Raad van State

No. W16.24.00336/II 's-Gravenhage, 19 februari 2025

Bij Kabinetsmissive van 6 december 2024, no.2024002833, heeft Uwe Majesteit, op voordracht van de Minister van Justitie en Veiligheid, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende de regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet), met memorie van toelichting.

Het wetsvoorstel implementeert de NIS2-richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU. Belangrijke maatschappelijke of economische processen vereisen adequate bescherming tegen cyberbeveiligingsrisico's. Met het oog op dit doel bepaalt het voorstel voor welke belangrijke en essentiële entiteiten verplichtingen van toepassing zijn om enerzijds dergelijke risico's te beheersen en incidenten te voorkomen en anderzijds de gevolgen van incidenten te beperken. Die verplichtingen omvatten onder meer een zorgplicht om maatregelen te nemen om cyberbeveiligingsrisico's te beheersen en een meldplicht bij significante incidenten.

De implementatie van de richtlijn moet worden ingebed in bestaande structuren waarin verschillende partijen verantwoordelijkheden hebben op het gebied van cyberbeveiliging. Het gaat om een ruim aantal partijen omdat de reikwijdte van het voorstel zich uitstrekt over uiteenlopende maatschappelijke en economische activiteiten; de verwachting is dat ruim 8000 entiteiten onder de wet zullen komen te vallen.[1] Cyberbeveiliging is een sector-overstijgend onderwerp. Het is in die situatie van belang dat duidelijk is wie waarvoor verantwoordelijk is, zowel wat betreft de instanties die het voorstel moeten uitvoeren als de entiteiten waarop het voorstel van toepassing is.

De diversiteit van de entiteiten waarop het voorstel van toepassing is brengt mee dat per sector en, tot op zekere hoogte, per entiteit, moet worden beoordeeld op welke wijze cyberbeveiligingsrisico's dienen te worden vermeden of beheerst. Dit vergt onder meer betrokkenheid van de vakministers, die worden aangewezen als bevoegde autoriteit. Tegelijkertijd kent het voorstel aan de minister van Justitie en Veiligheid een coördinerende rol toe.

De Afdeling advisering van de Raad van State adviseert om nader in te gaan op de wijze waarop invulling wordt gegeven aan de coördinerende taak en de (mede)betrokkenheid van de minister van Justitie en Veiligheid.

De Afdeling wijst erop dat de aan de vakministers toegekende bevoegdheid om toezicht te houden op cyberbeveiliging kan raken aan bevoegdheden die aan zelfstandige bestuursorganen zijn toegekend om voor bepaalde entiteiten toe te zien op de veiligheid (waaronder cyberbeveiliging). Het is van belang om te zorgen voor een

[1] Memorie van toelichting, algemeen deel, paragraaf 8.1.1, 'Inleiding'; overheidsinstanties zijn daarin niet meeberekend.

AAN DE KONING

duidelijke taakafbakening tussen vakministers en deze zelfstandige bestuursorganen om problemen door overlapping van bevoegdheden te vermijden.

De Afdeling adviseert om in het wetsvoorstel zoveel mogelijk te verduidelijken welke overheidsinstanties zijn uitgezonderd van het voorstel omdat zij activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving. De Afdeling adviseert bovendien om te verduidelijken of, en zo dit het geval is, op welke wijze, ten aanzien van het toezicht op de sector overheid wordt voldaan aan het vereiste van voldoende onafhankelijk toezicht, en zo nodig het voorstel aan te passen.

In verband met deze opmerkingen is aanpassing wenselijk van het wetsvoorstel en de toelichting.

1. Achtergrond en inhoud voorstel Cyberbeveiligingswet

a. *Implementatie NIS2-richtlijn, verhogen cyberbeveiliging, en samenhang CER-richtlijn*

Het wetsvoorstel is gericht op het verhogen van de cyberbeveiliging van belangrijke maatschappelijke of economische functies of activiteiten. Cyberbeveiliging spitst zich enerzijds toe op het beheersen van risico's en het voorkomen van incidenten en anderzijds het beperken van de gevolgen van incidenten.[2] Bedreigingen van de cyberbeveiliging kunnen afkomstig zijn van kwaadwillende statelijke en niet-statelijke actoren, bijvoorbeeld in de vorm van sabotage of een zogenoemde ransomware-aanval.[3] Maar zij kunnen ook voortvloeien uit kwetsbaarheden of technische fouten in het netwerk- en informatiesysteem, zoals bijvoorbeeld de uitval van deze systemen als gevolg van een foutieve update in de Crowdstrike-software.

