Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

36 764 Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet)

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 19 februari 2025 en het nader rapport d.d. 27 mei 2025, aangeboden aan de Koning door de Minister van Justitie en Veiligheid. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Blijkens de mededeling van de Directeur van Uw Kabinet van 6 december 2024, nr. 2024002833, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 19 februari 2025, nr. W16.24.00336/II, bied ik U hierbij aan.

De tekst van het advies treft U hieronder cursief aan, voorzien van mijn reactie.

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.

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

kst-36764-4
ISSN 0921 - 7371
's-Gravenhage 2025

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.[2] 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 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.

---

[2] *Memorie van toelichting, algemeen deel, paragraaf 8.1.1, «Inleiding»; overheidsinstanties zijn daarin niet meeberekend.*

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.[3] 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.[4] 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».[5]*

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 EU (NIS1-richtlijn) is geïmplementeerd.[6] Uit een evaluatie van die richtlijn kwam een aantal tekortkomingen naar voren.[7] Om die reden is de NIS2-richtlijn vastgesteld betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de EU.[8] 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.[9] De Afdeling brengt over beide implementatievoorstellen

---

[3] *Vergelijk voorgesteld artikel 2 Cbw.*

[4] *De versleuteling van bestanden van het slachtoffer door criminelen die tegen betaling van losgeld weer wordt ontsleuteld.*

[5] *Cybersecuritybeeld Nederland 2024 (Rapport NCTV), bijlage bij Kamerstukken II 2024/25, 26 643, nr. 1229, p. 27.*

[6] *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).*

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

[8] *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.*

[9] *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».*

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.[10]

Voor essentiële en belangrijke entiteiten geldt allereerst een zorgplicht.[11] 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.[12]

Daarnaast geldt voor essentiële en belangrijke entiteiten een meldplicht.[13] 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).[14] 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.[15]

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.[16] CSIRT's zijn verantwoordelijk voor het verlenen van bijstand aan entiteiten in het geval van een cyberincident.

---

[10] *Vergelijk paragrafen 15.2 en 15.3, in het bijzonder voorgesteld artikel 80, Cbw.*
[11] *Voorgesteld artikel 21 Cbw.*
[12] *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.*
[13] *Voorgesteld artikel 25 Cbw.*
[14] *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.*
[15] *Voorgesteld artikel 24 Cbw.*
[16] *Zie de definitie in het voorgestelde artikel 1 Cbw en artikel 8, eerste lid, van de NIS2-richtlijn.*

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.»[17] 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.[18] Volgens de toelichting zal het wetsvoorstel niet gelden voor «onder andere» de veiligheidsregio's, het Ministerie van Defensie, het openbaar ministerie en de politie.[19] 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.[20]

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.

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.[21] 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.

Naar aanleiding van dit advies van de Afdeling is in het wetsvoorstel artikel 5, eerste lid, Cbw aangepast, zodat bij wet is bepaald dat de Cbw niet van toepassing is op het Ministerie van Defensie, de Militaire Inlichtingen- en Veiligheidsdienst, de Algemene Inlichtingen- en Veiligheidsdienst, het openbaar ministerie, de politie en de veiligheidsregio's.

In artikel 5, eerste lid, Cbw is tevens voorzien in de grondslag om bij algemene maatregel van bestuur andere overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, van die toepasselijkheid uit te zonderen (onderdeel f). Van deze grondslag zal gebruik worden gemaakt indien na de inwerkingtreding van de Cbw onverhoopt tot het inzicht wordt gekomen dat een overheidsinstantie ontbreekt in de opsomming van artikel 5, eerste lid, Cbw. Hierbij wordt benadrukt dat het uitgangspunt is dat artikel 5, eerste lid, Cbw de complete opsomming betreft van overheidsinstanties die moeten worden uitgezonderd van het

---

[17] *Artikel 2, zevende lid, NIS2-richtlijn.*
[18] *Artikel 5 Cbw.*
[19] *Memorie van toelichting, algemeen deel, paragraaf 5.1.2, «Overheidsinstanties», onder «Uitgezonderde overheidsinstanties».*
[20] *Voorgestelde artikelen 23, 32, 45 en 48 Cbw.*
[21] *Aanwijzing 2.19, toelichting, van de Aanwijzingen voor de regelgeving.*

toepassingsbereik van de Cbw, omdat zij in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving.

