Inrichting als kernwetgeving

Met het oog op inrichting van de beoogde wet als kernwetgeving, stellen wij de volgende aanpassingen voor.

A.
Toevoeging aan artikel 1 van de volgende bepalingen:

- *aangewezen entiteiten*: entiteiten die bij of krachtens deze wet zijn aangewezen als:
a. centraal contactpunt;
b. bevoegde autoriteit;
c. CSIRT;
d. essentiële entiteit;
e. belangrijke entiteit.
- *beveiliging*: beveiliging van netwerk- of informatiesystemen;
- *beveiligingssystemen*: systemen voor beveiliging, of systeemcomponenten voor beveiliging;
- *gegevens*: informatie en gegevens, waaronder persoonsgegevens;
- *generieke infrastructuur*: generieke digitale infrastructuur als bedoeld in [het voorgestelde artikel in het hoofdstuk 'Generieke digitale infrastructuur] , eerste lid, van deze wet, met inbegrip van onderdelen van die infrastructuur zoals systemen en systeemcomponenten;
- *gevaar*: gevaar voor beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of diensten;
- *gevolgen van gevaar*: gevolgen of potentiële gevolgen van gevaar;
- *incidenten*: gebeurtenissen die een gevaar vormen voor gegevens die bij een entiteit berusten, of voor diensten die een entiteit aanbiedt of toegankelijk maakt via netwerk- of informatiesystemen.

B.
Invoeging na hoofdstuk 3 van de volgende twee hoofdstukken en artikelen per hoofdstuk.

B.1
Een hoofdstuk 'Algemene regels', met een artikel ('standaarden') met de volgende bepalingen:

1. Aangewezen entiteiten passen een ingevolge het tweede lid aangewezen standaard voor netwerk- en informatiebeveiliging toe, voor zover die standaard ingevolge het derde lid op hen van toepassing is.
2. Bij algemene maatregel van bestuur kan een standaard worden aangewezen, indien:
a. aanwijzing van die standaard noodzakelijk en proportioneel is gelet op:
- een hoog niveau van beveiliging;
- de mate of zwaarte van gevaar of gevolgen van gevaar;
- de goede werking, de veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid of de doelmatigheid van systemen voor beveiliging, of componenten van systemen voor beveiliging;
- uitvoering van verdragen of bindende besluiten van volkenrechtelijke organisaties.
b. de standaard tot stand is gekomen volgens een voor eenieder toegankelijke procedure; en
c. de standaard openbaar toegankelijk en kosteloos bruikbaar is en over de specificaties ervan blijvend vrijelijk kan worden beschikt of waarvan de specificaties blijvend kunnen worden verkregen tegen een redelijke vergoeding.

20240710 1936 0012

3. Bij algemene maatregel van bestuur wordt bepaald:
a. het functionele toepassingsbereik van een aangewezen standaard;
b. de organen waarvoor de verplichting tot toepassing van een aangewezen standaard geldt;
c. de datum waarop de verplichting tot toepassing van een aangewezen standaard ingaat.
4. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld.
5. Onze Minister kan een aanwijzing geven aan een entiteit waarvoor de verplichting tot toepassing van een aangewezen standaard geldt, indien de entiteit een gedragslijn hanteert die strijdig is met een aangewezen standaard.

B.2
Een hoofdstuk 'Generieke digitale infrastructuur', met een artikel met de volgende leden:

1. Onze Minister draagt zorg voor de inrichting van generieke digitale infrastructuur voor uitvoering van deze wet door aangewezen entiteiten, alsmede de beschikbaarstelling, instandhouding, werking en beveiliging van die infrastructuur.
2. De generieke infrastructuur bestaat tenminste uit infrastructuur voor veilige, betrouwbare en vertrouwelijke:
- gegevensuitwisseling tussen aangewezen entiteiten, met inbegrip van gegevensverstrekking tussen entiteiten die zijn aangewezen als essentiële entiteit of belangrijke entiteit;
- gegevensverstrekking aan betrokken personen.
3. Onze Minister bevordert de interoperabiliteit tussen de generieke infrastructuur en beveiligingssystemen bij aangewezen entiteiten.
4. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld met het oog op de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke infrastructuur.

C.
Vervanging van de bepaling in artikel 94 door de volgende bepaling:

Deze wet wordt aangehaald als: Algemene cyberbeveiligingswet.