Als illustratie van de ernst en omvang die cyberincidenten kunnen aannemen een citaat uit *Cybersecuritybeeld Nederland 2024*

"Op 19 juli introduceerde CrowdStrike een software-update die ervoor zorgde dat er wereldwijd zo'n 8,5 miljoen Windowssystemen onbruikbaar werden. De fout zorgde voor 'Blue Screens of Death' op Windowssystemen. Dit zorgde wereldwijd voor grote problemen, zo ook in Nederland. Schiphol annuleerde vluchten en in sommige ziekenhuizen werd de zorg afgeschaald. Ook delen van de overheid werden geraakt. Zo ondervonden het ministerie van Buitenlandse Zaken en het UWV hinder van de storing".[4]

Het wetsvoorstel treedt in de plaats van de Wet beveiliging netwerk- en informatiesystemen (Wbni), waarmee de richtlijn inzake maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de

[2] Vergelijk voorgesteld artikel 2 Cbw.
[3] De versleuteling van bestanden van het slachtoffer door criminelen die tegen betaling van losgeld weer wordt ontsleuteld.
[4] *Cybersecuritybeeld Nederland 2024* (Rapport NCTV), bijlage bij Kamerstukken II 2024/25, 26643, nr. 1229, p. 27.

EU (NIS1-richtlijn) is geïmplementeerd.[5] Uit een evaluatie van die richtlijn kwam een aantal tekortkomingen naar voren.[6] Om die reden is de NIS2-richtlijn vastgesteld betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU.[7] Het wetsvoorstel implementeert de NIS2-richtlijn. De implementatietermijn is op 17 oktober 2024 verstreken.

De doelstelling en systematiek van de NIS2-richtlijn hangt nauw samen met die van de gelijktijdig vastgestelde CER-richtlijn. Het voorstel voor een Wet weerbaarheid kritieke entiteiten (Wwke) implementeert de CER-richtlijn.[8] De Afdeling brengt over beide implementatievoorstellen gelijktijdig advies uit. De CER-richtlijn en de Wwke hebben uitsluitend betrekking op de fysieke weerbaarheid van kritieke entiteiten. Indien een entiteit op basis van de Wwke een kritieke entiteit is, is die entiteit van rechtswege een essentiële entiteit waarop het voorstel voor een Cyberbeveiligingswet (hierna: Cbw) van toepassing is.

b. *Hoofdlijnen voorstel Cbw*

Het wetsvoorstel bevat verplichtingen op het gebied van cyberbeveiliging voor bepaalde publieke en private organisaties, die opereren in economische sectoren en diensten aanbieden die van vitaal belang zijn. Daarbij wordt een onderscheid gemaakt tussen “essentiële” en “belangrijke” entiteiten. Het wetsvoorstel is van rechtswege, of na een daartoe strekkende aanwijzing, op entiteiten van toepassing. Omdat er meer risico’s zijn wat betreft de cyberbeveiliging van essentiële entiteiten, is op deze entiteiten een strenger toezichtsregime van toepassing dan voor belangrijke entiteiten.[9]

Voor essentiële en belangrijke entiteiten geldt allereerst een zorgplicht.[10] Deze plicht is erop gericht dat entiteiten maatregelen nemen om risico’s te beheersen en incidenten te voorkomen, of de gevolgen daarvan te beperken. Het wetsvoorstel bevat een opsomming van maatregelen die in dit verband in elk geval verplicht zijn. Verdere invulling van de zorgplicht zal plaatsvinden door de entiteiten zelf, eventueel met behulp van sectorspecifieke voorschriften die worden gesteld in een EU-rechtshandeling, of bij of krachtens algemene maatregel van bestuur.[11]

---

[5] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).

[6] Zie de impact assessment van de Europese Commissie, 16 december 2020, SWD(2020) 345 final, bijlage 5.

[7] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (PbEU 2022, L 333). De afkorting NIS is afkomstig van de aanduiding van de vorige richtlijn ten aanzien van netwerk- en informatiesystemen.

[8] Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten (PbEU 2022, L 333). De afkorting is afkomstig van de Engelstalige aanduiding van de richtlijn die verwijst naar ‘*critical entities’* en ‘*resilience’.*

[9] Vergelijk paragrafen 15.2 en 15.3, in het bijzonder voorgesteld artikel 80, Cbw.

[10] Voorgesteld artikel 21 Cbw.