Overigens is in artikel 5, tweede lid, Cbw, geregeld dat de Cbw wél van toepassing is op overheidsinstanties als bedoeld in het eerste lid, wanneer en voor zover zij optreden als verleners van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers.

Naar aanleiding van de wijzigingen in artikel 5, eerste lid, Cbw is ook in de memorie van toelichting de toelichting onder het kopje «Uitgezonderde overheidsinstanties» in paragraaf 5.1.2 en de artikelsgewijze toelichting op artikel 5 Cbw aangepast.

Voor de bijzondere opsporingsdiensten geldt dat zij ressorteren onder een Minister, niet zijnde de Minister van Defensie (zie artikel 2 Wet op de bijzondere opsporingsdiensten). Voor deze diensten geldt dat zij onderdeel zijn van de betreffende ministeries (zie artikel 9, eerste lid, Wet op de bijzondere opsporingsdiensten). De ministeries waar de bijzondere opsporingsdiensten onder ressorteren voeren niet in hoofdzaak activiteiten uit op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten (artikel 2, zevende lid, NIS2-richtlijn in samenhang met overweging 8 van de NIS2-richtlijn). Omdat de ministeries waar de bijzondere opsporingsdiensten onder ressorteren onder het toepassingsbereik van de Cbw vallen, vallen ook de bijzondere opsporingsdiensten onder het toepassingsbereik van de Cbw.

De bijzondere opsporingsdiensten voeren activiteiten uit op het gebied van rechtshandhaving, zie de opsomming van hun taken in artikel 3 Wet op de bijzondere opsporingsdiensten. Zodra de Cbw in werking treedt en daarmee de ministeries waar de bijzondere opsporingsdiensten onder ressorteren onder het toepassingsbereik van de Cbw komen te vallen, zullen die ministeries met betrekking tot de activiteiten die de bijzondere opsporingsdiensten uitvoeren, op grond van de artikelen 23, 32, 45 en 48 Cbw worden ontheven van de verplichtingen uit de artikelen 21, 25 tot en met 30, 44 en 47 Cbw.

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.[22] 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.[23]

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

---

[22] *Voorgesteld artikel 14, aanhef en onder b, artikel 19 en artikel 20, Cbw.*

[23] *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»).*

NIS2-richtlijn ervoor gekozen om de verschillende vakministers aan te wijzen als bevoegde autoriteit.[24]

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.[25] *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 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.

Bij de implementatie van de NIS2-richtlijn is er voor gekozen om aan te sluiten bij de huidige verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid, waarbij elke Minister verantwoordelijk is voor de digitale weerbaarheid en de continuïteit van de entiteiten binnen zijn portefeuille. De ratio hierbij is dat netwerk- en informatiesystemen verweven zijn met alle processen binnen de samenleving en een sector- of entiteitspecifieke toepassing hebben. Dit vraagt om sectorspecifieke kennis en een holistische blik op de samenhang van de risico's ten aanzien van netwerk- en informatiesystemen met andere risico's binnen de sector.

De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op cybersecurity en nationale veiligheid. Vanuit deze rol zorgt hij voor een goed functionerend cybersecuritystelsel en borgt hij dat de impact op de nationale veiligheid voldoende wordt meegewogen in de keuzes die de vakministers hierin maken. In de praktijk betekent dit dat wanneer de vakminister nadere regels of besluiten voor zijn sector «na overleg met» of «in overeenstemming met» de Minister van Justitie en Veiligheid vaststelt, de Minister van Justitie en Veiligheid zal toetsen en adviseren op onder meer sectoroverstijgende effecten, de druk op het cybersecuritystelsel en de bredere impact op de nationale veiligheid.

