Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

32 761 Verwerking en bescherming persoonsgegevens

Nr. 304

BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING EN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 juni 2024

Op 9 februari 2023 bood de Minister voor Rechtsbescherming, mede namens de Staatssecretaris Koninkrijksrelaties en Digitalisering, uw Kamer het onderzoeksrapport «Verkennende analyse: Naleving van de AVG door overheden» aan (Kamerstuk 32 761, nr. 261), dat in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is uitgevoerd door Pro Facto en Hooghiemstra & Partners. Met deze brief ontvangt u de beleidsreactie op dat onderzoek.

Aanleiding

Bescherming van persoonsgegevens is een fundamenteel grondrecht. De Algemene Verordening Gegevensbescherming (AVG) is er onder meer om te waarborgen dat dit grondrecht wordt gerespecteerd. Het is in onze democratische rechtsstaat van het grootste belang dat juist de overheid geen ongerechtvaardigde inbreuken maakt op de grondrechten van mensen. De overheid is er tenslotte voor de burger en haar handelen moet zorgvuldig en rechtmatig zijn. Daartoe behoort ook dat overheden bij de verwerking van de persoonsgegevens de normen van de AVG in acht nemen. Dat houdt in dat verwerking van persoonsgegevens moet plaatsvinden op een manier die rechtmatig, behoorlijk en transparant is, die gebonden is aan specifieke doelen en die niet verder gaat dan voor het betreffende doel noodzakelijk is. Ook moeten de gegevens juist zijn en moeten passende organisatorische en technische maatregelen zijn genomen voor de beveiliging daarvan. De burger moet erop kunnen vertrouwen dat persoonsgegevens bij de overheid goed zijn beschermd. In de afgelopen jaren hebben zich echter meerdere situaties voorgedaan waarin overheden (zowel op rijksniveau als decentraal) tekort bleken te schieten in de naleving van de AVG. Het rapport dat uw Kamer op 25 januari 2023 is gezonden, doet verslag van een onderzoek naar de naleving van de AVG door overheden. De centrale vraag daarbij luidde: wat zijn de meest voorkomende onduidelijkheden en problemen binnen

kst-32761-304
ISSN 0921 - 7371
's-Gravenhage 2024

overheidsorganisaties bij naleving van de AVG en welke oorzaken vallen daarvoor aan te wijzen?

Het onderzoek

De onderzoekers hebben informatie opgehaald bij onder meer de Auditdienst Rijk (ADR) en de Autoriteit Persoonsgegevens (AP), en hebben daarnaast negen kwalitatieve onderzoeken (door de onderzoekers casestudy's genoemd) gedaan bij verschillende overheidsorganisaties.[1] Getracht is daarbij om een zo goed mogelijk beeld te krijgen van de inrichting van de organisatie, de verdeling van verantwoordelijkheden en het interne toezicht. Hoewel niet zeker is dat met de onderzochte negen organisaties een exact beeld is verkregen van de naleving van de AVG door àlle overheden, is sprake van een representatieve selectie. De belangrijkste typen overheidsorganisaties zijn daarin namelijk vertegenwoordigd. Ook kwam uit de negen kwalitatieve onderzoeken een vrij consistent beeld naar voren.

Het algehele beeld is dat de naleving van de AVG zich positief ontwikkelt. Er komt steeds meer aandacht voor het onderwerp en dit vertaalt zich in de praktijk. Er zijn echter ook aspecten die meer aandacht verdienen, ten eerste de borging van verantwoordelijkheden. Uit de informatie van de ADR en de AP bleek onder meer dat de rollen van verwerkingsverantwoordelijke en verwerker niet altijd helder zijn. Daarnaast is er binnen de organisatie vaak sprake van rolvermenging tussen de Functionaris voor Gegevensbescherming (FG) en de privacy officer. De AP geeft aan dat de onafhankelijkheid van de FG regelmatig onder druk staat.

Daarnaast schat de AP in dat zaken als het uitvoeren van Data Protection Impact Assessments (DPIA's) niet altijd goed geregeld zijn. Ook lijkt er regelmatig sprake te zijn van «dominantie van de doelstelling», wat inhoudt dat gegevensverwerking vaak als oplossing voor problemen wordt gezien in plaats van een middel, zonder alle relevante kaders daarbij goed in te vullen. Ten aanzien van departementen en uitvoeringsorganisaties constateren de AP en de ADR dat er sterke verschillen zijn bij naleving van de AVG bij de overheid. De ADR ziet vooral een rol voor de organisatietop; goede sturing is cruciaal voor naleving binnen de gehele organisatie. Het interne toezicht is naar mening van de AP bij een aantal departementen nog voor verbetering vatbaar. De ADR ziet ook dat de FG in het verleden vaak werd geacht een deel van de verantwoordelijkheid voor gegevensbescherming op te pakken. De ADR constateert dat het primaire proces bij departementen altijd voorrang krijgt en dat daarbij alles zo snel en efficiënt mogelijk moet. Bovendien wil men vanwege bezuinigingen vaak niet investeren in privacybescherming.