[11] Voorgesteld artikel 21, vijfde lid, en artikel 22, Cbw; memorie van toelichting, algemeen deel, paragraaf 5.2, ‘Zorgplicht’, waar de eigen verantwoordelijkheid voor het vaststellen van de maatregelen ter uitwerking van de zorgplicht wordt onderstreept.

Daarnaast geldt voor essentiële en belangrijke entiteiten een meldplicht.[12] Op basis van deze plicht moeten entiteiten gefaseerd – dat wil zeggen van vroegtijdige waarschuwing tot eindverslag – melding doen van een “significant incident” bij zowel het CSIRT (computer security incident response team) als de bevoegde autoriteit (de verantwoordelijke minister).[13] Met het wetsvoorstel gelden ook verplichtingen voor leden van het bestuur van de entiteiten. Zij moeten zorgplichtmaatregelen goedkeuren en toezien op de uitvoering daarvan. Tevens dienen zij een opleiding te volgen om voldoende kennis te hebben van risico’s op het gebied van cyberbeveiliging.[14]

Voor de goede uitvoering van het wetsvoorstel zijn een aantal instanties verantwoordelijk. Zeven vakministers worden bij wet aangewezen als bevoegde autoriteit, met de taak om toezicht te houden op de naleving van de verplichtingen door entiteiten, actief in sectoren of subsectoren die onder de beleidsverantwoordelijkheid van de betreffende vakminister vallen.[15] CSIRT’s zijn verantwoordelijk voor het verlenen van bijstand aan entiteiten in het geval van een cyberincident.

2. Afbakening van de reikwijdte

De richtlijn is niet van toepassing op “overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.”[16] Deze bepaling uit de richtlijn is vrijwel letterlijk overgenomen in het voorstel voor de Cbw. Om welke organisaties het precies gaat wordt echter niet verder uitgewerkt.[17] Volgens de toelichting zal het wetsvoorstel niet gelden voor “onder andere” de veiligheidsregio’s, het ministerie van Defensie, het openbaar ministerie en de politie.[18] Overheidsinstanties waarvan de activiteiten slechts zijdelings verband houden met nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving zullen via ontheffingen van de eerstverantwoordelijke minister worden uitgezonderd van de verplichtingen voorzien in het wetsvoorstel.[19]

De woorden “onder andere”, die in de toelichting worden gebruikt, roepen de vraag op welke overheidsinstanties nog meer geacht worden onder deze uitzondering te vallen. Zo is onduidelijk of de inlichtingen- en veiligheidsdiensten onder deze uitzondering moeten worden begrepen. Daarnaast is de vraag of het de bedoeling is dat de diensten, bedoeld in de Wet op de bijzondere opsporingsdiensten, onder de uitzondering zullen vallen.

---

[12] Voorgesteld artikel 25 Cbw.
[13] Er is tevens de mogelijkheid tot het doen van een vrijwillige melding in geval van incidenten, bijna-incidenten en cyberdreigingen, zie voorgesteld artikel 33 Cbw.
[14] Voorgesteld artikel 24 Cbw.
[15] Zie de definitie in het voorgestelde artikel 1 Cbw en artikel 8, eerste lid, van de NIS2-richtlijn.
[16] Artikel 2, zevende lid, NIS2-richtlijn.
[17] Artikel 5 Cbw.
[18] Memorie van toelichting, algemeen deel, paragraaf 5.1.2, ‘Overheidsinstanties’, onder “Uitgezonderde overheidsinstanties”.
[19] Voorgestelde artikelen 23, 32, 45 en 48 Cbw.

De reikwijdte van een wet dient in hoofdzaak in de wet zelf te worden geregeld, omdat het een van de hoofdelementen van de wet is.[20] Het is niet bevorderlijk voor de duidelijkheid en de rechtszekerheid wanneer overheidsinstanties die over wezenlijke taken en bevoegdheden beschikken (zoals op het gebied van de nationale veiligheid), niet uitdrukkelijk in de wet worden uitgezonderd. Voor (onderdelen van) overheidsorganisaties waarvan de taken en bevoegdheden beperkter en minder indringend zijn, is nog voorstelbaar dat die – krachtens de wet – worden uitgezonderd bij algemene maatregel van bestuur.

De Afdeling adviseert deze uitzonderingen zo veel mogelijk te concretiseren in het wetsvoorstel.