Het verschil tussen «na overleg met» en «in overeenstemming met» is dat bij «na overleg met» eventueel verschil van inzicht kan worden opgelost via de gangbare afstemmings- en overlegstructuren, maar de vakminister uiteindelijk eigenstandig de eindbeslissing neemt. Bij «in overeenstemming met» dient de Minister van Justitie en Veiligheid bij eventueel uiteenlopende inzichten alsnog mede te beslissen. Deze variant is gekozen

[24] *Voorgesteld artikel 15 Cbw.*
[25] *Zie voetnoot 22.*

bij de bepalingen waarbij de handelingen van de vakminister het integrale stelsel raken, en dus van invloed zijn op de stelselverantwoordelijkheid van de Minister van Justitie en Veiligheid.

4. Handhaving van bijzondere wetten door zelfstandige bestuursorganen

In het wetsvoorstel worden uitsluitend Ministers aangewezen als bevoegde autoriteit.[26] 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.[27] 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.[28] Echter, in de Kernenergiewet zijn toezichts- en handhavingsbevoegdheden uitdrukkelijk toegekend aan de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS).[29] 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.[30]

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 wordt aangewezen als bevoegde autoriteit.[31] 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.

---

[26] *Voorgesteld artikel 15, eerste lid, Cbw.*

[27] *Voorgestelde artikelen 68, eerste lid, en 73 tot en met 79, Cbw.*

[28] *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).*

[29] *Artikelen 3, derde lid, onderdeel b, 58 en 59 van de Kernenergiewet.*

[30] *Kamerstukken II 2014/15, 34 219, nr. 3, p. 4–5, nader uitgewerkt in p. 5–17.*

[31] *Voorbeelden van andere zbo's zijn de Autoriteit Consument en Markt (Kamerstukken II 2011/12, 33 186, nr. 3, p. 6), de Dienst Wegverkeer RDW, en de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (Kamerstukken II 2021/22, 36 138, nr. 3, p. 15). De ACM houdt mede toezicht op veiligheid, bijvoorbeeld artikel 15, eerste lid, van de Elektriciteitswet 1998.*

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.[32]

Entiteiten kunnen onder toezicht staan vanuit andere wettelijke kaders, uitgeoefend door bijvoorbeeld een zelfstandig bestuursorgaan. Het ligt in de rede dat de toezichthouders met raakvlakken hierover met elkaar in contact treden om samenwerkingsafspraken te maken, die de doeltreffendheid en doelmatigheid van het toezicht waarborgen. Hierbij wordt onder meer gedacht aan afspraken over samenloop van toezicht op eenzelfde entiteit, het voorkomen van onevenredige toezichtslasten en de uitwisseling van gegevens. Het heeft daarbij de voorkeur dat deze afspraken worden vastgelegd in een samenwerkafspraak of een vergelijkbaar instrument en dat deze wordt gepubliceerd. Dit zorgt voor transparantie over de gemaakte afspraken en maakt voor entiteiten die onder toezicht staan helder op welke wijze de toezichthouders invulling geven aan voorgenoemde aspecten.

Daarbij is het van belang om in die samenwerkingsafspraken voor ogen te houden dat de verschillende wetten in het veiligheidsdomein verschillende aspecten van veiligheid regelen, geredeneerd vanuit wettelijk verschillende gedefinieerde te beschermen belangen. De betreffende toezichthouders zullen derhalve elk op basis van hun eigen wettelijke grondslag hun taken uitvoeren en overlap in bevoegdheden doet geen afbreuk aan de bevoegdheden en verantwoordelijkheden van de respectievelijke toezichthouders.

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.[33] *Voor de sector overheid is de Minister van Binnenlandse Zaken en Koninkrijksrelaties de bevoegde autoriteit voor het toezicht op de naleving en de handhaving.*[34] *Uit de toelichting blijkt dat de Rijksinspectie Digitale Infrastructuur (RDI), onderdeel van het Ministerie van Economische Zaken, toezicht gaat houden op de sector overheid.*[35] *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.

