pro facto

Verkennende analyse

Naleving van de AVG door overheden

Groningen, december 2022

www.pro-facto.nl

rijksuniversiteit groningen

Colofon

Pro Facto
Ossenmarkt 5
9712 NZ Groningen
www.pro-facto.nl
info@pro-facto.nl
050-3139853

Auteurs	Prof. dr. Heinrich Winter, dr.ir. Bieuwe Geertsema, mr. Thijs Drouen, mr. Ernst van Bergen, mr. Christian Boxum
Opdrachtgever	WODC
Datum	december 2022
Status	Eindrapport

Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum – uitgevoerd door Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs.

Begeleidingscommissie:
Prof. dr. A.J.A. (Bert) Felling, emeritus hoogleraar methodenleer, Radboud Universiteit (voorzitter)
Prof. dr. L. (Leonie) Heres-van Rossum, bijzonder hoogleraar integriteit lokaal bestuur, Erasmus universiteit, docent en onderzoeker USBO, Universiteit Utrecht
Prof. Dr. E. (Elianne) van Steenbergen, bijzonder hoogleraar psychologie van toezicht, Universiteit Utrecht en senior toezichthouder gedrag & cultuur bij de Autoriteit Financiële Markten
Mr. R. (Robbert) de Groot, senior beleidsmedewerker, ministerie Justitie en Veiligheid
Dr. L. (Leontien) van der Knaap, projectbegeleider WODC

Voor de inhoud van het rapport zijn de onderzoekers verantwoordelijk. Het leveren van een bijdrage (als medewerker van een organisatie of als lid van de begeleidingscommissie) betekent niet automatisch dat de betrokkene instemt met de gehele inhoud van het rapport. Dat geldt eveneens voor het ministerie van Justitie en Veiligheid en zijn minister.

© 2022 WODC, ministerie van Justitie en Veiligheid. Auteursrechten voorbehouden.

Samenvatting

Inleiding

Overheden dienen bij de verwerking van de persoonsgegevens de normen van de Algemene Verordening Gegevensbescherming (AVG) in acht te nemen: de verwerking moet plaatsvinden op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is, gebonden zijn aan specifieke doelen en mag niet verder gaan dan voor het betreffende doel noodzakelijk is. De verwerkingsverantwoordelijke – degene die het doel en de middelen van de gegevensverwerking bepaalt – moet ervoor zorgen dat de gegevens juist zijn, passende organisatorische en technische maatregelen nemen voor de beveiliging daarvan en kunnen aantonen dat de gegevens zorgvuldig worden verwerkt. De overheid heeft een voorbeeldfunctie bij de naleving van wettelijke en verdragsrechtelijke normen en burgers moeten erop kunnen vertrouwen dat hun gegevens 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. Op 28 juni 2021 is door de minister van Binnenlandse Zaken en de minister voor Rechtsbescherming overeengekomen dat onderzoek moet worden gedaan naar de naleving van de AVG door overheden. Dit rapport doet verslag van dat onderzoek.

Vraagstelling en onderzoeksthema's

Doel van het onderzoek is het schetsen van een beeld van de naleving van de AVG door overheden. De centrale vraag luidt als volgt:

Wat zijn de meest voorkomende onduidelijkheden en problemen binnen overheidsorganisaties bij naleving van de AVG en welke oorzaken vallen daarvoor aan te wijzen?

Voor de beantwoording van deze vraag hebben we een verkenning van het huidige beeld over de naleving van de AVG door overheden opgesteld, dat vervolgens door middel van een negental casestudy's bij verschillende overheidsorganisaties is verdiept. Aan de hand van de verkenning en casestudy's is een nieuw beeld geschetst, op basis waarvan een aantal aanbevelingen is geformuleerd.

Onderzoeksaanpak

We beschrijven in hoofdstuk 2 dat een uitgangspunt van het onderzoek was om vanuit het bestaande beeld van naleving van de AVG door overheden verbredend en verdiepend onderzoek te doen. Daarvoor zijn we gestart met een aantal oriënterende gesprekken met het oog op het verzamelen van nadere informatie over het onderzoeksonderwerp. Vervolgens is het onderzoek uitgevoerd aan de hand van negen casestudy's bij verschillende overheidsorganisaties: een uitvoeringsorganisatie op rijksniveau, een ministerie, drie zelfstandige bestuursorganen (zbo's), drie gemeenten en een waterschap. We selecteerden een uitvoeringsorganisatie en zbo's op verschillende beleidsterreinen en van uiteenlopende grootte. Datzelfde geldt voor de gemeenten die we selecteerden, namelijk één van de vier grote steden, een 100.000+-gemeente en een gemeente met 35.000 inwoners. Als decentraal, functioneel bestuursorgaan kozen we voor een waterschap van een gemiddelde omvang.