De onderzoekers concluderen uit de casestudy's dat het type uitvoeringsorganisatie van invloed kan zijn op de mate van naleving van de AVG. Zij constateren een belangrijk verschil tussen «politieke» overheidsorganisaties en «technische» overheidsorganisaties. Waar laatstgenoemde organisaties op een meer vanzelfsprekende manier de normen van de AVG naleven, is de naleving van privacynormen bij «politieke» organisaties in sterkere mate afhankelijk is van een afweging van belangen. De dominantie van beleidsdoelen kan dan een zwaarwegende factor zijn ten koste van privacynormen; veeleer ligt het accent op de doelmatige uitvoering van primaire processen en komt het aspect van de bescherming van persoonsgegevens daar pas op een later moment als

[1] Een uitvoeringsorganisatie op rijksniveau, een ministerie, drie zelfstandige bestuursorganen (zbo's), drie gemeenten (één van de vier grote steden, een 100.000+ gemeente en een gemeente met 35.000 inwoners) en een waterschap.

aandachtspunt bij. Naleving van de AVG wordt zo te vaak nog gezien als iets dat vooral samenhangt met techniek en beveiliging en minder als een belang dat doorwerkt in alle processen binnen de organisatie. Privacy, zo stellen de onderzoekers naar de mening van het kabinet terecht, behoort echter al aan de voorkant bij de verwerking van gegevens aandacht te krijgen en niet pas nadat de belangrijkste beslissingen reeds genomen zijn.

De onderzoekers stellen vast dat overheden veel hebben gedaan op het vlak van de bescherming van persoonsgegevens. De algemene indruk is dat het op dit moment beter gesteld is met de naleving van privacy-normen door overheden dan voor de komst van de AVG. De AVG heeft zonder twijfel gezorgd voor een toegenomen bewustzijn bij overheden. Dat bewustzijn is ook gevolgd door concrete acties, waardoor het op dit moment duidelijk beter gesteld is met de waarborgen voor zorgvuldige omgang met persoonsgegevens door overheden. De onderzoekers hebben geconstateerd dat de aandacht voor correcte verwerking van persoonsgegevens na invoering van de AVG een positieve ontwikkeling heeft doorgemaakt. De kennis van de AVG bij overheden neemt toe. Dat betekent echter niet dat naleving van de AVG bij de overheid altijd vanzelfsprekend is, wat een zorgelijk gegeven is gezien de rol van de overheid in de maatschappij. Het is vaak geen bewuste keuze. Soms ontbreekt voldoende besef dat het beoordelen van AVG-aspecten vooraf moet gaan aan een verwerking van persoonsgegevens. Slechts zelden is echter expliciet sprake van een keuze om niet na te leven. Dat zijn uitzonderingen die de regel bevestigen: het gaat steeds beter met de naleving van de AVG.

Aanbevelingen

Het onderzoek leidt tot een aantal aanbevelingen gericht op versterking van de naleving van de AVG binnen overheidsorganisaties (hoofdstuk 7).

1. De Minister voor Rechtsbescherming en de Minister van BZK wordt aangeraden om verdere investeringen bij overheidsorganisaties te doen en een stimulerende rol te pakken om zo de privacy-organisatie bij overheden steviger te funderen en privacybewustzijn sterker te verankeren.
2. Bij de overheidsorganisaties is specifiek aandacht nodig voor het tijdig betrekken van privacybelangen bij de ontwikkeling van (wetgevings)projecten die gepaard zullen gaan met verwerking van persoonsgegevens, bijvoorbeeld door het tijdig opstellen van een DPIA en een serieus gesprek over de relevante processen, risico's en data-ethische aspecten.
3. Het *three lines of defense*-model[2] wordt breed toegepast en bewijst zijn waarde. De onderzoekers zien wel dat het invullen van de belangrijke rollen, waaronder aandachtsfunctionarissen in de lijnorganisatie, moeizaam verloopt. Dit vraagt om gerichte investeringen in bestaande medewerkers, maar ook om inzet op de aanbodkant van de arbeidsmarkt door het stimuleren van opleidingen op dit gebied.
4. Organisaties die bij de beoordeling en toetsing een privacy officer en de FG betrekken geven een betere inhoudelijke invulling aan hun