---

[32] *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».*

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

[34] *Voorgesteld artikel 15, eerste lid, Cbw.*

[35] *Memorie van toelichting, algemeen deel, paragraaf 9.14, «Uitvoerings- en handhaafbaarheidstoetsen».*

In artikel 31, vierde lid, NIS2-richtlijn is bepaald dat lidstaten ervoor moeten zorgen dat de bevoegde autoriteiten bij het toezicht op de naleving van de NIS2-richtlijn door overheidsinstanties en bij het opleggen van handhavingsmaatregelen inzake inbreuken op de NIS2-richtlijn over passende bevoegdheden beschikken om bij de uitvoering van deze taken operationeel onafhankelijk te zijn van de overheidsinstanties waarop zij toezicht houden.

Het toezicht op de naleving van het bepaalde bij of krachtens de Cbw ten aanzien van entiteiten uit de sector overheid (met uitzondering van de waterschappen) zal worden uitgevoerd door de Rijksinspectie Digitale Infrastructuur (hierna: RDI). De RDI valt onder het Ministerie van Economische Zaken en zal de hiervoor bedoelde taken uitvoeren namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties als bevoegde autoriteit van de entiteiten die vallen binnen de sector overheid, met uitzondering van de waterschappen. Aangezien beide ministeries zelf ook onder de Cbw zullen vallen, dient het toezicht in voldoende mate operationeel onafhankelijk te zijn. Ten aanzien van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is er een organisatorische scheiding doordat de RDI onder een ander ministerie valt. Verder is de operationele onafhankelijkheid mede geborgd door de Aanwijzingen inzake de rijksinspecties. Zo is in aanwijzing 14, vijfde lid, bepaald dat de beleidsinhoudelijk verantwoordelijke Minister zijn aanwijzingsbevoegdheid niet gebruikt om een rijksinspectie ervan te weerhouden een specifiek onderzoek te verrichten of af te ronden, noch om in te grijpen in de wijze waarop een rijksinspectie een specifiek onderzoek verricht, noch om invloed uit te oefenen op de bevindingen, oordelen en adviezen van een rijksinspectie. De Minister van Binnenlandse Zaken en Koninkrijksrelaties zal vanuit zijn verantwoordelijkheid als bevoegde autoriteit van de entiteiten die vallen binnen de sector overheid borgen dat er geen operationele bemoeienis is, zoals via openbaar kenbare relatiestatuten, regelingen of procedures.

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.[36] Deze grondslag is toegevoegd naar 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)[37] 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

---

[36] *Voorgesteld artikel 64 Cbw.*

[37] *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).*

gegevens worden verwerkt en verdient daarom extra bescherming.[38] 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.[39] 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.[40]

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.[41] 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.[42]

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.

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.

Naar aanleiding van het advies van de Afdeling over de beperking van de grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens is artikel 64 Cbw gewijzigd en is de artikelsgewijze toelichting op dit artikel aangepast. De wijziging houdt ten eerste in dat het eerste lid van genoemd artikel de grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens regelt voor zover het gaat om de

---

[38] *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.*

[39] *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.*

[40] *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.*

[41] *HvJEU 8 april 2014, gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238, punt 54.*

[42] *Artikel 9, tweede lid, onderdeel g, AVG.*

taakuitoefening van de bevoegde autoriteit. Die grondslag ziet op de uitoefening van alle in de Cbw geregelde taken van de bevoegde autoriteit. Het is de verwachting dat in het kader van de uitoefening van al deze taken van de bevoegde autoriteit (waaronder de taken in het kader van het toezicht, maar ook bijvoorbeeld die in het kader van meldingen van significante incidenten) het noodzakelijk kan zijn dat de bevoegde autoriteit bijzondere categorieën van persoonsgegevens moet verwerken.