3. Coördinerende taak minister van Justitie en Veiligheid

De coördinerende taak van de minister van Justitie en Veiligheid in het kader van het voorstel voor de Cbw houdt in ieder geval in dat hij de sectoroverstijgende samenwerking tussen de bevoegde autoriteiten bevordert, en dat hij de nationale cyberbeveiligingsstrategie en het nationaal plan cyberbeveiligingsincidenten en crisisrespons vaststelt.[21] Daarnaast bevat het voorstel bepalingen waarbij ministeriële regelingen of ontheffingen worden vastgesteld door vakministers ‘in overeenstemming met’ of ‘na overleg met’ de minister van Justitie en Veiligheid.[22]

Als coördinerend bewindspersoon voor cyberveiligheid moet de minister van Justitie en Veiligheid sturend kunnen optreden bij departementoverstijgende keuzes. Tegelijkertijd is bij de implementatie van de NIS2-richtlijn ervoor gekozen om de verschillende vakministers aan te wijzen als bevoegde autoriteit.[23]

In de toelichting ontbreekt een nadere uitwerking van de invulling van de coördinerende taak van de minister van Justitie en Veiligheid op basis van het voorstel. Hierdoor is niet inzichtelijk op welke wijze de minister invulling geeft aan zijn taak als coördinerend bewindspersoon op het gebied van cyberveiligheid, alsmede of hij daarvoor in het voorliggende wetsvoorstel voldoende in positie wordt gebracht.

Daarnaast is in de toelichting niet uiteengezet waarom in de voorbereiding van ministeriële regelingen of besluiten van vakministers de betrokkenheid van de minister van Justitie beperkt blijft tot overleg en niet is gekozen voor een formele vorm van medebetrokkenheid.[24] Deze regelingen of besluiten kunnen gevolgen hebben voor de nadere uitleg en goede werking van de wet en raken daarmee het te bereiken niveau van cyberveiligheid in Nederland. Voor een goede coördinatie is van belang dat de minister van Justitie en Veiligheid betrokken is bij essentiële beslissingen, zodat deze overzicht houdt over het gehele stelsel en het functioneren daarvan. In het licht van het voorgaande dient dan ook in de toelichting te worden gemotiveerd waarom bij

---

[20] Aanwijzing 2.19, toelichting, van de Aanwijzingen voor de regelgeving.
[21] Voorgesteld artikel 14, aanhef en onder b, artikel 19 en artikel 20, Cbw.
[22] Zie voorgestelde artikelen 9, eerste lid, 10, 11, eerste lid, 13, eerste lid, en 16, tweede lid, Cbw (‘na overleg met’); voorgestelde artikelen 23, eerste lid, artikel 32, eerste lid, artikel 45, eerste lid, en artikel 48, eerste lid, Cbw (‘in overeenstemming met’).
[23] Voorgesteld artikel 15 Cbw.
[24] Zie voetnoot 22.

regelingen of beslissingen van vakministers de medebetrokkenheid van de minister van Justitie en Veiligheid niet is vereist.

De Afdeling adviseert om in de toelichting nader in te gaan op de wijze waarop invulling wordt gegeven aan de coördinerende taak en de (mede)betrokkenheid van de minister van Justitie en Veiligheid, en zo nodig het wetsvoorstel op dit punt aan te passen.

4. Handhaving van bijzondere wetten door zelfstandige bestuursorganen

In het wetsvoorstel worden uitsluitend ministers aangewezen als bevoegde autoriteit.[25] De ministers – of de door hen aangewezen ambtenaren – krijgen de bevoegdheid om toezicht te houden op de naleving met gebruikmaking van de toezichthoudende bevoegdheden die in de Algemene wet bestuursrecht zijn geregeld. Ook krijgen zij handhavingsbevoegdheden, zoals bestuursdwang, dwangsom en bestuurlijke boete.[26] Dat past bij het uitgangspunt dat het overheidsbeleid op rijksniveau zoveel mogelijk moet worden uitgeoefend onder ministeriële verantwoordelijkheid. Echter, in sommige gevallen vallen entiteiten reeds onder het toezicht op en de handhaving van specifieke wetten, opgedragen aan autoriteiten die hun bij wet toegekende taken in hoofdzaak uitoefenen buiten ministeriële verantwoordelijkheid. Zulke autoriteiten zijn ook bekend als zelfstandige bestuursorganen (zbo's).