[2] Hierbij zijn het management en de door het management gemandateerde organisatie-onderdelen, inclusief de privacy officers, als eerste lijn primair verantwoordelijk voor de naleving van privacywetgeving. De tweede lijn wordt gevormd door de Chief Information Officer (CIO), een centraal aangestelde functionaris die belast is met ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringsbeleid en met het beheer van de informatiesystemen. De derde lijn wordt gevormd door interne toezichthouders en de Auditdienst Rijk.

verantwoordelijkheden. Voorwaardelijk daarvoor is de aanwezigheid van aandachtsfunctionarissen, contactpersonen of aanspreekpunten in de eerste lijn. De casestudy's laten zien dat deze functionarissen zeer waardevol zijn als ambassadeurs van het privacybeleid van de organisatie. Zij kunnen het privacybewustzijn in de organisatie stimuleren en het belang daarvan bewaken.

5. Voor management en bestuur is het cruciaal dat het belang van privacybescherming wordt benadrukt, in woord en in daad. Dit behelst voorbeeldgedrag, maar ook organisatorische borging van bescherming van privacy in de afweging tegen beleidsdoelstellingen.
6. De AP lijkt als toezichthouder vooral de handhavende taak prioriteit te geven. Vanuit het veld is een duidelijke behoefte aan meer communicatie, voorlichting en sturing door de AP. Specifiek is het wenselijk om meer (informeel) contact mogelijk te maken met een meedenkend en adviserend karakter. Voor zover capaciteitsproblemen op dit vlak terughoudendheid veroorzaken, zou een uitbreiding van die capaciteit mogelijk soelaas bieden.
7. De AP zou op meer punten een bredere taakopvatting kunnen kiezen. Het zou goed zijn als er meer werk gemaakt wordt van terugkoppeling bij ingediende meldingen van datalekken. Ook het systeemgerichte toezicht van de AP (momenteel slechts twee medewerkers) komt voor versterking in aanmerking, door investeringen in de capaciteit en door de bestaande netwerken van FG's effectiever in te zetten.

Reactie

Maatregelen ter versterking van privacy kennis en bewustzijn

De sleutel tot het verbeteren van de bescherming van persoonsgegevens ligt vooral in het versterken en professionaliseren van de AVG-expertise binnen de organisatie. Dan kan het gaan om financiële middelen, maar niet alles is een kwestie van budget. Bewustwording en normbesef zijn begrippen die voor de hele maatschappij gelden: voor iedere burger, ieder bedrijf en iedere organisatie die persoonsgegevens verwerkt. De overheid vormt daarop geen uitzondering. Integendeel: de overheid zou zelf voorop moeten lopen als het gaat om de naleving van wettelijke normen. De overheid heeft immers een voorbeeldfunctie bij de naleving van wettelijke en verdragsrechtelijke normen en burgers moeten erop kunnen vertrouwen dat hun gegevens goed zijn beschermd.

In elk geval geldt hoe meer AVG-bewustzijn er is op besluitvormend niveau, hoe meer voorkomen wordt dat er werkprocessen worden ingericht die indruisen tegen de AVG. Daarom vergroot het kabinet de kennis over de AVG binnen de Rijksoverheid. Met de Algemene Bestuursdienst (ABD) zijn afspraken gemaakt dat in het opleidingstraject van topambtenaren de bewustwording en kennis van de AVG wordt vergroot door middel van een privacy leergang. Deze ambtenaren kunnen immers bij uitstek bepalende invloed uitoefenen op de werkprocessen en daarmee ook op de mate waarin gegevensbeschermingsaspecten in die processen zijn meegenomen. Wanneer de top van een organisatie doordrongen is van het belang van naleving van de AVG, zal dat zijn weerslag hebben op de organisatie als geheel.