2. Cyberbeveiliging als taak

Om in de beoogde Cbw uit te drukken dat cyberbeveiliging door essentiële en belangrijke entiteiten ook een taak van algemeen nut is, stellen wij de volgende aanpassingen voor.

A.
Toevoeging aan artikel 23 van een vijfde lid, met de volgende bepaling:

5. Het nemen van de maatregelen bedoeld in het eerste lid door essentiële en belangrijke entiteiten, wordt mede aangemerkt als vervulling door die entiteiten van een taak van algemeen nut als bedoeld in artikel 6, eerste lid, onder e, van de AVG.

3. Governance

Ter aanpassing van de bepaling waarmee u taken voor besturen van provincies niet neerlegt bij het formele provinciebestuur, maar ambtenaren, stellen wij de volgende optie voor.

2024071618-001

A.
Toevoeging aan artikel 1 van de volgende bepaling:

- *overheidsinstantie*: een overheidsinstantie als bedoeld in de NIS2-richtlijn.

B.
Vervanging van de bepaling in artikel 26, achtste lid, door de volgende twee bepalingen:

8. Voor de toepassing van het bepaalde bij of krachtens het tweede tot en met zesde lid worden als leden van het bestuur van een ministerie aangemerkt de leden van de ambtelijke leiding.
9. Voor zover bij andere wet dan deze wet aan een overheidsinstantie of orgaan daarvan de taak, verantwoordelijkheid of bevoegdheid is toegekend om een voorziening vast te stellen die mede is aan te merken als maatregel als bedoeld in het eerste lid, moet een dergelijke vaststelling mede worden aangemerkt als goedkeuring als bedoeld in dat lid.

4. Consistent taalgebruik

Om de beoogde Cbw te voorzien van taalgebruik dat consistenter is met taalgebruik in andere recente, nieuwe weerbaarheidswetgeving, stellen wij de volgende aanpassingen voor.

A.
Toevoeging aan artikel 1 van de volgende bepalingen:

- *gegevensuitwisseling*: uitwisseling van gegevens voor uitvoering van deze wet, met inbegrip van gegevensverstrekkingen tussen entiteiten die zijn aangewezen als essentiële entiteit of belangrijke entiteit.

B.
Vervanging van de term 'informatie' in artikelen in uw huidige conceptwetsvoorstel, waaronder van de term 'informatie' als onderdeel van bredere woorden, door de term 'gegevens'.

N.B.: zo wordt de term 'informatie-uitwisseling' dan bijvoorbeeld 'gegevensuitwisseling' (zie ook hiervoor).

C.
Gebruik van de term 'persoonsgegevens' waar specifiek wordt gedoeld op gegevens in de vorm van persoonsgegevens als bedoeld in de AVG.

N.B.: zo wordt, voor wat betreft verwerking van persoonsgegevens, een term als gegevensverwerking dan 'verwerking van persoonsgegevens'.

5. Gegevensverwerking bij cyberbeveiliging,
6. inclusief horizontale uitwisseling

Om de beoogde Cbw te voorzien van nadrukkelijke grondslagen en kaders voor verwerkingen van gegevens (waaronder persoonsgegevens) bij concrete cyberbeveiliging door essentiële en belangrijke entiteiten, stellen wij de volgende aanpassingen voor.

N.B.: in deze aanpassingen zijn ook bepalingen geïntegreerd met nadrukkelijke grondslagen en kaders voor 'horizontale gegevensuitwisseling, oftewel gegevensverstrekkingen tussen entiteiten die zijn aangewezen als essentiële of belangrijke entiteit, en voor regelingen tussen zulke entiteiten over dergelijke horizontale gegevensuitwisseling.

20240710.168.0014

A.
Toevoeging aan artikel 1 van de volgende bepaling:
- *regeling over gegevensverstrekking*: een regeling als bedoeld in [verwijzing naar het voorgestelde tweede artikel in paragraaf 15.2).

B.
Toevoeging aan hoofdstuk 15 van een paragraaf 15.1 ('Verwerking door essentiële en belangrijke entiteiten') met de volgende subparagrafen.

B.1
Een subparagraaf 15.1.1 ('Begripsbepaling') met een artikel met de volgende bepaling.