Daarnaast is er een nieuw lid toegevoegd (tweede lid) met de grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens door het CSIRT. Die laatstbedoelde grondslag is beperkt tot de taken die zijn opgenomen in artikel 16, tweede lid, onderdelen a tot en met e, Cbw. Het CSIRT moet bij het uitvoeren van die taken soms bijzondere categorieën van persoonsgegevens verwerken. Te denken valt aan een dataset die inloggegevens (*credentials*) bevat waarin ook e-mailadressen zitten waaruit het lidmaatschap van een vakbond, vereniging voor LHBTI-rechten of politieke partij blijkt. Daarnaast kan het bijvoorbeeld voorkomen dat een server van een zorginstelling op het internet staat die medische gegevens bevat of andere bijzondere persoonsgegevens, zoals de dieetwensen van cliënten of patiënten waaruit de geloofsovertuiging kan worden afgeleid.

Ten aanzien van het advies van de Afdeling over waarborgen met betrekking tot de verwerking van bijzondere categorieën van persoonsgegevens is de reactie als volgt. De Algemene verordening gegevensbescherming en de Uitvoeringswet Algemene verordening gegevensbescherming zijn van toepassing op het CSIRT en de bevoegde autoriteit en vereisen onder meer het nemen van passende technische en organisatorische maatregelen met betrekking tot het verwerken van persoonsgegevens. Het CSIRT moet bovendien op grond van artikel 11, eerste lid, NIS2-richtlijn voldoen aan hoge eisen. In aanvulling op het voorgaande is in artikel 65 Cbw voorzien in de maximale bewaartermijnen voor bijzondere categorieën van persoonsgegevens. Daarbij is die termijn ten aanzien van bijzondere categorieën van persoonsgegevens die door het CSIRT worden verwerkt verkort van 60 naar 12 maanden door de aanpassing van het tweede lid en het toevoegen van een nieuw lid (derde lid). Gelet op al het voorgaande zijn voldoende waarborgen aanwezig ten aanzien van de verwerking van bijzondere categorieën van persoonsgegevens door de bevoegde autoriteiten en de CSIRT's.

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.[43]

[43] *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.*

Het voorstel werkt, met uitzondering van bepaalde samenwerkingsvormen,[44] 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.

Naar aanleiding van dit advies van de Afdeling is in artikel 51, tweede lid, Cbw verduidelijkt dat de verstrekking van gegevens door de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt aan de in dit artikellid opgesomde andere instanties plaatsvindt voor zover die verstrekking noodzakelijk is met het oog op de samenwerking die de eerstgenoemde instanties ten behoeve van hun taakuitoefening aangaan met die andere instanties. Daarmee zal verstrekking dus gegevens betreffen die relevant zijn voor de uitoefening van de taken die die andere instanties krachtens hun eigen wettelijke regimes uitoefenen en waarvoor de samenwerking met de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt aangewezen is. In verband hiermee is ook de artikelsgewijze toelichting op artikel 51 Cbw aangepast.

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.[45] Voor het effectief voorkomen en bestrijden van cyberaanvallen is het van belang dat de 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

Voor het zo goed mogelijk uitoefenen van de onderscheidenlijke taken van enerzijds de CSIRT's, de bevoegde autoriteiten en het centrale contactpunt en anderzijds de inlichtingen- en veiligheidsdiensten is het, zoals de Afdeling terecht opmerkt, van belang dat zij samenwerken en in het kader daarvan informatie zoveel als nodig voor de uitoefening van die taken met elkaar kunnen uitwisselen. Het wetsvoorstel dat ter advies is voorgelegd aan de Afdeling voorzag daartoe met artikel 16, derde lid, aanhef en onderdeel b, Cbw (thans artikel 16, tweede lid, aanhef en onderdeel b, Cbw) op zich al in de grondslag, voor zover het gaat om de verstrekking van informatie door een CSIRT aan de inlichtingen- en veiligheidsdiensten. Dat artikelonderdeel regelt dat een CSIRT tot taak heeft om