Het vergroten van kennis en bewustzijn over de AVG bij alle overheidsorganisaties wordt verder gestimuleerd door het Kenniscentrum van de Interbestuurlijke Datastrategie (IBDS),[3] waarbij verantwoord datagebruik

[3] Het Kenniscentrum van de IBDS is te vinden via: https://realisatieibds.pleio.nl/ en: Over de IBDS Realisatie IBDS (pleio.nl)

voor maatschappelijke opgaven centraal staat, onderdeel van de Werkagenda Waardengedreven Digitaliseren. Het kenniscentrum bevat onder meer een Toolbox verantwoord datagebruik, een wegwijzer voor Privacy Enhancing Technologies (PET's) en een keuzehulp voor dataopleidingen, waaronder over gegevensbescherming en beveiliging.[4] De IBDS doet dit door verantwoord datagebruik te stimuleren en in samenhang te bezien wat er (technisch) kan, mag (juridisch) en wat (ethisch) wenselijk is rondom datagebruik voor het realiseren van maatschappelijke opgaven. Zeker bij nieuwe slimme technologische toepassingen is dit wenselijk, omdat de ervaring leert dat hierdoor ook de mogelijkheden om gegevens te verzamelen en te gebruiken toeneemt, zonder dat niet altijd duidelijk is dat daarmee een risico ontstaat.

Maatregelen om tijdig en integraal privacybelangen mee te wegen

Bij de aanpak van maatschappelijke opgaven, herziening van bestaand beleid of nieuw beleid door het Rijk wordt het Beleidskompas gevolgd. Daarin staan essentiële elementen voor een goede beleidsvoorbereiding, waaronder een paragraaf over het uitvoeren van een DPIA wanneer beleid wordt gemaakt waarin persoonsgegevens worden verwerkt. In 2023 is door BZK een handleiding ontwikkeld om een DPIA Rijksdienst uit te voeren ten aanzien van beleidsstukken. Aan de ontwikkeling van een Rijksmodel DPIA voor Beleidsstukken wetgeving wordt momenteel gewerkt. In de praktijk is namelijk gebleken dat in beleid soms ten onrechte onvoldoende aandacht wordt besteed aan gegevensbeschermingsaspecten. De handleiding zal een verdere stap zijn in het bewustwordingsproces om in een vroeg stadium rekening te houden met deze vraagstukken. Tevens heeft de AP voor raadsleden van gemeenten een handreiking opgesteld die helpt om binnen de gemeente een gesprek te starten over de privacyaspecten van de inzet van technologie.[5] Door deze maatregelen zullen privacyrisico's en benodigde maatregelen eerder worden onderkend waardoor niet meer op het laatste moment of achteraf extra maatregelen nodig zijn.

Daarnaast is in 2023 het DPIA model geactualiseerd onder de vernieuwde naam model DPIA Rijksdienst. Onderdeel van het model is een proceskader. Ook is er een doorontwikkeld afwegingskader (Pre-scan DPIA[6]) beschikbaar gesteld die organisaties binnen de overheid vrijblijvend kunnen gebruiken om een afgewogen inschatting te maken of het uitvoeren van een DPIA noodzakelijk is. Door gebruik te maken van deze modellen wordt in een vroegtijdig stadium de focus gelegd op de grootste privacyrisico's en de benodigde maatregelen.

Het gebruik van dergelijke DPIA's is vaak verplicht voor de overheid en ontzettend belangrijk. Een voorbeeld van het gebruik van zo'n DPIA door de overheid is de DPIA die op verzoek van uw Kamer is uitgevoerd op het gebruik van Facebook Pagina's (Facebook Pages) door de overheid. Uit deze DPIA bleken zeven hoge privacyrisico's voor burgers bij het gebruik van Facebook Pages door de Rijksoverheid. Als bij brief van 19 april jl. (Kamerstuk 32 761, nr. 297) aan uw Kamer medegedeeld is het Ministerie van BZK momenteel in onderhandeling met Meta – de eigenaar van Facebook Pages – over het wegnemen van deze privacyrisico's. De AP heeft bevestigd dat er duidelijkheid moet komen in de rollenverdeling tussen BZK en Meta en dat indien deze duidelijkheid er niet is, adviseert de AP de verwerkingen te beëindigen. Vervolgens moeten ook de in de

---

[4] *Kamerstukken II* 2021/22, 26 643, nr. 797.

[5] https://www.autoriteitpersoonsgegevens.nl/documenten/gemeenten-en-privacy-wat-kunt-u-als-raadslid-doen-bij-de-inzet-van-technologie

[6] Producten/diensten - cip-overheid

DPIA geconstateerde hoge risico's weggenomen worden om gebruik te kunnen blijven maken van Facebook Pages. Tevens is de Europese Commissie hierover geïnformeerd; zij heeft laten weten onze zorgen serieus te nemen en bestudeert hoe dit mee te nemen in haar onderzoeken naar de grote tech platforms. In de hierop volgende weken is er meermaals contact geweest tussen BZK en Meta. Dit heeft recent geresulteerd in een overleg tussen Meta en meerdere ministeries. We zijn verheugd dat we nu concreet in overleg zijn en dat Meta heeft aangegeven er met ons uit te willen komen. Gelet op het feit dat deze gesprekken besloten zijn, kunnen wij uw Kamer op dit moment nog niet over de inhoud berichten. Het volgende kabinet zal de gesprekken met Meta definitief tot een goed einde moeten brengen.