Voor toepassing van deze paragraaf wordt verstaan onder:
- *betrokkene*: een ieder die vanwege betrokkenheid bij uitvoering of toepassing van deze wet de beschikking heeft, krijgt of heeft gekregen over gegevens;
- *bewaring van gegevens*: bewaring en archivering van gegevens;
- *buitengewoon opsporingsambtenaar*: personen als bedoeld in artikel 142, eerste lid, onderdelen a tot en met c, van het Wetboek van Strafvordering;
- *deelnemers*: entiteiten die partij zijn bij een regeling over gegevensverstrekking;
- *dienstverleners en leveranciers*: dienstverleners en leveranciers van essentiële entiteiten of belangrijke entiteit, met inbegrip van dienstverleners met de hoedanigheid van:
a. een overheidsinstantie die diensten verleent aan een entiteit;
b. een samenwerkingsverband waaraan een entiteit deelneemt.
- *entiteit*: een essentiële entiteit of belangrijke entiteit;
- *geautomatiseerde analyse*: analyse van gegevens die wordt verricht zonder menselijke tussenkomst;
- *gegevensverwerking*: verwerking van gegevens als bedoeld in [het voorgestelde eerste artikel van subparagraaf 15.1.2, eerste lid] ;
- *gegevensverwerking door systemen*: gegevensverwerking door of met behulp of van systemen;
- *interne gegevensverwerking*: gegevensverwerking binnen een organisatie van een entiteit;
- *regeling over gegevensverstrekking*: een regeling of overeenkomst tussen entiteiten over gegevensverstrekking tussen entiteiten;
- *samenwerkingsverband*: samenwerkingsverband als bedoeld in de Wet gegevensverwerking door samenwerkingsverbanden.

B.2
Een subparagraaf 15.1.2 ('Grondslagen gegevensverwerking') met de volgende artikelen.

B.2.1
Een eerste artikel ('doelen') met de volgende bepalingen:

1. Entiteiten verwerken gegevens, waaronder persoonsgegevens, voor doelen bij deze wet en de bij of krachtens de wet aan hen toegekende verplichtingen en taken op het gebied van beveiliging.
2. Tot de doelen bedoeld in het eerste lid worden mede de volgende soorten specifieke doelen gerekend:
a. voorkoming van incidenten, detectie van incidenten, beheersing van incidenten, reactie op incidenten en herstel van incidenten;

b. verhoging van het niveau van informatiebeveiliging door onder meer:
- vergroting van bewustwording met betrekking tot cyberdreigingen;
- het beperken of belemmeren van het vermogen tot verspreiding van cyberdreigingen;
- een reeks verdedigingscapaciteiten;
- herstel en openbaarmaking van kwetsbaarheden;
- het opsporen van dreigingen;
- het ondersteunen van beheersings- en preventietechnieken, beperkingsstrategieën of respons- en herstelfasen;
- het bevorderen van gezamenlijk onderzoek naar cyberdreigingen door entiteiten.

B.2.2
Een tweede artikel ('soorten verwerkingen') met de volgende bepalingen:

1. Gegevensverwerking kan bestaan uit elk soort verwerking dat noodzakelijk is in verband met doelen en verplichtingen of taken als bedoeld in [het voorgestelde eerste artikel van subparagraaf 15.1.2] , met inbegrip van:
a. interne gegevensverwerking;
b. gegevensverstrekking aan derden;
c. gegevensverwerking door systemen, met inbegrip van:
- geautomatiseerde verwerking van persoonsgegevens;
- geautomatiseerde analyse, waaronder geautomatiseerde analyse van persoonsgegevens.
2. Gegevensverwerking aan derden kan onder meer bestaan uit:
a. gegevensverstrekking aan:
- een centraal contactpunt;
- een bevoegde autoriteit; of
- een CSIRT.
b. gegevensverstrekking aan een dienstverlener of leverancier;
c. gegevensverstrekking tussen entiteiten.