Zo vallen kerncentrales onder het wetsvoorstel en daarmee ook onder het toezicht van de minister van Infrastructuur en Waterstaat als de bevoegde autoriteit.[27] Echter, in de Kernenergiewet zijn toezichts- en handhavingsbevoegdheden uitdrukkelijk toegekend aan de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS).[28] In 2016 is de ANVS bij wet aangewezen als zbo; zij verkreeg daarbij nog meer zelfstandigheid dan standaard is geregeld in de Kaderwet zelfstandige bestuursorganen. De regering was destijds van oordeel dat die ruime mate van onafhankelijkheid noodzakelijk was op grond van internationaal en Europees recht. De beslissingen van het regulerende lichaam over nucleaire veiligheid en stralingsbescherming moeten namelijk genomen kunnen worden zonder druk van belangen die kunnen conflicteren met het belang van veiligheid, zo meende de regering.[29]

Het wetsvoorstel zorgt ervoor dat het wettelijk toezicht op de veiligheid van kerncentrales, dat momenteel uitsluitend berust bij de ANVS, tevens komt te liggen bij de minister van Infrastructuur en Waterstaat. Daarmee kan overlapping van bevoegdheden ontstaan.

Het voorbeeld van de ANVS staat niet op zichzelf. Er zijn meer toezichthouders die de status van zelfstandig bestuursorgaan hebben, waarbij de ministeriele verantwoordelijkheid is beperkt, maar waarbij via het wetsvoorstel ook de minister

---

[25] Voorgesteld artikel 15, eerste lid, Cbw.
[26] Voorgestelde artikelen 68, eerste lid, en 73 tot en met 79, Cbw.
[27] Kerncentrales zullen worden aangewezen als kritieke entiteit in de zin van de Wwke, omdat zij elektriciteit produceren en daarnaast ook medische isotopen leveren (voorstel Wwke, bijlage, sector "Energie" en sector "Gezondheidszorg"). Kritieke entiteiten zijn van rechtswege essentiële entiteit in de zin van de Cbw (voorgesteld artikel 8, eerste lid, onderdeel i, Cbw).
[28] Artikelen 3, derde lid, onderdeel b, 58 en 59 van de Kernenergiewet.
[29] Kamerstukken II 2014/15, 34219, nr. 3, p. 4-5, nader uitgewerkt in p. 5-17.

wordt aangewezen als bevoegde autoriteit.[30] Wanneer meer toezichthouders tegelijk bevoegd zijn, kan onduidelijk zijn voor de entiteiten wie het toezicht uitoefent, en het gevaar bestaat dat de toezichthouders met elkaar concurreren, óf dat geen van beide toezicht en handhaving uitoefent.

De Afdeling adviseert om in kaart te brengen welke zbo's belast zijn met toezichts- en handhavingstaken gericht op veiligheid, en om in de toelichting aan te geven hoe voorkomen wordt dat de uitoefening van deze taken in de praktijk tot problemen leidt, doordat zij overlapt met taken die zijn toebedeeld via het wetsvoorstel.[31]

5. Toezicht en handhaving ten aanzien van de sector overheid

Het wetsvoorstel wijst onder andere ministeries, met inbegrip van de daartoe behorende dienstonderdelen, aan als essentiële entiteiten.[32] Voor de sector overheid is de minister van Binnenlandse Zaken en Koninkrijksrelaties de bevoegde autoriteit voor het toezicht op de naleving en de handhaving.[33] Uit de toelichting blijkt dat de Rijksinspectie Digitale Infrastructuur (RDI), onderdeel van het ministerie van Economische Zaken, toezicht gaat houden op de sector overheid.[34] Voor zover onderdelen van het ministerie van Economische Zaken zelf kwalificeren als essentiële of belangrijke entiteit betekent dit dat het toezicht op die onderdelen "operationeel onafhankelijk" moet zijn, als bedoeld in artikel 31, vierde lid, van de NIS2-richtlijn. De toelichting besteedt geen aandacht aan de vraag of een dergelijk 'zelftoezicht' in voldoende mate onafhankelijk is en welke voorzieningen daartoe zijn of worden getroffen.

De Afdeling adviseert om in de toelichting nader in te gaan op de vraag of, en zo ja hoe, ten aanzien van de sector overheid wordt voldaan aan het vereiste van voldoende onafhankelijk toezicht, en zo nodig het voorstel aan te passen.

6. De verwerking van persoonsgegevens

a. *Bijzondere categorieën van persoonsgegevens*

Het wetsvoorstel bevat een grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens (het betreft alle categorieën bijzondere persoonsgegevens met uitzondering van genetische en biometrische gegevens) door een CSIRT of de bevoegde autoriteit, voor zover die verwerking noodzakelijk is voor de uitoefening van hun taken op grond van het wetsvoorstel.[35] Deze grondslag is toegevoegd naar

---

[30] Voorbeelden van andere zbo's zijn de Autoriteit Consument en Markt (Kamerstukken II 2011/12, 33186, nr. 3, p. 6), de Dienst Wegverkeer RDW, en de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (Kamerstukken II 2021/22, 36138, nr. 3, p. 15). De ACM houdt mede toezicht op veiligheid, bijvoorbeeld artikel 15, eerste lid, van de Elektriciteitswet 1998.

[31] Voor de ANVS wordt dit besproken in de toelichting bij de Wwke, algemeen deel, paragraaf 7.8, 'Ministerie van Klimaat en Groene Groei, Ministerie van Infrastructuur en Waterstaat en Ministerie van Volksgezondheid, Welzijn en Sport'.

[32] Voorgesteld artikel 8, eerste lid, onderdeel g, Cbw.

[33] Voorgesteld artikel 15, eerste lid, Cbw.

[34] Memorie van toelichting, algemeen deel, paragraaf 9.14, 'Uitvoerings- en handhaafbaarheidstoetsen'.

[35] Voorgesteld artikel 64 Cbw.

aanleiding van de door de Autoriteit Persoonsgegevens (AP) verrichte toets bij een eerdere versie van het wetsvoorstel. De AP adviseerde om bij algemene maatregel van bestuur de categorieën van bijzondere persoonsgegevens aan te wijzen waarvan de verwerking noodzakelijk is voor de doeleinden van het wetsvoorstel.

Op basis van de Algemene verordening gegevensbescherming (AVG)[36] is de verwerking van bijzondere categorieën van persoonsgegevens onderworpen aan specifieke voorschriften. De verwerking van bijzondere categorieën van persoonsgegevens is bijzonder gevoelig vanuit een oogpunt van de eerbiediging van het privéleven van de persoon wiens gegevens worden verwerkt en verdient daarom extra bescherming.[37] Een inmenging in dit recht moet bij wet zijn voorzien, waarbij op voldoende duidelijke wijze is aangeven onder welke voorwaarden de inmenging is toegestaan, en mag niet verder gaan dan wat noodzakelijk is.[38] Voor de bescherming van gevoelige gegevens is het essentieel dat de bevoegdheden tot gebruik, inzage en doorgifte, voldoende precies zijn omschreven en voldoende bescherming bieden tegen arbitrair gebruik van deze bevoegdheden.[39]

Een nauwkeurige afbakening van de situaties waarin de persoonsgegevens mogen worden verwerkt is onder meer van belang om te verzekeren dat personen doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens.[40] Daarnaast geldt op basis van de AVG vanwege de bijzonder gevoelige aard van deze categorie persoonsgegevens het vereiste dat passende en specifieke waarborgen moeten gelden voor de verwerking van bijzondere categorieën van persoonsgegevens.[41]

Aan dit vereiste kan niet worden voldaan door middel van een grondslag voor de verwerking van vrijwel alle bijzondere categorieën persoonsgegevens voor in beginsel alle taken die door een CSIRT of de bevoegde autoriteit worden verricht. Het is mogelijk dat voor de effectieve uitoefening van bepaalde bevoegdheden, bijvoorbeeld indien het voor een CSIRT noodzakelijk is om realtime het netwerk- en informatiesysteem van een entiteit te monitoren, de in het voorstel genoemde bijzondere categorieën van persoonsgegevens worden ingezien. Voor de meeste bevoegdheden lijkt er echter geen noodzaak aanwezig te zijn om bijzondere categorieën van persoonsgegevens te verwerken terwijl het wetsvoorstel daar wel toe machtigt.

---

[36] Artikel 9, tweede lid, onderdeel g, van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEU 2016, L 119).
[37] Artikelen 7 en 8 van het Handvest van de grondrechten van de EU; artikel 8 EVRM; artikel 10 van de Grondwet. Zie tevens overweging 51 van de considerans bij de AVG.
[38] Zie artikel 9, tweede lid, onderdeel g, AVG; EHRM 26 april 1979, *Sunday Times t. Verenigd Koninkrijk (nr. 1)*, nr. 6538/74, ECLI:CE:ECHR:1979:0426JUD000653874, punt 49.
[39] EHRM 29 april 2014, *L.H. t. Letland*, nr. 52019/07, ECLI:CE:ECHR:2014:0429JUD005201907, punten 58 en 59; EHRM 4 december 2008 (GK), *S. en Marper t. Verenigd Koninkrijk*, nr. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, punten 95 en 96.
[40] HvJEU 8 april 2014, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland,* ECLI:EU:C:2014:238, punt 54.
[41] Artikel 9, tweede lid, onderdeel g, AVG.

De Afdeling advisering wijst er bovendien op dat het wetsvoorstel niet voorziet in passende en specifieke waarborgen in het kader van de verwerking van bijzondere categorieën van persoonsgegevens. De aanwezigheid van deze waarborgen is des te meer van belang gelet op de potentieel omvangrijke inzage in bijzonder gevoelige gegevens bij de uitoefening van bepaalde bevoegdheden op basis van het voorstel.

De Afdeling adviseert om de grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens te beperken tot de uitoefening van taken die worden opgedragen in het wetsvoorstel waarvoor verwerking van bijzondere categorieën van persoonsgegevens noodzakelijk is en te voorzien in passende en specifieke waarborgen.

b. *Gegevensverwerkingen in het kader van samenwerking*
Het wetsvoorstel regelt de samenwerking en informatie-uitwisseling tussen verscheidene instanties die belast zijn met de uitvoering van het voorstel, zoals bijvoorbeeld tussen de bevoegde autoriteiten en CSIRT's, tussen de CSIRT's onderling en de samenwerking en informatie-uitwisseling tussen deze instanties en overige instanties, zoals de bevoegde autoriteiten ingevolge de Wwke en de politie en het Openbaar Ministerie. Het wetsvoorstel schrijft voor dat de instanties onderling alle noodzakelijke gegevens, waaronder persoonsgegevens, uitwisselen ten behoeve van de doeltreffende en doelmatige uitvoering van de taken uit hoofde van het wetsvoorstel.[42]

Het voorstel werkt, met uitzondering van bepaalde samenwerkingsvormen,[43] niet nader uit hoe de samenwerking zal worden ingericht. Wel volgt uit de gekozen formulering dat de informatie die overige instanties delen met de instanties die belast zijn met de uitvoering van het voorstel, de uitvoering van hun taken uit hoofde van het voorstel dient. Omgekeerd is niet geregeld met welk doel informatie door bijvoorbeeld een CSIRT wordt gedeeld met overige instanties, zoals bijvoorbeeld de politie. Daardoor is niet op voorhand duidelijk welke gegevens noodzakelijkerwijs worden gedeeld ten behoeve van die samenwerking.

De Afdeling adviseert om in het voorstel te verduidelijken voor welke doeleinden er wordt samengewerkt en informatie wordt uitgewisseld.

c. *Samenwerking met de inlichtingen- en veiligheidsdiensten*
Het wetsvoorstel regelt de uitwisseling van gegevens tussen de bevoegde autoriteiten, de CSIRT's, het centrale contactpunt en organisaties zoals het openbaar ministerie en de politie, maar noemt niet de inlichtingen- en veiligheidsdiensten. Uit de toelichting blijkt dat uitwisseling met deze diensten wel plaatsvindt, maar dat het gebeurt op grondslag van de Wet op de inlichtingen- en veiligheidsdiensten 2017.[44] Voor het effectief voorkomen en bestrijden van cyberaanvallen is het van belang dat de

---

[42] Zie voorgesteld artikel 51 Cbw. De voorgestelde artikelen 57 en 58 Cbw bevatten een afwijkende formulering en verbinden de verwerking van persoonsgegevens aan de samenwerking met de aldaar genoemde autoriteiten.
[43] Zie bijvoorbeeld, voor de samenwerking tussen bevoegde autoriteiten op basis van het voorstel voor de Cbw en de Wwke, voorgesteld artikel 56 Cbw.
[44] Toelichting, paragraaf 9.11 (CSIRT), onder "Taken van het CSIRT".

bevoegde autoriteiten, de CSIRT's, politie, openbaar ministerie en de inlichtingen- en veiligheidsdiensten informatie snel en effectief kunnen delen, zodat zij een zo volledig mogelijk beeld kunnen vormen van de dreigingen.

De Afdeling adviseert in de toelichting in te gaan op de vraag of de Wet op de inlichtingen- en veiligheidsdiensten 2017 voldoende grondslag biedt voor effectieve samenwerking tussen deze organisaties en indien dit niet het geval is, om alsnog te voorzien in een wettelijke grondslag

7. Duidelijke en kenbare omzetting

Artikel 32, zevende lid, NIS2-richtlijn vereist dat bij het nemen van de voorgeschreven handhavingsmaatregelen de bevoegde autoriteiten tenminste rekening houden met een aantal specifieke omstandigheden. De toelichting geeft aan dat deze bepaling reeds is geïmplementeerd via het evenredigheidsvereiste in de Awb.[45]

Richtlijnbepalingen zijn niet rechtstreeks toepasselijk in de nationale rechtsordes en vereisen omzetting in nationaal recht.[46] De omzettingsmaatregelen moeten dwingende kracht bezitten en specifiek, nauwkeurig en duidelijk zijn. Het is niet altijd nodig dat de richtlijnbepaling wordt overgenomen in wettelijke voorschriften. Afhankelijk van de inhoud van de richtlijn kan een algemeen rechtskader volstaan, met name door algemene beginselen van constitutioneel of administratief recht. Daarvoor geldt echter de voorwaarde dat deze beginselen de volledige toepassing van de richtlijn daadwerkelijk garanderen.

Bovendien is het van belang dat, indien de richtlijn rechten voor particulieren beoogt te scheppen, de rechtssituatie die uit deze beginselen voortvloeit voldoende bepaald en duidelijk moet zijn, zodat particulieren kennis kunnen nemen van al hun rechten en verplichtingen en deze in voorkomend geval geldend kunnen maken voor de nationale rechterlijke instanties.[47] Deze voorwaarden stellen grenzen aan de implementatie via algemene beginselen. Enige terughoudendheid is daarom van belang bij de keuze voor deze vorm van implementeren.[48]

Toegepast op de implementatie van artikel 32, zevende lid, NIS2-richtlijn door middel van het evenredigheidsvereiste in de Awb, wijst de Afdeling op de specifieke aard van de criteria in de richtlijnbepaling en dat die criteria beogen om waarborgen toe te kennen aan de essentiële entiteit.[49] Gelet op deze omstandigheden lijkt de voorgestelde implementatiewijze ontoereikend.

De Afdeling adviseert om in de toelichting hierop nader in te gaan en het voorstel zo nodig aan te passen.

---

[45] Artikel 3:4, tweede lid, Awb. Zie de memorie van toelichting, algemeen deel, paragraaf 5.9, 'Rechtsbescherming en vereisten aan besluiten', en de transponeringstabel.
[46] Artikel 288, derde alinea, VWEU.
[47] HvJEU 11 juni 2015, zaak C-29/14, *Commissie t. Polen,* ECLI:EU:C:2015:379, punten 37 en 38.
[48] Zie ook de Handleiding Wetgeving en Europa, p. 21.
[49] In het geval van een schorsing, welke sanctie is opgenomen in voorgesteld artikel 77 Cbw, komen deze waarborgen toe aan de bestuursleden van de essentiële entiteit.

8. Uitzonderingen op de Wet open overheid

Het voorstel bepaalt dat de bevoegde autoriteit, het centrale contactpunt, het CSIRT en de minister van Justitie en Veiligheid vertrouwelijke gegevens kunnen verstrekken, mits dat noodzakelijk en evenredig is, en mits de veiligheids- en commerciële belangen van de betrokken entiteit worden beschermd.[50] De Wet open overheid (Woo) is niet van toepassing op deze gegevens, tenzij het gaat om milieu-informatie.

a. *Afwijken van een algemene wet*
De Woo is een algemene wet, waarvan alleen kan worden afgeweken als daarvoor de noodzaak is aangetoond.[51] De Woo stelt openbaarheid van overheidsinformatie voorop, maar kent uitzonderingen in verband met, onder meer, de veiligheid van de Staat, bedrijfs- en fabricagegegevens en de eerbiediging van de persoonlijke levenssfeer.[52] Deze wettelijk verankerde uitzonderingen roepen de vraag op of het noodzakelijk is om de Woo niet van toepassing te verklaren op gegevens die in het kader van dit wetsvoorstel worden verstrekt.

De Afdeling adviseert om nader te motiveren waarom een afwijking, gezien de beperkingen in de Woo, noodzakelijk is.

b. *Verduidelijking van de tekst*
De voorgestelde bepalingen maken niet duidelijk *aan wie* de gegevens kunnen worden verstrekt. Uit de NIS2-richtlijn blijkt dat het niet gaat om verstrekking aan derden, maar om onderlinge uitwisseling van gegevens tussen de bevoegde autoriteit, het centrale contactpunt, het CSIRT en de minister, en dat ook uitwisseling met de Europese Commissie mogelijk moet zijn.[53]

De Afdeling adviseert om in het voorstel te verduidelijken aan wie de gegevens kunnen worden verstrekt.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

De vice-president van de Raad van State,

---

[50] Voorgestelde artikelen 66 en 100 Cbw.
[51] Aanwijzing 2.46 van de Aanwijzingen voor de regelgeving.
[52] Artikel 5.1, eerste lid, onderdelen b, c en d, en tweede lid, onderdelen e en f, Woo.
[53] Artikel 2, dertiende lid, NIS2-richtlijn.