De onderzoekers concluderen dat tijdsdruk en de dominantie van beleidsdoelen een verstorende rol kunnen spelen bij het beoordelen van AVG-aspecten. Het accent ligt dan op de doelmatige uitvoering van primaire processen, waardoor aandacht voor privacyvraagstukken er soms bij inschiet. Het kabinet deelt vanzelfsprekend het belang van goede taakuitvoering van primaire processen en vindt het mede daarom van belang dat gegevensbeschermingsvraagstukken daarvan vanaf een vroegtijdig stadium deel uitmaken, zodat het belang van adequate gegevensbescherming goed wordt geborgd en niet achteraf wordt geconstateerd dat een proces daarmee onvoldoende rekening houdt. Zoals ook de Algemene Rekenkamer vorig jaar schreef in haar brief aan de Tweede Kamer, biedt de AVG voldoende ruimte voor het verwerken van persoonsgegevens voor de uitvoering van overheidstaken.[7] Het verwerken van persoonsgegevens is mogelijk zolang de baten van de verwerking goed zijn afgewogen tegen de gevolgen ervan voor burgers en er een wettelijke basis voor bestaat. De problemen ontstaan niet omdat de AVG zelf een knelpunt is, maar omdat de door de AVG verlangde afweging niet, of niet op tijd, gemaakt is. Daarbij kan het zijn dat voor een vorm van verwerking een wettelijke basis ofwel een grondslag moet worden gecreëerd. Wanneer deze gegevensbeschermingsafweging meteen in de beginfase wordt meegenomen bij een geconstateerd probleem of beleidsdoel, kan de oplossing van dat knelpunt versneld worden. Een dergelijke afweging hoeft dan ook niet in de weg te staan aan primaire processen, mits zij onderdeel is vanaf het beginstadium en niet pas aan bod komt nadat de belangrijkste beslissingen reeds genomen zijn. Elke organisatie dient er dan ook op toe te zien dat naleving van de privacywetgeving in een vroegtijdig stadium bij processen wordt betrokken en dat hier zo nodig intern over wordt gerapporteerd en erop wordt toegezien. De eerder genoemde privacy leergang van de ABD kan daaraan bijdragen, nu deze zorgt voor meer bewustzijn op besluitvormend niveau binnen de Rijksoverheid. Naast deze cursus voor managers is het van belang dat de managers privacy in relatie zien met de andere I-disciplines. Momenteel wordt er aan gewerkt om privacy onderdeel te laten zijn van het I-stelsel waardoor de relatie van privacy met de andere I-disciplines wordt versterkt en aandacht voor privacyaspecten wordt gewaarborgd.

Persoonsgegevens kunnen ook onderdeel uitmaken van de inzet van algoritmen. Vanuit BZK is een Impact Assessment voor Mensenrechten bij de inzet van Algoritmes (IAMA) ontwikkeld. Dat is een vrijwillig instrument dat ondersteuning biedt bij het nakomen van bestaande wettelijke verplichtingen en helpt om AI en algoritmen op verantwoorde wijze te ontwikkelen en in te zetten. Aangezien er bij de inzet van algoritmes ook persoonsgegevens kunnen worden verwerkt is er voor de samenhang

[7] *Kamerstukken II* 2022/23, 32 761, nr. 264

tussen een DPIA en een IAMA een Handreiking gezamenlijk gebruik IAMA en Model DPIA Rijksdienst ontwikkeld.

Vanuit BZK wordt ook actief gewerkt aan de ontwikkeling van een Algoritmekader dat zorgvuldige inzet van algoritmes bevordert bij (overheids)organisaties. Dit kader legt sterk de nadruk op privacy en gegevensbescherming als essentiële pijlers. De vereisten van de AVG worden nauwgezet geïntegreerd in het kader, wat zorgt voor helderheid omtrent de minimale eisen en praktische richtlijnen voor overheidsinstanties gedurende alle fases van de levenscyclus van algoritmische toepassingen.