B.2.3
Een derde artikel ('soorten gegevens') met de volgende bepalingen:

1. Gegevensverwerking kan bestaan uit verwerking van elke soort gegevens waarvan het verwerken noodzakelijk is in verband met doelen en verplichtingen en taken als bedoeld in [het voorgestelde eerste artikel van subparagraaf 15.1.2] .
2. Gegevens als bedoeld in het eerste lid, kunnen mede bestaan uit gevoelige gegevens, waaronder tenminste te rekenen gegevens als bedoeld in het derde tot en met zevende lid, voor zover van toepassing.
3. Gegevens als bedoeld in het eerste lid kunnen mede bestaan uit gegevens over cyberdreigingen, bijna-incidenten, kwetsbaarheden, methoden en technieken, procedures, indicatoren voor aantasting, vijandige tactieken, cyberbeveiligingswaarschuwingen en aanbevelingen over configuratie van beveiligingssystemen om cyberaanvallen te detecteren.
4. Gegevens als bedoeld in het eerste lid kunnen mede bestaan uit persoonsgegevens, met inbegrip van:
- persoonsgegevens die oorspronkelijk zijn vergaard of samengesteld voor andere doelen dan de doelen bedoeld in [het voorgestelde eerste artikel van subparagraaf 15.1.2] ;
- bijzondere persoonsgegevens;
- persoonsgegevens in de vorm van dreigingsactorspecifieke gegevens, IP-adressen, domeinnamen, URL's, referrer-URL's en persoonlijke HTML-pagina's, e-mailadressen, logbestanden en gegevens in persoonlijke berichten.

5. Bij entiteiten die buitengewoon opsporingsambtenaren tewerkstellen, kunnen gegevens als bedoeld in het eerste lid mede bestaan uit persoonsgegevens van strafrechtelijke aard.
6. Bij entiteiten die bestuursorganen zijn als bedoeld in artikel 3, eerste lid, van de Wet bevordering integriteitsbeoordeling door het openbaar bestuur, of die mede bestaan uit dergelijke organen, kunnen gevoelige gegevens als bedoeld in het eerste lid mede bestaan uit gegevens, waaronder persoonsgegevens, uit onderzoek door deze bestuursorganen op grond van die wet.
7. Bij entiteiten die deelnemers aan een samenwerkingsverband zijn, of die mede bestaan uit dergelijke deelnemers, kunnen gevoelige gegevens als bedoeld in het eerste lid mede bestaan uit gegevens, waaronder persoonsgegevens, uit activiteit van of in een dergelijk verband.

B.2.4
Een vierde lid artikel ('nadere regels') met de volgende bepalingen:

Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot gegevensverwerking, met inbegrip van regels over:
- soorten specifieke doelen bij de gegevensverwerking;
- soorten gegevens die kunnen worden verwerkt bij de gegevensverwerking;
- soorten verwerkingen waaruit de gegevensverwerking kan bestaan.

B.3
Een subparagraaf 15.1.3 ('Waarborgen') met de volgende artikelen.

B.3.1
Een eerste artikel ('noodzakelijkheid') met de volgende bepalingen:

Entiteiten verwerken gegevens uitsluitend voor zover een verwerking:
a. noodzakelijk is in verband met doelen en verplichtingen of taken als bedoeld in [het voorgestelde eerste artikel van subparagraaf 15.1.2];
b. niet in strijd is met een geheimhoudingsbepaling bij of krachtens de wet.

B.3.2
Een tweede artikel ('gegevensverstrekking') met de volgende bepalingen:

1. Gegevensverstrekking als bedoeld in [het voorgestelde tweede artikel van subparagraaf 15.1.2], tweede lid, onder a, vindt uitsluitend plaats voor zover dit noodzakelijk is met het oog op:
a. het indienen bij een CSIRT of de bevoegde autoriteit of autoriteiten van de gegevens bedoeld in de artikelen 28 tot en met 31 en artikel 35;
b. het informeren van afnemers van diensten als bedoeld in artikel 32;
c. het indienen van informatie in verband met sectorspecifieke rechtshandelingen als bedoeld in artikel 33;
d. kennisgeving aan natuurlijke personen of rechtspersonen op aanwijzing van een bevoegde autoriteit of autoriteiten als bedoeld in artikel 40;
e. toezicht of handhaving door een bevoegde autoriteit als bedoeld in hoofdstuk 15 van deze wet;
f. taken van een CSIRT als bedoeld in artikel 17, tweede lid, onder a tot en met e, en derde lid, van deze wet.
2. Gegevensverstrekking als bedoeld in [het voorgestelde tweede artikel van subparagraaf 15.1.2], tweede lid, onder c, omvat uitsluitend gevoelige gegevens als bedoeld in [het voorgestelde derde artikel van subparagraaf 15.1.2], tweede lid, voor zover:
a. de verstrekkende entiteit en de ontvangende entiteit beiden deelnemer zijn in eenzelfde regeling over gegevensverstrekking; en
b. wordt voldaan aan elk van de eisen in [het voorgestelde tweede, derde en vierde artikel in paragraaf 15.1.4].

C

B.3.3
Een derde artikel ('verwerkingen door systemen') met de volgende bepalingen:

1. Bij gegevensverwerking door een systeem, zorgt een entiteit ervoor dat uitsluitend geautoriseerde personen toegang hebben tot het systeem.
2. Een entiteit onderhoudt een geordend geheel van autorisaties van personen als bedoeld in het tweede lid.
3. Bij autorisatie als bedoeld in het tweede lid, autoriseert een entiteit slechts personen die zijn aangewezen voor:
a. uitvoering of uitoefening van relevante verantwoordelijkheden;
b. uitvoering van toezicht op grond van andere wet- of regelgeving dan deze wet over informatiebeveiliging of gegevensverwerking;
c. beheer of onderhoud van systemen.
4. Een entiteit zorgt voor vastlegging langs elektronische weg (logging) van gegevensverwerkingen door een systeem.
5. Gegevens die worden vastgelegd vanwege het vierde lid, worden uitsluitend gebruikt voor:
a. controle van de rechtmatigheid van de gegevensverwerking;
b. intern toezicht;
c. waarborging van de integriteit en de beveiliging van de persoonsgegevens; of
d. gerechtelijke procedures.

B.3.4
Een vierde artikel ('geautomatiseerde analyse') met de volgende bepalingen:

1. Bij geautomatiseerde analyse wordt voldaan aan de volgende eisen:
a. de gegevens die bij de analyse worden verwerkt, zijn juist en volledig;
b. de analyse heeft een goede kwaliteit;
c. bij de analyse worden uitsluitend algoritmes gebruikt waarvan de uitkomsten navolgbaar en controleerbaar zijn;
d. een resultaat van de analyse wordt uitsluitend verwerkt nadat door menselijke tussenkomst is beoordeeld of het resultaat zorgvuldig tot stand is gekomen.
e. de analyse vindt plaats op zodanige wijze dat na bij of krachtens de wet algemene maatregel van bestuur te bepalen fasen, gebruikte gegevens niet meer zijn te herleiden tot specifieke personen, behoudens met gebruik van aanvullende gegevens;
f. gegevens die zijn verwerkt door geautomatiseerde analyse, zijn door gebruik van aanvullende gegevens als bedoeld onder e altijd weer te koppelen aan een betrokken persoon;
g. aanvullende gegevens als bedoeld onder e worden afzonderlijk bewaard;
h. toegang door onbevoegden tot aanvullende gegevens als bedoeld onder e is uitgesloten.
i. Een entiteit koppelt gegevens die zijn verwerkt door geautomatiseerde analyse, uitsluitend opnieuw aan een betrokken persoon voor zover die gegevens op basis van resultaten van de analyse duiden op gevaar.
2. Onverminderd verplichtingen uit de AVG tot verstrekking van informatie over verwerkingen van persoonsgegevens, verschaft een entiteit bij geautomatiseerde analyse op toegankelijke wijze uitleg aan het publiek over de gehanteerde patronen en indicatoren of andere onderliggende logica.
3. Bij toepassing van het vierde lid zijn de uitzonderingsgronden uit de Wet open overheid van overeenkomstige toepassing.

B.3.5
Een vijfde artikel ('anonimisering, einde verwerking en correctie') met de volgende bepalingen.

1. Gegevens die worden verwerkt vanwege op grond van deze paragraaf, worden:

a. niet verder verwerkt zodra dit niet langer noodzakelijk is voor relevante doelen;
b. geanonimiseerd zodra bewaring in niet-geanonimiseerde vorm niet langer noodzakelijk is voor relevante doelen;
c. verwijderd uit systemen in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking;
d. vernietigd zodra bewaring of bewaring in geanonimiseerde vorm niet langer noodzakelijk is voor relevante doelen.
2. Onverminderd het eerste lid, worden gegevens waarvan tijdens geautomatiseerde analyse blijkt dat ze onjuist zijn, onverwijld gecorrigeerd.
3. Voor zover onjuiste gegevens als bedoeld in het tweede lid afkomstig zijn van een derde, meldt de entiteit waarbij de gegevens berusten, de gebleken onjuistheid ook aan die derde.
4. Een entiteit kan van het eerste tot en met derde lid afwijken voor zover dit noodzakelijk is voor:
a. het voldoen aan een voorschrift uit andere wet- of regelgeving dan deze wet; of
b. het instellen, uitoefenen of onderbouwing van een rechtsvordering.

B.3.6
Een zesde artikel ('Geheimhouding') met de volgende bepalingen:

1. Onverminderd verplichtingen tot geheimhouding van persoonsgegevens die al toepasselijk zijn uit hoofde van ambt, beroep of voorschrift uit andere wetgeving, is een betrokkene gehouden tot geheimhouding van persoonsgegevens waarover hij beschikt vanwege zijn betrokkenheid bij uitvoering of toepassing van deze wet.
2. Het eerste lid is niet van toepassing voor zover:
a. een verplichting of bevoegdheid tot gegevensverstrekking bestaat vanwege een bepaling in deze wet, in nadere regels die op grond van deze wet zijn vastgesteld bij of krachtens een algemene maatregel van bestuur, of in andere wetgeving.
b. gegevensverstrekking noodzakelijk is voor het afleggen van verantwoording in verband met toezicht op grond van deze wet, waaronder intern toezicht.
3. Het eerste lid is van overeenkomstige toepassing voor zover een betrokkene door betrokkenheid bij uitvoering of toepassing van deze wet beschikt over gegevens die geen persoonsgegevens zijn, maar waarvan een betrokkene het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, waaronder gegevens waarover een betrokkene beschikt vanwege betrokkenheid bij een audit of inspectie.

B.3.7
Een zevende artikel ('nadere regels') met de volgende bepalingen:

Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld met waarborgen bij gegevensverwerking.

B.3.8
Een achtste artikel ('beheermaatregelen') met de volgende bepaling:

Een entiteit neemt adequate technische, operationele en organisatorische maatregelen om te bewerkstelligen dat wordt voldaan aan verplichtingen in deze subparagraaf en aan nadere regels als bedoeld in [het voorgestelde zevende artikel van subparagraaf 15.1.3] .

B.4
Een subparagraaf 15.1.4 ('Regelingen over gegevensverstrekkingen tussen entiteiten') met de volgende artikelen.

2024071.0.168.0015

B.4.1
Een eerste artikel ('begripsbepaling') met de volgende bepalingen:

Voor toepassing van deze subparagraaf wordt verstaan onder:
- *deelnemers*: entiteiten die partij zijn bij een regeling over gegevensverstrekking;
- *gegevensverstrekking*: gegevensverstrekking tussen entiteiten;
- *geautoriseerde persoon*: een natuurlijke persoon die door een ontvangende entiteit is gemachtigd tot kennisname van verstrekte gegevens, of is geautoriseerd om toegang te nemen tot systemen waarin zich dergelijke gegevens bevinden;
- *ontvangende entiteit*: een entiteit die bij gegevensverstrekking gegevens ontvangt;
- *verstrekkende entiteit*: een entiteit die bij gegevensverstrekking gegevens verstrekt;
- *verstrekte gegevens*: gegevens die een verstrekkende entiteit verstrekt of heeft verstrekt aan een ontvangende entiteit;
- *wettelijke verplichting*: een verplichting uit Unierecht of bij of krachtens de wet.

B.4.2
Een tweede artikel ('algemeen') met de volgende bepalingen:

1. Entiteiten kunnen met elkaar regelingen over gegevensverstrekkingen overeenkomen.
2. Een regeling over gegevensverstrekking heeft tenminste betrekking op verstrekking tussen entiteiten van gevoelige of potentieel gevoelige gegevens als bedoeld in [het voorgestelde derde artikel van paragraaf 15.1.2).
3. In een regeling over gegevensverstrekking bepalen deelnemers dat:
- de gegevensverstrekking waarover de regeling gaat, een vrijwillig karakter heeft;
- de regeling voor het overige een regeling is die deelnemers ten aanzien van elkaar bindt.