---

[44] *Zie bijvoorbeeld, voor de samenwerking tussen bevoegde autoriteiten op basis van het voorstel voor de Cbw en de Wwke, voorgesteld artikel 56 Cbw.*

[45] *Toelichting, paragraaf 9.11 (CSIRT), onder «Taken van het CSIRT».*

informatie over cyberdreigingen, kwetsbaarheden en incidenten te verstrekken aan andere relevante partijen dan de in dat onderdeel bijvoorbeeld genoemde essentiële entiteiten en belangrijke entiteiten. De inlichtingen- en veiligheidsdiensten zijn, zoals was aangegeven in de artikelsgewijze toelichting bij artikel 16 Cbw, juist als het informatie betreft die relevant is voor de uitoefening van hun wettelijke taken, zulke relevante partijen.

Voor zover het echter gaat om verstrekking van informatie door de bevoegde autoriteiten en het centrale contactpunt aan de inlichtingen- en veiligheidsdiensten bevatte het wetsvoorstel nog niet de grondslag daarvoor. Naar aanleiding hiervan is artikel 51, tweede lid, Cbw aangepast, door de inlichtingen- en veiligheidsdiensten toe te voegen aan de in dat artikellid opgenomen opsomming van instanties waarmee de CSIRT's, de bevoegde autoriteiten en het centrale contactpunt nadrukkelijk samenwerken en in het kader daarvan voor de taakuitoefening van die instanties relevante informatie verstrekken. Deze aanpassing betekent ook dat de informatieverstrekking door het CSIRT aan de inlichtingen- en veiligheidsdiensten voortaan zal plaatsvinden op grond van artikel 51, tweede lid, Cbw. In verband hiermee zijn ook de artikelsgewijze toelichtingen bij de artikelen 16 en 51 Cbw en paragraaf 9.11 van de memorie van toelichting aangepast.

Andersom wordt in de artikelen 62 e.v. van de Wet op de inlichtingen- en veiligheidsdiensten voorzien in de bevoegdheid van de inlichtingen- en veiligheidsdiensten om in het kader van de goede taakuitvoering over door hen verwerkte gegevens mededeling te doen aan onder meer Ministers en andere bestuursorganen voor wie die gegevens voor hun taakuitoefening relevant zijn. Daarmee wordt een voldoende grondslag voor de samenwerking tussen enerzijds de CSIRT's, de bevoegde autoriteiten en het centrale contactpunt enerzijds en de inlichtingen- en veiligheidsdiensten anderzijds geboden.

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.[46]

Richtlijnbepalingen zijn niet rechtstreeks toepasselijk in de nationale rechtsordes en vereisen omzetting in nationaal recht.[47] *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

---

[46] *Artikel 3:4, tweede lid, Awb. Zie de memorie van toelichting, algemeen deel, paragraaf 5.9, «Rechtsbescherming en vereisten aan besluiten», en de transponeringstabel.*

[47] *Artikel 288, derde alinea, VWEU.*

instanties.[48] Deze voorwaarden stellen grenzen aan de implementatie via algemene beginselen. Enige terughoudendheid is daarom van belang bij de keuze voor deze vorm van implementeren.[49]

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.[50] 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.

Naar aanleiding van dit advies van de Afdeling is ter implementatie van artikel 32, zevende lid, NIS2-richtlijn in het wetsvoorstel artikel 69 Cbw (nieuw) ingevoegd, is voorzien in een artikelsgewijze toelichting op dit nieuwe artikel, is paragraaf 5.9 aangevuld met passages onder verwijzing naar artikel 69 Cbw (nieuw) en is de transponeringstabel op dit punt aangepast.

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.[51] 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.[52] 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.[53] 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.

Er is aanleiding gezien voor de in de artikelen 66, tweede lid, en 101 Cbw (100 oud) opgenomen uitzondering op de toepasselijkheid van de Wet open overheid (hierna: Woo), omdat het van groot belang is dat de vertrouwelijkheid van gegevens die bijvoorbeeld door entiteiten als zodanig aan het CSIRT of de bevoegde autoriteit worden verstrekt zo veel mogelijk wordt gewaarborgd. De door de Afdeling genoemde uitzonderingsgronden zijn niet toereikend, omdat deze niet de garantie bieden dat

---

[48] *HvJEU 11 juni 2015, zaak C-29/14, Commissie t. Polen, ECLI:EU:C:2015:379, punten 37 en 38.*
[49] *Zie ook de Handleiding Wetgeving en Europa, p. 21.*
[50] *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.*
[51] *Voorgestelde artikelen 66 en 100 Cbw.*
[52] *Aanwijzing 2.46 van de Aanwijzingen voor de regelgeving.*
[53] *Artikel 5.1, eerste lid, onderdelen b, c en d, en tweede lid, onderdelen e en f, Woo.*

alle vertrouwelijke gegevens die in het kader van de Cbw worden verwerkt, niet openbaar kunnen worden gemaakt op grond van de Woo.

In het geval van het CSIRT geldt dat de redenen daarvoor zijn gelegen in het zo veel mogelijk voorkomen van schade bij entiteiten, zoals reputatieschade, toegenomen kwetsbaarheid voor aanvallen en benadeling van de concurrentiepositie, en het door het CSIRT voor onder meer bijstand aan entiteiten kunnen gebruiken van deze gegevens zonder daarbij gehinderd te worden door het mogelijk vroegtijdig openbaar worden daarvan. Daarnaast is ook van belang dat als het gaat om gegevens die niet verplicht hoeven te worden gemeld, het risico bestaat dat entiteiten terughoudend worden met het delen van die informatie, als de vertrouwelijkheid daarvan niet zo veel mogelijk is gewaarborgd, en het CSIRT daardoor serieus benadeeld wordt in de goede uitoefening van zijn wettelijke taken. In de huidige praktijk onder de Wet beveiliging netwerk- en informatiesystemen is namelijk al gebleken dat het Nationaal Cyber Security Centrum als CSIRT voor zijn taakuitoefening in grote mate afhankelijk is van vrijwillige meldingen. Artikel 66, tweede lid, Cbw biedt entiteiten op voorhand de zekerheid dat vertrouwelijke gegevens niet openbaar kunnen worden gemaakt op grond van de Woo. Het is noodzakelijk om die zekerheid op voorhand te kunnen bieden, om zo onder meer te voorkomen dat informatie, die van groot belang is voor de goede taakuitoefening van het CSIRT, niet met het CSIRT wordt gedeeld en daardoor de goede taakuitoefening door het CSIRT in het geding komt.

Het centrale contactpunt heeft onder andere als taak om andere lidstaten te informeren in het geval van incidenten met grensoverschrijdende gevolgen. Om dit te kunnen doen dient het centrale contactpunt relevante informatie te delen met centrale contactpunten van andere lidstaten. Daarbij kan het gaan om informatie die het CSIRT heeft verkregen vanuit de meldplicht of vanuit een vrijwillige melding. Het is van belang om te voorkomen dat dezelfde informatie, die bij het CSIRT op voorhand is voorzien van bovenbedoelde waarborgen, niet van deze waarborgen is voorzien als deze berust bij het centrale contactpunt. Tevens dient de uitzondering op de toepasselijkheid van de Woo om te waarborgen dat in geval van entiteiten die in meerdere lidstaten actief zijn Nederlandse wet- en regelgeving er niet voor zorgt dat vertrouwelijke informatie die door deze entiteiten vertrouwelijk is verstrekt in Nederland onbedoeld openbaar wordt. Het is daarom noodzakelijk om dezelfde zekerheid op voorhand te bieden dat vertrouwelijke gegevens, die berusten bij het centrale contactpunt, niet openbaar kunnen worden gemaakt.

Voor de bevoegde autoriteit geldt de overweging dat deze ter uitvoering van haar toezichtsactiviteiten komt te beschikken over vertrouwelijke informatie over de stand van de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten en belangrijke entiteiten, evenals incidenten bij deze entiteiten. De vertrouwelijkheid van gegevens moet zo veel mogelijk worden geborgd om reputatieschade, benadeling van de concurrentiepositie en toegenomen kwetsbaarheid voor aanvallen te voorkomen. Artikel 66, tweede lid, Cbw biedt entiteiten op voorhand de zekerheid dat deze vertrouwelijke gegevens niet openbaar kunnen worden gemaakt door de bevoegde autoriteit op grond van de Woo. Hiermee geldt er een gelijkluidend regime voor het CSIRT, het centrale contactpunt en de bevoegde autoriteit.

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.[54]

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

Het door de Afdeling in voetnoot 53 aangehaalde artikel 2, dertiende lid, NIS2-richtlijn ziet op de voorwaarden waarbinnen de uitwisseling van vertrouwelijke informatie met de daarin genoemde actoren mogelijk is. De bepaling belet echter niet de uitwisseling van vertrouwelijke informatie met anderen dan de in de bepaling genoemde actoren. Er is ervoor gekozen in het wetsvoorstel te voorzien in de mogelijkheid om vertrouwelijke gegevens ook te kunnen uitwisselen met andere partijen, bijvoorbeeld in het kader van de wettelijk geregelde samenwerking tussen instanties. Ook kan het gaan om het delen van vertrouwelijke informatie met getroffen entiteiten voor zover het gaat om de eigen gegevens van die entiteit en schakelorganisaties en andere relevante partijen wanneer deze uitwisseling noodzakelijk is om de weerbaarheid van entiteiten of de achterban van schakelorganisaties te borgen.

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,
Th.C. de Graaf

Van de gelegenheid is gebruik gemaakt om het wetsvoorstel op enkele punten te wijzigen. Hierna worden de belangrijkste wijzigingen toegelicht.

Eén van de wijzigingen betreft de wijziging van de in artikel 16 Cbw opgenomen delegatiegrondslag en overheveling daarvan van het tweede lid naar het zevende lid van dat artikel. Met deze wijziging wordt het mogelijk om niet alleen bij ministeriële regeling, maar ook bij algemene maatregel van bestuur in generieke zin regels te stellen over de vereisten waaraan een organisatie die als CSIRT wordt aangewezen, moet voldoen.

Een andere wijziging betreft de toevoeging van een derde lid in artikel 25 Cbw. In die bepaling wordt geregeld dat bij of krachtens algemene maatregel van bestuur de criteria worden vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident als bedoeld in artikel 25, tweede lid, Cbw. Naar aanleiding van de hiervoor bedoelde toevoeging van een derde lid in artikel 25 Cbw is ook artikel 35 Cbw aangepast, zodat er geen overlap is in de grondslagen in beide artikelen.

Een andere wijziging betreft de toevoeging van een derde lid in artikel 51 Cbw. Tot het inzicht is namelijk gekomen dat het wetsvoorstel nog niet voorziet in de grondslag voor de bevoegde autoriteiten, de CSIRT's en het centrale contactpunt om informatie uit te kunnen wisselen met de cyberbeveiligingsdeskundigen, bedoeld in artikel 19, eerste lid, NIS2-richtlijn.

Een andere wijziging betreft de wijziging van artikel 100 Cbw, waarin de Telecommunicatiewet wordt gewijzigd. Het betreffen hierbij technische wijzigingen in artikel 11a.3 van de Telecommunicatiewet, waarbij de relevante aanbieders met het oog op de continuïteit van omroepetherdis-

[54] *Artikel 2, dertiende lid, NIS2-richtlijn.*

tributie hun zorgplicht en het opstellen van een continuïteitsplan behouden.

Voorts is artikel 101 Cbw (oud), over de wijziging van de Wet op de economische delicten, uit het wetsvoorstel gehaald. De desbetreffende bepaling uit de Wet op de economische delicten die betrekking heeft op de Telecommunicatiewet had niet moeten worden geschrapt.

Ik verzoek U het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Minister van Justitie en Veiligheid,
D.M. van Weel