Daarnaast is er vanuit BZK recent een Kinderrechten Impact Assessment (KIA) en een afwegingskader ontwikkeld om kinderen beter te beschermen bij de inzet van digitale technologieën. Het KIA helpt (overheids)organisaties bij het ontwikkelen of aanbieden van online producten of diensten aan kinderen, zoals voor onderwijs. Het KIA geeft aandacht aan alle mogelijke risico's voor kinderen, waaronder privacy- en gegevensbeschermingsrisico's, en het waarborgen van de rechten en het welzijn van kinderen. Het KIA kan samen met een DPIA en een IAMA geïntegreerd worden uitgevoerd. Daarvoor is een Handleiding opgesteld.

Ter stimulering van de verantwoorde ontwikkeling van dataprojecten van overheidsorganisaties die gepaard gaan met verwerking van persoonsgegevens is er, ook als onderdeel van de IBDS, de Centrale Commissie Gegevensgebruik opgericht, onder voorzitterschap van DG Digitalisering, een Adviesfunctie verantwoord datagebruik opgericht.[8] Het doel van dit loket is om met een advies gegevensdeling mogelijk te maken en kennis te vergaren over (on)duidelijkheden over de knelpunten en om deze kennis vervolgens ook te kunnen delen. Ter structurele borging van dit loket wordt er gewerkt aan de inrichting van een vast interbestuurlijk triageloket voor gegevensdeling. Hiermee worden niet alleen Rijksoverheden maar ook medeoverheden geholpen bij het naleven van de AVG.

Vanuit de Ministeries van JenV en BZK wordt aan de ontwikkeling van (kennis, techniek, normen, processen) PET's een impuls gegeven door middel van een tijdelijke financiering van het Nationaal Innovatie Centrum Privacy Enhancing Technologies (NICPET)[9], een samenwerking tussen de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) en het Centrum Informatiebeveiliging en Privacybescherming (CIP). Met PET's is het mogelijk om veiliger data te analyseren en daarbij privacy te waarborgen. Het is een vorm van dataminimalisatie en kunnen in die zin bijdragen aan een betere naleving van de AVG. PET's kunnen daarnaast, wanneer ze worden toegepast binnen de bestaande wettelijke kaders, een positieve bijdrage leveren aan het aanpakken van maatschappelijke opgaven en handelingsverlegenheid bij (overheids)organisaties wegnemen.

Op 19 oktober 2023 is een Handreiking over de verheldering van het juridisch kader en de beantwoording van de vragenlijst van gemeenten met betrekking tot online onderzoek door gemeenten in het kader van de Openbare Orde en Veiligheid (OOV) gepubliceerd.[10] De documenten zijn in nauwe samenwerking met het Ministerie van BZK, JenV en de Vereniging van Nederlandse Gemeenten (VNG) opgesteld. Dit komt ten goede aan zowel de eenduidigheid waarmee gemeenten handelen ten

---

[8] De Adviesfunctie verantwoord datagebruik is te vinden via https://realisatieibds.pleio.nl/page/view/f896fe3b-f93f-450e-a107-e280cbe8ecf6/adviesfunctie.

[9] https://nicpet.pleio.nl/.

[10] *Kamerstukken II* 2023/24, 32 761, nr. 287.

aanzien van online onderzoek, als aan de rechtszekerheid, omdat duidelijker wordt wat van gemeenten op dit gebied kan worden verwacht. De Handreiking stimuleert tevens gemeenten om actief met hun privacy-organisatie aan de slag te gaan en na te denken over gegevensbescherming als onderdeel van de werkzaamheden in het kader van openbare orde en veiligheid. Ook voor Rijksoverheden bestaat er behoefte aan meer duidelijkheid over wat er is «online» is toegestaan. Dit volgt uit het rapport «Grondslag gezocht» van de onderzoekscommissie Brouwer naar het Land Information Manoeuvre Centre (LIMC) van het Ministerie van Defensie.[11] In dit rapport werd geconcludeerd dat voor de inzet van (sociale) mediamonitoringtools door rijksoverheden een integraal kader ontbreekt. De Ministeries van JenV en BZK zullen gezamenlijk het voortouw nemen om een integraal kader te ontwikkelen.

Voorts geeft de op 16 november 2023 uitgebrachte Handleiding Privacy by Design (PbD) van het Ministerie van JenV een praktisch overzicht van de stappen die op het gebied van privacy en gegevensbescherming moeten worden doorlopen bij de ontwikkeling van nieuw beleid of het ontwerp van nieuwe systemen waarmee persoonsgegevens worden verwerkt.[12]