De eerste stap in een casestudy was deskresearch waarin op basis van de beschikbare documenten om een zo goed mogelijk beeld te vormen van de inrichting van de (privacy-)organisatie, de verdeling van verantwoordelijkheden en het interne toezicht. Vervolgens zijn interviews afgenomen met interne functionarissen (alle FG's en vaak ook (chief) privacy officers), andere medewerkers in de privacy-organisatie, medewerkers of managers in de lijnorganisatie en iemand vanuit het bestuur of de directie. Aan het eind van het onderzoek hebben we in een expertmeeting de bevindingen en de voorlopige analyse voorgelegd en hierop gereflecteerd met de experts.

Juridisch kader

De AVG en de Uitvoeringswet AVG (UAVG) vormen het juridisch kader (hoofdstuk 3) voor dit onderzoek). Hierin is geregeld welke rollen van belang zijn bij de verwerking van persoonsgegevens en welke wettelijke grondslagen bestaan voor de verwerking van persoonsgegevens. Voor overheden zijn de relevante grondslagen gebaseerd op de noodzakelijkheid van gegevensverwerking voor 1) het voldoen aan een wettelijke verplichting die op de betreffende overheid als verwerkingsverantwoordelijke rust (artikel 6, lid 1, onder c van de AVG) of voor 2) de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van openbaar gezag dat de verwerkingsverantwoordelijke is opgedragen (artikel 6, lid 1, onder e van de AVG). In het juridisch kader gaan we vervolgens in op vereisten die gelden voor de verwerking, de technische en organisatorische verplichtingen die daaruit voortkomen, en het instrumentarium dat de verwerkingsverantwoordelijke daarbij ter beschikking staat.

Bestaand beeld

De eerste fase van het empirische onderzoek betrof het in kaart brengen van het bestaande beeld van de naleving van de AVG door overheden (hoofdstuk 4). Hiervoor hebben we informatie opgehaald bij de Vereniging Nederlandse Gemeenten (VNG), de Auditdienst Rijk (ADR), de Autoriteit Persoonsgegevens (AP) en een onafhankelijk expert die zich laat inhuren als extern FG bij meerdere gemeenten, aangevuld met anekdotische bevindingen uit andere publicaties.

Hierbij moet worden opgemerkt dat het beeld van naleving bij deze gesprekspartners beperkt is. Het beeld van de AP (de toezichthouder) is ten eerste beperkt door de mate waarin de onder toezicht gestelde overheden signalen over datalekken melden. Daarnaast zijn namens de toezichthouder slechts twee medewerkers belast met het proactief, systeemgericht

toezicht op de gehele sector overheid. Het jaarlijks opgestelde 'sectorbeeld' voor de overheid zou een waardevolle bron kunnen zijn geweest voor dit onderzoek, maar dit is enkel voor interne informatievoorziening bedoeld en is niet aan ons ter beschikking gesteld. Ook de ADR en de VNG hebben een beperkt beeld, voortkomend uit audits en signalen die hen bereiken in hun adviseringstaken.

De indruk van de gesprekspartners is dat gemeenten niet altijd voldoende kennis hebben van de relevante wet- en regelgeving en de toepassing ervan, terwijl daar veel persoonsgegevens worden verwerkt. De rollen van verwerkingsverantwoordelijke en verwerker zijn niet altijd helder en binnen de privacyorganisatie is vaak sprake van rolvermenging tussen de FG en de privacy officer. De AP schat in dat zaken als DPIA's en borging van verantwoordelijkheden niet altijd goed geregeld zijn en dat de onafhankelijkheid van de FG regelmatig onder druk staat. Tegelijk lijkt er regelmatig sprake te zijn van 'dominantie van de doelstelling', wat inhoudt dat gegevensverwerking vaak als oplossing voor problemen wordt gezien, zonder alle relevante kaders daarbij goed in te vullen. Het algehele beeld is dat de naleving zich positief ontwikkelt. Er komt steeds meer aandacht voor het onderwerp en dit vertaalt zich in de praktijk.

Ten aanzien van departementen en uitvoeringsorganisaties constateren de AP en de ADR dat er sterke verschillen zijn bij naleving van de AVG, soms per departement en soms zelfs per afdeling. 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 FG's in het verleden vaak werden 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. Over de gehele linie zijn overigens de ontwikkelingen in de laatste jaren wel positief, mede naar aanleiding van de invoering van de AVG.

Bevindingen uit de casestudy's

In hoofdstuk 5 zijn de beknopte verslagen van de negen casestudy's gepresenteerd. In hoofdstuk 6 zijn de belangrijkste overeenkomsten en verschillen op een rij gezet.

Typen organisaties
Het type uitvoeringsorganisatie kan van invloed zijn op naleving van de AVG. Overheidsorganisaties die werken met bijzondere persoonsgegevens zijn zich sterker bewust van het belang van de AVG en hebben steeds een goed uitgewerkte privacy-organisatie ingericht. In kleinere organisaties lijken privacyfunctionarissen makkelijke herkenbaar en benaderbaar, terwijl in grote organisaties in personele zin meer mogelijkheden bestaan om gekwalificeerde medewerkers aan te trekken en aan zich te binden.

Beleid en organisatie
Bij alle bestudeerde organisaties zagen we dat er een actueel en compleet privacybeleid is opgesteld. Bij alle organisaties zien we een vorm van het *three lines of defence*-model met het bestuur als verwerkingsverantwoordelijke (waarbij deze verantwoordelijkheid gemandateerd wordt in de lijnorganisatie), privacyfunctionarissen (CPO en andere privacy officers) als ondersteuning en een FG als adviseur en toezichthouder. In de tweede lijn zijn ook vaak de security

officer en de Chief Information Officer gepositioneerd, die verantwoordelijk zijn voor het informatievoorzienings- en digitaliseringsbeleid en het beheer van de informatiesystemen.

De praktijksituatie
In de casestudy's hebben we niet kunnen vaststellen hoe het precies is gesteld met de naleving van de AVG in het concrete handelen van medewerkers. Hooguit hebben we op basis van beschikbare documenten en uitspraken van betrokkenen in algemene zin het nalevingsniveau kunnen bepalen en/of de richting waarin zich dat ontwikkelt.

We hebben geconstateerd dat bij alle organisaties veel aandacht is voor kennisontwikkeling en het belang van houding en gedrag. We zien wel dat het kennisniveau tussen medewerkers verschilt en nog niet altijd voldoende is. Hierbij speelt mee dat het gegevensbeschermingsrecht een ingewikkeld rechtsgebied is en antwoorden op vragen niet altijd eenvoudig te geven zijn. Vervolgens spelen tijdsdruk en de dominantie van beleidsdoelen een verstorende rol; vooral bij het bestudeerde departement en gemeenten zien we dit effect in sterke mate terugkomen.

We zien bij het bestuur en management van de bestudeerde organisaties dat die over het algemeen relatief veel aandacht hebben voor het belang van naleving van de AVG, maar dat opvolging van adviezen vanuit de privacy-organisatie soms toch achterwege blijft. Extra complicerend is dat AVG-vragen en uitdagingen door de eerste lijn vaak laat of zelfs niet worden herkend. Het opstellen van DPIA's is niet altijd op orde; dit gebeurt soms te laat en soms op basis van onvoldoende privacy-expertise. De protocollen voor datalekken zijn doorgaans wel goed opgesteld en worden ook goed nagevolgd.

Knelpunten
Naast het hierboven genoemde knelpunt van dominantie van beleidsdoelen en doelmatigheidsoverwegingen, is een tweede knelpunt de bezetting van posities in de privacy-organisatie, mede vanwege de krappe arbeidsmarkt. Hierdoor worden privacyfunctionarissen soms uit hun rol getrokken vanwege ontbrekende kennis of capaciteit elders in de organisatie. Als derde knelpunt zien we dat naleving van de AVG soms wordt vertaald naar een sterke focus op techniek en beveiliging, maar minder naar de bescherming van persoonsgegevens en het waarborgen van dat belang in alle processen binnen de organisatie.

Conclusie
In de casestudy's blijft het beeld overeind dat aandacht voor correcte verwerking van persoonsgegevens na invoering van de AVG een positieve ontwikkeling heeft doorgemaakt, maar nog niet op het gewenste niveau is. De kennis van de AVG bij overheden neemt toe. Maar dat betekent niet dat naleving van de AVG altijd vanzelfsprekend is. Dat is vaak geen bewuste keuze. Soms ontbreekt voldoende besef dat het beoordelen van AVG-aspecten vooraf moet gaan aan een verwerking van persoonsgegevens. Een enkele keer is expliciet sprake van een keuze om niet na te leven, en is de beleidsdoelstelling leidend ten koste van AVG-naleving. Dan zou echt gesproken kunnen worden van tekortkomingen op 'willen'. Maar dat zijn eerder de uitzonderingen die de regel, het gaat steeds beter met de naleving van de AVG, bevestigen.

Aanbevelingen
Het onderzoek leidt tot een aantal aanbevelingen gericht op versterking van de naleving van de AVG binnen overheidsorganisaties (hoofdstuk 7). We presenteren deze aanbevelingen hier op beknopte wijze.

- We raden de minister voor Rechtsbescherming en de minister van BZK aan 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.
- Bij de overheidsorganisaties is specifiek is aandacht nodig voor het tijdig betrekken van privacybelangen bij de ontwikkeling van projecten die gepaard zullen gaan met verwerking van persoonsgegevens, bijvoorbeeld door het tijdig opstellen van een DPIA na een serieus gesprek over de relevante processen, risico's en data-ethische aspecten.
- Het *three lines of defense*-model wordt breed toegepast en bewijst zijn waarde. We 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.
- Organisaties die bij de beoordeling en toetsing een privacy officer en de FG betrekken geven een betere inhoudelijke invulling aan hun 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.
- 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.
- 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.
- 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 het bestaande netwerk van FG's effectiever in te zetten.


pro facto