B.4.3
Een derde artikel ('persoonsgegevens') met de volgende bepalingen:

1. Een regeling over gegevensverstrekking omvat ten minste bepalingen over:
a. de soorten persoonsgegevens die deelnemers elkaar kunnen verstrekken;
b. de aard van de verwerkingen door een ontvangende entiteit van verstrekte persoonsgegevens;
d. waarborgen bij verwerkingen door een ontvangende entiteit van verstrekte persoonsgegevens.
2. Bepalingen als bedoeld in het eerste lid omvatten ten minste de volgende bepalingen:
a. de ontvangende entiteit neemt ten aanzien van verstrekte persoonsgegevens artikel 32 van de AVG in acht;
b. de ontvangende entiteit waarborgt dat geautoriseerde personen zich ertoe verbinden dat zij vertrouwelijkheid in acht nemen bij kennisname van verstrekte persoonsgegevens;
c. de ontvangende entiteit geeft verstrekte persoonsgegevens niet door aan derden die geen deelnemers zijn aan de regeling, waaronder niet aan een derde land of internationale organisatie, tenzij een doorgifte strekt tot uitvoering van een wettelijke verplichting;
d. in geval van een doorgifte als bedoeld onder c door de ontvangende entiteit, stelt de ontvangende entiteit de verstrekkende entiteit voorafgaand aan de doorgifte in kennis van de doorgifte, tenzij een wettelijke verplichting aan die kennisgeving in de weg staat;
e. de ontvangende entiteit en de verstrekkende entiteit verlenen elkaar, ten aanzien van verstrekte gegevens en voor zover redelijkerwijze nodig en mogelijk, bijstand bij:
- het voldoen aan hun verplichtingen uit hoofde van de rechten van personen bedoeld in hoofdstuk III van de AVG;
- het aantonen, waaronder bij audits of inspecties, van nakoming van verplichtingen uit dit artikel.
3. Een regeling over gegevensverstrekking voldoet aan bij of krachtens algemene maatregel van bestuur gestelde nadere eisen over de inhoud van regelingen voor gegevensverstrekking.

2024007110 - 168 - 0047

B.4.4
Een vierde artikel ('kennisgeving regeling') met de volgende bepalingen:

1. Indien een entiteit een regeling over gegevensverstrekking aangaat, stelt de entiteit de bevoegde autoriteit of autoriteiten daarvan in kennis.
2. Indien een entiteit haar deelname aan een regeling over gegevensverstrekking beëindigt, stelt de entiteit de bevoegde autoriteit of autoriteiten daarvan in kennis zodra de beëindiging van kracht wordt.

7. Coördinatie boetes

Om te voorkomen dat bij handhaving van de beoogde Cbw – kort gezegd – meerdere bevoegde autoriteiten elk een boete opleggen voor dezelfde feiten, stellen wij voor dat u aan artikel 77 een zevende lid toevoegt, met de volgende bepaling:

7. In geval bij een overtreding van het bepaalde bij of krachtens deze wet meerdere bevoegde autoriteiten bevoegd zijn tot toepassing van het eerste lid of tweede lid, coördineren deze bevoegde autoriteiten die toepassing zodanig dat niet voor dezelfde feiten meer dan één bevoegde autoriteit een boete oplegt.

Tevens stellen wij voor om in artikel 77, ook te verwijzen naar artikel 59, zodat duidelijk wordt dat er ook geen dubbele boete opgelegd kan worden door de Autoriteit Persoonsgegevens en de bevoegde autoriteit(en) van de Cbw.

8. Significante incidenten
Om te bepalen of een incident significant is, zijn in artikel 27, derde lid, NIS2-richtlijn drie parameters opgenomen. In artikel 37 is een delegatiegrondslag opgenomen om bij of krachtens een AMvB de meldplicht verder uit te werken en kan gebruikt worden om de parameters nader in te vullen en regels vast te stellen over aanvullende parameters.

Wij geven u in overweging mee om de parameters door middel van classificatie of taxonomie nader te specificeren en deze af te stemmen met de Rijks-SOC's en de SOC's van de essentiële entiteiten. Dit is in lijn met artikel 17 zesde lid.

9. Informatieverstrekking ten behoeve van nationale register
Wij verzoeken u om bij artikel 45 zevende lid toe te voegen dat de gegevens zoveel mogelijk gehaald worden uit bestaande registraties.

20240710.168.0018

Herengracht 23
2511 EG Den Haag

Interprovinciaal Overleg

FMHaaglanden
09 JULI 2024
Ontvangen

Gezien scankamer
JenV
09 JULI 2024