Vanuit het Ministerie van BZK is op 11 december 2023 een voorlopig standpunt gepubliceerd voor Rijksorganisaties bij het gebruik van generatieve AI met daarin aandacht voor het naleven van geldende wet- en regelgeving, waaronder de AVG.[13] Het standpunt wordt verder uitgewerkt in een Handreiking voor Rijksorganisaties bij het gebruik van generatieve AI. Verschillende acties worden ondernomen om het gebruik van generatieve AI binnen de Rijksoverheid op een veilige en verantwoorde manier te bevorderen, waaronder het opzetten van een community om overheidsbreed van elkaar te leren, kennisdeling via trainingen (via de RijksAcademie voor Digitalisering en Informatisering Overheid) en andere bijeenkomsten via de community over de mogelijkheden voor veilig gebruik van generatieve AI. Ook worden interbestuurlijke inkoopvoorwaarden aangescherpt met het oog op generatieve AI, waarbij publieke waarden als veiligheid, transparantie, non-discriminatie, privacy- en gegevensbescherming worden geborgd.

Tot slot is een AVG-register door de Rijksoverheid ontworpen voor ministeries, zodat deze voldoen aan de transparantie- en verantwoordingverplichtingen uit de AVG.[14] Alle ministeries in Nederland kunnen het AVG-register gebruiken om de verwerkingsactiviteiten te publiceren. Het AVG-register biedt naast transparantie de mogelijkheid om verantwoording af te leggen. Het AVG-register wordt daarnaast gebruikt door de FG's voor het houden van toezicht. Het gepubliceerde deel van het AVG-register geeft inzicht in welk type gegevens wordt verwerkt, waarvoor deze gegevens zijn verzameld, wat er met de gegevens wordt gedaan en wie er verantwoordelijk is voor de verwerking.

Maatregelen om privacygovernance te versterken en borgen

In de werkagenda Waardengedreven Digitaliseren is opgenomen dat het Ministerie van JenV en het Ministerie van BZK onderzoeken hoe overheidsorganisaties kunnen worden ondersteund op het gebied van verantwoord datagebruik en privacy.[15] In deze actie is het verkennen van een introductie van een Chief Privacy Officer (CPO) bij departementen, in

---

[11] *Kamerstukken II* 2022/23, 32 761, nr. 258.
[12] Handleiding Privacy by Design, online via: Handleiding Privacy by Design (pleio.nl).
[13] *Kamerstukken II* 2023/24, 26 643, nr. 1125.
[14] https://www.avgregisterrijksoverheid.nl/
[15] *Kamerstuk* 26 643, nr. 940.

de tweede lijn van het *three lines of defence*-model een van de resultaten. De verkenning van de introductie van een CPO binnen departementen of binnen CIO Rijk is medio 2023 gestart en loopt tot en met het eerste kwartaal van 2024. De verkenning van de rol en taken van CPO vindt in nauwe samenwerking plaats met de departementale FG's. Het opstellen van een profiel en het positioneren van een CPO binnen het *three lines of defence*-model wordt duidelijkheid verschaft over de rol en taken van de CPO in relatie tot de FG. De CPO's zullen in 2024 worden opgenomen in het vernieuwde CIO-stelsel waardoor de interdepartementale samenwerking wordt versterkt.

Ook bij gemeenten wordt gewerkt aan het waarborgen van een goede privacygovernance. Vanuit de Informatiebeveiligingdienst (IBD) van de Vereniging van Nederlandse Gemeenten (VNG) zijn functieprofielen voor gemeentelijke privacy officers (PO) en de FG opgesteld.

Maatregelen om de rol van de FG te versterken en borgen

De verantwoordelijkheid voor de naleving van de AVG ligt uiteindelijk bij de verwerkingsverantwoordelijke onder de AVG, dat is ook logisch: alleen deze partij kan het eigen gedrag aanpassen. Organisaties moeten zichzelf als het ware «doorlichten». Overheidsorganisaties zijn bijna altijd verplicht een FG aan te stellen.[16] De FG is de onafhankelijke, interne toezichthouder op de toepassing en naleving van de privacywetgeving binnen de organisatie en vormt het schakelpunt met de externe toezichthouder (AP). De FG kan ook aan de bel trekken bij misstanden en monitort de organisatie doorlopend. Zo'n FG moet – ingevolge de wettelijke verplichtingen uit de AVG -tijdig en naar behoren worden betrokken door het management van de organisatie en moet voldoende toegang en middelen krijgen om de taken te kunnen vervullen en de deskundigheid in stand te houden.

Het kabinet vindt de rol van FG binnen een organisatie en daarmee ook binnen de overheid van groot belang. Dit belang is onlangs ook benadrukt in een onderzoeksrapport van het Europees Comité voor gegevensbescherming (EDPB) over de positie van de FG binnen organisaties.[17] De Minister voor Rechtsbescherming heeft een verkenning uitgevoerd naar de wenselijkheid en haalbaarheid van een openbaar (kwaliteits)register voor FG's. Door de positie van de FG verder te professionaliseren wordt een belangrijke stap gezet in het versterken van dat toezicht, ook voor overheidsorganisaties. Een FG is de interne toezichthouder op adequate gegevensbescherming binnen organisaties en is verplicht voor overheidsorganisaties en diverse andere sectoren en organisaties. Specifiek voor de overheid heeft het kabinet in de Geactualiseerde Werkagenda Waardengedreven Digitaliseren 2024 het streven opgenomen dat inzicht wordt verkregen in hoe de positie en competenties van FG's kunnen worden versterkt en hoe een FG register en kwaliteitseisen voor de overheid kunnen worden opgezet.[18]

De rol en taken van een FG zijn in grote lijnen wettelijk vastgelegd in de AVG, maar in de praktijk blijkt het inhoudelijke niveau en de positionering van de ruim 10.000 FG's in Nederland nogal uiteen te lopen. De grote verschillen tussen FG's vragen om nadere beoordeling en mogelijke borging van de eisen die aan de beroepsgroep zouden kunnen worden

---

[16] Met uitzondering van gerechten of onafhankelijke rechterlijke autoriteiten **die handelen in het kader van hun gerechtelijke taken.** Voor andere taken zijn zij wel verplicht om een FG aan te stellen.

[17] https://www.autoriteitpersoonsgegevens.nl/actueel/europees-onderzoek-positie-fg-moet-beter.

[18] *Kamerstukken II* 2023/24, 26 643, nr. 973.

gesteld. Een openbaar (kwaliteits)register voor erkende FG's zou kunnen bijdragen aan die kwalitatieve impuls, zo bleek uit de genoemde verkenning. Er wordt momenteel gewerkt aan de praktische kanten van zo'n (kwaliteits)register, waaronder toetsingscriteria en -procedure, voorwaarden voor toelating tot het register en adequate bescherming van de gegevens in het register. Het is de verwachting en intentie om in de loop van 2024 te kunnen komen tot de concrete oprichting en daarmee de operationele start van het Nationaal Register voor FG's (NRFG). Ook voor dit vervolgtraject is JenV de opdrachtgever. De markt wordt actief betrokken bij de oprichting van het (kwaliteits)register om zo de uitvoerbaarheid, maatschappelijke betrokkenheid en de bekendheid van het (kwaliteits)register te vergroten. Hoewel met de oprichting van het (kwaliteits)register een belangrijke stap wordt gezet in het versterken van de positie van de FG, blijft JenV in gesprek treden met onder andere de AP om te bezien op welke wijze deze positie nog verder kan worden versterkt, waaronder de optimale positionering van de FG binnen de organisatie.

De Autoriteit Persoonsgegevens

Tot slot doen de onderzoekers aan de AP enkele aanbevelingen die zien op de taakuitoefening van de AP.

Op grond van de AVG is elke lidstaat ertoe verplicht een onafhankelijke autoriteit verantwoordelijk te maken voor het toezicht op de toepassing van de verordening. Voor Nederland is dat de AP. In artikel 52 AVG is vastgelegd dat de toezichthoudende autoriteit volledig onafhankelijk optreedt bij de uitvoering van de taken en de uitoefening van de bevoegdheden die haar overeenkomstig de AVG zijn toegewezen. De leden van de toezichthoudende autoriteit dienen bovendien bij de uitvoering van hun taken en bevoegdheden overeenkomstig de AVG vrij blijven van al dan niet rechtstreekse externe invloed van wie dan ook. Daarmee ligt de onafhankelijkheid van de AP vast, en kan ook het kabinet geen bemoeienis hebben – direct of indirect – met de uitvoering van de taken en de uitoefening van de bevoegdheden van de AP overeenkomstig de AVG. Het is dan ook aan de AP zelf om te bezien of en hoe opvolging wordt gegeven aan de aanbevelingen van de onderzoekers.

Tot slot

De naleving van de AVG blijft in veel gevallen mensenwerk. Dat betekent dat nooit helemaal kan worden uitgesloten dat de naleving in voorkomende gevallen tekortschiet. Waar het echter gaat om factoren die een rol spelen bij structurele tekortkomingen, meent het kabinet met de hiervoor genoemde initiatieven te beschikken over een evenwichtig pakket aan stappen dat de naleving van de AVG binnen overheidsorganisaties zal bevorderen.

De Minister voor Rechtsbescherming,
F.M. Weerwind

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen