pro facto

Verkennende analyse

Naleving van de AVG door overheden

Groningen, december 2022

Click or tap here to enter text.

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.

Lijst van afkortingen

ADR	Auditdienst Rijk
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BIO	Baseline informatiebeveiliging overheid
CDO	Chief Data Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
DPIA	Data Protection Impact Assessment
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	Functionaris voor gegevensbescherming
IBP	Informatiebeveiliging en privacy
IBD	Informatiebeveiligingsdienst
ISMS	Information Security Management System
ISO	International Organization for Standardization
JZ	Juridische zaken
MT	Managementteam
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NEN	Nederlands Normalisatie Instituut
PDCA	Plan-Do-Check-Act
PIT	Privacy en informatieveiligheidsteam
UAVG	Uitvoeringswet algemene verordening gegevensbescherming
VNG	Vereniging van Nederlandse gemeenten
Wbp	Wet bescherming persoonsgegevens
Wpg	Wet politiegegevens
Zbo	Zelfstandig bestuursorgaan

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.

Inhoud

1 Inleiding

1.1 Inleiding

Op 27 april 2016 hebben het Europees Parlement en de Raad van de Europese Unie de Algemene Verordening Gegevensbescherming (AVG) vastgesteld. Deze verordening bevat regels over de verwerking van persoonsgegevens binnen de Europese Unie. Artikel 5 AVG omschrijft de beginselen waar de verwerking van persoonsgegevens aan moet voldoen: 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.

Ook overheden dienen bij de verwerking van de persoonsgegevens de normen van de AVG in acht te nemen. In de afgelopen jaren hebben zich echter meerdere situaties voorgedaan waarin overheden tekort bleken te schieten in de naleving van de AVG. Dit geldt zowel voor overheidsorganisaties op landelijk niveau als voor decentrale overheidsorganisaties. Een aantal van deze situaties zijn ook in de Tweede Kamer besproken, zoals bijvoorbeeld:

— In november 2020 kwam naar buiten dat het Land Information Manoeuvre Centre (LIMC) van het ministerie van Defensie vanaf half maart 2020 op grote schaal gegevens over de Nederlandse samenleving verzamelde om zicht te krijgen op de coronacrisis en op de verspreiding van desinformatie en dat hiervoor geen mandaat bestond.[1]
— In januari 2021 werd bekend dat een aantal medewerkers van de GGD in de tweede helft van 2020 persoonsgegevens uit de systemen voor coronatests en bron- en contactonderzoek te koop hebben aangeboden.[2]
— In januari 2021 werd bekend dat het Centraal Orgaan Opvang Asielzoekers (COA) jarenlang persoonsgegevens van asielzoekers had gedeeld met de politie, zonder dat daar een grondslag voor was.[3]

[1] E. Rosenberg & K. Berkhout, 'Hoe defensie de eigen bevolking in de gaten houdt', *NRC* 15 november 2020.
[2] RTL Nieuws, 'Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD', 25 januari 2021, te raadplegen via rtlnieuws.nl.
[3] M. Kuiper & R. van der Poel, 'Grapperhaus erkent: delen van gegevens asielzoekers met politie was onrechtmatig', *NRC* 18 januari 2021.

— In april 2021 kreeg de gemeente Enschede een boete opgelegd door de Autoriteit Persoonsgegevens. Tussen mei 2018 en mei 2020 had de gemeente 'wifi-tracking' ingezet en daarbij telefoons van burgers geregistreerd, zonder de privacy goed te waarborgen.[4]

Tekortkomingen in de naleving van de AVG door overheidsorganisaties hebben op meerdere momenten tot parlementaire discussie geleid. In hun antwoord op Kamervragen van 15 januari 2021 over onrechtmatige verwerking van persoonsgegevens hebben de minister voor Rechtsbescherming, de minister van Justitie en Veiligheid, de minister van Defensie en de minister van Sociale Zaken en Werkgelegenheid aangegeven dat de overheid voorop dient te lopen bij de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens. 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.[5] 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.

1.2 Vraagstelling en onderzoeksthema's

Het onderzoek heeft tot doel een beeld te schetsen van de naleving van de AVG door overheden. De centrale vraag is: wat zijn de meest voorkomende onduidelijkheden en problemen binnen overheidsorganisaties bij naleving van de AVG en welke oorzaken vallen daarvoor aan te wijzen? Deze vraag is beantwoord aan de hand van een verkenning van het huidige beeld over de naleving van de AVG door overheden, dat vervolgens door middel van casestudy's bij een negental 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.

Wij onderscheiden de volgende onderzoeksthema's en deelvragen.

Onderzoeksthema I: verkenning huidig beeld
Het eerste onderzoeksthema bestaat uit de verkenning van het huidige beeld van de naleving van de AVG door overheden, de wijze waarop dat beeld tot stand komt en de lacunes daarin. We beantwoorden de volgende vragen:

1. Op welke manier kunnen overtredingen door overheidsorganisaties in beeld komen?
2. Welke instanties zijn betrokken bij het in beeld krijgen van deze overtredingen?
3. Wat is het huidige beeld van de naleving van de AVG en gerelateerde wet- en regelgeving?
4. Wat zijn mogelijke lacunes in de kennis van de naleving?
5. Welke selectie van cases geeft de beste kansen om tot een actueel beeld te komen van overtredingen door overheidsinstanties en de onderliggende redenen?

Onderzoekthema II: casestudy's
Op basis van het huidige beeld van de naleving van de AVG zoals dat in onderzoeksthema I is beschreven, hebben wij een negental overheidsorganisaties geselecteerd dat we in evenveel

[4] NOS, *Privacywaakhond legt Enschede boete op van 600.000 euro vanwege wifitracking*, 29 april 2021, https://nos.nl/artikel/2378665-privacywaakhond-legt-enschede-boete-op-van-600-000-euro-vanwege-wifitracking, geraadpleegd op 1 december 2022.
[5] Aanhangsel Handelingen II 2020/2021, nr. 2287, p. 1.

casestudy's nader onder de loep hebben genomen. In het kader van de casestudy's zijn de volgende vragen beantwoord:

6. Hoe luidt het privacybeleid bij de bestudeerde overheidsorganisaties en hoe is de privacy-organisatie ingericht?
7. Welke onduidelijkheden, problemen en risico's kunnen binnen de bestudeerde overheidsorganisaties worden onderscheiden bij de naleving van de AVG?
8. Hoe werken de interne toezichtsmechanismen op de naleving van de AVG door deze overheidsorganisaties en hoe was de rol van de functionaris voor gegevensbescherming (FG) in het proces geborgd?

Onderzoeksthema III: analyse en veralgemenisering van het verkregen beeld
In het derde onderzoeksthema nemen wij de bevindingen uit de verkenning van het huidige beeld en de casestudy's samen om tot een rijker ingevuld beeld van de naleving van de AVG door overheden te komen. In dat verband zijn de volgende vragen beantwoord:

9. Welke overeenkomsten zijn er te vinden in de cases?
10. Welke verschillen zijn geconstateerd? Wat zijn de verklarende factoren voor deze verschillen?
11. In hoeverre zijn de bestudeerde cases naar verwachting representatief voor de situatie bij overheidsorganisaties in het algemeen?
12. Wat zegt bovenstaande over de algemene situatie (uitgesplitst naar de vragen 6 - 8)?
13. Welke lacunes bevat het opgestelde beeld van de algemene situatie? Hoe zijn deze eventueel nog in te vullen?
14. Welke aanbevelingen kunnen worden gedaan om de naleving van de AVG door overheidsorganisaties te verbeteren?

1.3 Leeswijzer

In hoofdstuk 2 wordt de onderzoeksaanpak nader uiteengezet. Hoofdstuk 3 schetst het juridisch kader voor de verwerking van persoonsgegeven door overheden. Hoofdstuk 4 bevat een beschrijving van het huidige algemene beeld dat bestaat van de naleving van de AVG door overheden; hoofdstuk 5 bevat de bevindingen uit de casestudy's. In hoofdstuk 6 worden de bevindingen uit het onderzoek, het huidige algemene beeld en de bevindingen uit de casestudy's nader geanalyseerd. In hoofdstuk 7 worden de onderzoeksvragen beantwoord en aanbevelingen geformuleerd.

2 Onderzoeksaanpak

2.1 Inleiding

In dit hoofdstuk beschrijven we de onderzoeksmethoden en het kader dat is gebruikt bij de uitvoering van de casestudy's en bij de analyse van de resultaten daarvan. De beschrijving van de onderzoeksmethoden is opgenomen in paragraaf 2.3. We beginnen het hoofdstuk met het schetsen van het kader voor de casestudy's.

2.2 Kader voor de casestudy's

De belangrijkste methode van gegevensverzameling die we in het onderzoek hanteerden is de uitvoering van casestudy's. In deze paragraaf schetsen we een kader voor het casestudy-onderzoek. Dat kader bestaat uit elementen die functioneerden als richtingaanwijzers tijdens onze zoektocht naar factoren die de naleving van de AVG bij overheden bevorderen of belemmeren. Door dat kader hebben we ons ook laten leiden bij het analyseren van de bevindingen uit de casestudy's. We hanteren dat kader nadrukkelijk niet als theorie. De reden daarvoor is dat het onderzoek overwegend een verkennend karakter kent. Voor een theorie-toetsend onderzoek beschikken we over te weinig informatie over de praktijk van de naleving van de AVG bij overheden. Voor de beschrijving van die praktijk hebben we gekozen voor het gebruik van twee conceptuele modellen die we als zoeklicht en ter inspiratie in het onderzoek hanteerden. Het gaat om het AMO-model en de Tafel van Elf. Hierna gaan we daarop wat dieper in.

AMO-model
Het AMO-model is een model dat gedrag van individuen verklaart en dat onderscheid maakt tussen abilities (kunnen), motivation (willen) en opportunities (mogen).[6] We hebben inzichten uit dit model verlegd naar het aggregatieniveau van de organisatie. En we hebben 'kunnen, willen en mogen' omgezet in 'weten, willen en kunnen'. Daarmee bewegen we ons dus strikt genomen niet langer op het niveau waarop het AMO-model zich richt en hanteren we ook andere elementen.

De wijziging van het aggregatieniveau is ingegeven door de noodzaak om ons in het onderzoek te richten op de naleving van de AVG door overheden. Uiteraard wordt de naleving van de AVG door een overheidsorganisatie bepaald door het gedrag dat medewerkers binnen die

[6] E. Appelbaum, T. Bailey, P. Berg, & A. Kalleberg, *Manufacturing advantage: Why high-performance work systems pay off*, Cornwell University Press: Ithaca 2000.

organisatie vertonen. Maar in een onderzoek als het onderhavige is het niet mogelijk te focussen op het gedrag van individuele medewerkers. Dat zou wellicht kunnen als we ons op de naleving binnen een enkele overheidsorganisatie hadden gericht, maar daarmee zouden we geen antwoord kunnen geven op de onderzoeksvraag. Dan zou het de ministers ook bijna onmogelijk maken aan de Tweede Kamer te rapporteren over de naleving van de AVG door de overheid. Verder hebben we de factoren waarnaar we in het onderzoek op zoek zijn afgeleid van het AMO-model, maar hebben we daarin wel gevarieerd. Door te kiezen voor 'weten, willen en kunnen', sluiten we goed aan bij de factoren die – volgens de bevindingen uit enkele oriënterende interviews – bij overheden van belang lijken te zijn als het gaat om de naleving van de AVG.

Bij de naleving van de AVG door overheden is in de eerste plaats – 'weten' – de kennis binnen de organisatie van belang, van zowel de regels van de AVG als van de technische middelen die worden ingezet. We letten daarbij op de scholing en training van medewerkers en bijscholingsactiviteiten. Ook kijken we naar manieren waarop het bewustzijn van het belang van het waarborgen van privacybelangen in de organisatie wordt bevorderd. Vervolgens zijn in de tweede plaats – 'willen' – de drijfveren van belang: in hoeverre is de organisatie gemotiveerd de AVG na te leven, met andere woorden welke prioriteit geeft de organisatie aan de naleving van de AVG in verhouding tot de uitvoering van haar kerntaken. Daarbij kijken we naar de *tone at the top.* Daarbij komen vragen aan de orde als: in hoeverre is privacy voor management en bestuur een belangrijk uitgangspunt?; op welke wijze komt dat in besluitvorming tot uitdrukking?; hoe wordt het onderwerp door de top van de organisatie besproken?; geven bestuur en directie op dat punt het goede voorbeeld? In de derde plaats zijn de mogelijkheden – 'kunnen' – die de organisatie heeft om de AVG na te leven relevant. Die mogelijkheden worden onder meer bepaald door de aanwezige capaciteit en de werkdruk, de inrichting van de privacy-organisatie en de beschikbare technische hulpmiddelen. Op deze wijze zijn 'weten, willen en kunnen' in het onderzoek gehanteerd als *zoeklichten* om vast te kunnen stellen hoe het binnen de bestudeerde overheidsorganisaties gesteld is met de kennis van de AVG en van de technische hulpmiddelen, in hoeverre sprake is van nalevingsbereidheid en of ook de randvoorwaarden aanwezig zijn om vervolgens bij voldoende kennis en wil de AVG in de praktijk na te kunnen leven.

Tafel van Elf

Om de bevindingen van de casestudy's te ordenen hebben we behalve van 'weten, willen en kunnen' als zoeklichten ook gebruik gemaakt van de door het expertisecentrum Rechtspleging en Rechtshandhaving opgestelde Tafel van Elf.[7] De Tafel van Elf bevat elf dimensies voor de naleving van wetgeving. Deze zijn ondergebracht in twee groepen: dimensies van spontane naleving en handhavingsdimensies. Voor het casestudy-onderzoek hebben we ons met name laten inspireren door de dimensies van spontane naleving, die in zekere zin beschouwd kunnen worden als een verdieping op de drieslag 'weten, willen en kunnen'. Hierna werken we die dimensies nader uit.

De dimensies van spontane naleving

— Kennis van regels

7 https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/integraal-afwegingskader-voor-beleid-en-regelgeving/instrumenten/analyse-instrumenten/tafel-van-elf

Het spreekt voor zich dat kennis van de inhoud van de normen van de AVG een noodzakelijke, maar niet voldoende, voorwaarde is voor het naleven van die normen. Behalve de vraag naar de kennis van de regels is ook van belang wat overheden doen om het kennisniveau binnen de organisatie te bevorderen.

— Kosten en baten

Het gaat bij de kosten en baten van de naleving om de (im)materiële voor- en nadelen die uit het overtreden of het naleven van de regels volgen, uitgedrukt in tijd, geld en moeite.

— Mate van acceptatie

Voor de naleving is relevant de mate waarin de normen van de AVG door overheden worden geaccepteerd. Dit hangt samen met de vraag in hoeverre de AVG als obstakel wordt gezien voor het behalen van bepaalde beleidsdoelen.

— Normgetrouwheid van de overheidsorganisatie

Hier gaat het om de bereidheid van de organisatie om zich te conformeren aan het gezag van de toezichthouder wanneer die overtredingen constateert.

— Maatschappelijke controle

Inwoners, cliënten en andere afnemers van overheidsdiensten kunnen overtredingen van de AVG door de overheidsorganisatie signaleren en daartegen actie ondernemen. Denk bijvoorbeeld aan het signaleren van een datalek. Het bewustzijn bij het publiek voor het gebruik van persoonsgegevens door de overheid speelt hier een belangrijke rol.

De zes handhavingsdimensies uit de Tafel van Elf (meldingskans, controlekans, detectiekans, selectiviteit, sanctiekans en sanctie-ernst) spelen in het casestudy-onderzoek een minder belangrijke rol. Uit veel onderzoek is bekend dat de toezichthouder op de naleving van de AVG, de Autoriteit Persoonsgegevens (AP), kampt met problemen bij de uitvoering van haar taken.[8] Daaraan zou onder meer een gebrek aan capaciteit ten grondslag liggen. Aangenomen kan worden dat de handhavingsdimensies niet in belangrijke mate bijdragen aan het handelen conform de normen omdat onder meer de controlekans, de detectiekans en de sanctiekans als laag moeten worden ingeschat. Dat betekent dat het onderzoek in de casestudy's zich niet al te zeer daarop heeft gericht.

De hierboven onderscheiden elementen die we hanteren bij het beschrijven en analyseren van de bevindingen uit de casestudy's stellen ons in staat aan de hand van een 'between-case-vergelijking' een aantal mechanismen te benoemen die binnen overheidsorganisaties aan de orde zijn bij de naleving van de AVG. Aan de hand daarvan gaan we in hoofdstuk 6 in op mechanismen die de naleving van de AVG belemmeren en op *good practices* die in de praktijk van overheidsorganisaties aan het licht zijn gekomen. Uiteraard past bij het veralgemeniseren van de bevindingen uit de casestudy's terughoudendheid, gelet op het feit dat uit het grote aantal overheidsorganisaties de AVG-praktijk binnen slechts negen organisaties nader is bekeken.

[8] Heinrich Winter, Thijs Drouen e.a., *Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en boetebevoegdheid*, Groningen/Den Haag 2022; de organisatie zelf gaat in haar meerjarenbegroting uit van een wenselijke groei van 184 naar 470 fte: https://autoriteitpersoonsgegevens.nl/nl/nieuws/groei-ap-noodzakelijk-voor-bescherming-burgers-digitaliserend-nederland, mede op basis van onderzoek uitgevoerd door KPMG in opdracht van het ministerie van JenV en de AP: *Onderzoek naar taken en financiële middelen bij AP*, 2 november 2020.

2.3 Onderzoeksmethoden

Oriënterende gesprekken en documentstudie
Het onderzoek startte met een aantal oriënterende gesprekken met de betrokken beleidsmedewerker van het ministerie van Justitie en Veiligheid (JenV), met de VNG, de Auditdienst Rijk, met een functionaris voor gegevensbescherming en met de Autoriteit Persoonsgegevens (AP). Deze gesprekken dienden om nadere informatie te verzamelen over:

- de achtergrond van het onderzoeksonderwerp;
- mogelijke valkuilen of probleempunten die we konden verwachten bij de uitvoering van het onderzoek;
- relevante documentatie en literatuur.

In deze fase van het onderzoek is tevens de relevante wet- en regelgeving geïnventariseerd en beschreven waaronder uiteraard de AVG en de UAVG.

Casestudy's
Het onderzoek is met name uitgevoerd aan de hand van casestudy's. De casestudy's voerden we uit bij een negental overheidsorganisaties: een uitvoeringsorganisatie op rijksniveau, een ministerie, drie zelfstandige bestuursorganen, drie gemeenten en een waterschap. We selecteerden een uitvoeringsorganisatie en zbo's op verschillende beleidsterreinen en met een uiteenlopende schaal. Datzelfde was het geval bij de gemeenten die we selecteerden: een 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.

Omdat de aanleiding voor het onderzoek mede is gelegen in zorg over de naleving van de AVG door overheden naar aanleiding van een aantal incidenten, hebben we bij de selectie van de organisaties ook gekozen voor een drietal organisaties die in het recente verleden kampten met problemen bij de naleving van de AVG en waarbij incidenten in de publiciteit zijn gekomen. Een overheidsorganisatie waar een AVG-incident speelde, haakte lopende het onderzoek af, maar konden we vervangen door een andere organisatie waar ook een probleem met AVG-naleving aan de orde was. Bij de verschillende organisaties speelden uiteenlopende problemen met de naleving van de AVG. Bij een van de overheidsorganisaties werden persoonsgegevens uit openbaar toegankelijke bronnen verzameld, terwijl de desbetreffende organisatie niet over een wettelijke taak beschikte in het kader waarvan dergelijke gegevens in die specifieke omstandigheid mochten worden verwerkt. In zoverre ontbrak er dus een grondslag als bedoeld in artikel 6, eerste lid, van de AVG om persoonsgegevens te mogen verwerken. Bij een van de andere overheidsorganisatie was sprake van een beveiligingsincident, waarbij persoonsgegevens mogelijk gelekt waren en systemen tijdelijk onbruikbaar waren. Bij een andere overheidsorganisatie was sprake van gegevensproducten die volgens de toezichthouder niet aan de privacywetgeving voldeden.

Juridisch bestaat er AVG-technisch geen onderscheid tussen uitvoeringsorganisaties en ministeries. De minister is verwerkingsverantwoordelijke, ook wanneer een uitvoeringsdienst gegevens verwerkt. Gaat Rijkswaterstaat of de Belastingdienst in de fout dan is de verantwoordelijk minister AVG-technisch het aanspreekpunt voor de toezichthouder. We maken toch het onderscheid tussen ministeries en uitvoeringsorganisaties omdat het wel om verschillende typen organisaties gaat die zich richten op beleid en op uitvoering. Uiteraard is het bestuur van een

zelfstandig bestuursorgaan wel verwerkingsverantwoordelijke. Daarom selecteerden we ook een drietal zbo's voor de casestudy's.

De eerste stap in een casestudy vormde deskresearch waarin op basis van de beschikbare documenten, zoals het privacybeleid, een zo goed mogelijk beeld is gevormd van de inrichting van de organisatie en de verdeling van verantwoordelijkheden. Ook is in kaart gebracht hoe in het algemeen in de organisatie de verantwoordelijkheden zijn belegd ten aanzien van het verzamelen en verwerken van persoonsgegevens en het interne toezicht daarop. Vervolgens zijn daar waar dat mogelijk was documenten bestudeerd die zijn opgesteld naar aanleiding van geconstateerde overtreding(en) van de AVG. Hierbij valt te denken aan memo's, overlegstukken of (interne) evaluatierapporten. In de verslagen van de casestudy's is verwezen naar de documenten die ter beschikking zijn gesteld en die zijn bestudeerd.

De interviews bij elke casestudy zijn afgenomen met twee doelen. Ten eerste zijn enkele interviews afgenomen met interne functionarissen. In ieder geval is in alle casestudy's gesproken met de FG. Veelal zijn daarnaast gesprekken gevoerd met een privacy officer of met de chief privacy officer (CPO). Ook met functionarissen belast met beveiliging van informatie is meestal gesproken. Vervolgens spraken we in de casestudy's met een medewerker binnen een team of afdeling, of een manager daarvan. Daarnaast waren de gesprekspartners steeds een manager, bestuurder of directeur van de organisatie. Wanneer er overtredingen van de AVG waren is ook gesproken met medewerkers die daarbij inhoudelijk waren betrokken. De gespreksverslagen van de interviews hebben we ter accordering aan de respondenten voorgelegd. Bijlage 1 bevat een overzicht van de respondenten naar functietype die we in de verschillende casestudy's hebben gesproken; in de verslagen worden de respondenten ook genoemd.

Elke casestudy is afzonderlijk geanalyseerd. Daarbij hebben we aandacht besteed aan de wijze waarop in de organisatie kennis over relevante wet- en regelgeving wordt verworven en hoe de toepassing van die kennis bij het opzetten van gegevensverzameling en -verwerking wordt geborgd. We schonken bij de analyse aandacht aan 'weten, willen en kunnen' en de relevante elementen van de Tafel van Elf (zie paragraaf 2.2). Per casestudy hebben we een rapportage opgesteld. Die casestudy-rapporten zijn opgenomen als bijlagen bij dit rapport. In hoofdstuk 5 hebben we van de casestudy's beknopte samenvattingen opgenomen. In hoofdstuk 6 volgt de vergelijking tussen de bevindingen uit de negen casestudy's en komen we tot een analyse van enkele algemene mechanismen die we in de cases aantroffen. Daarbij richten we ons op de belemmeringen in relatie tot naleving van de AVG en op opvallende *good practices*.

Aan de organisaties die aan het onderzoek meewerkten is vertrouwelijkheid toegezegd. Dat betekent dat de verslagen van de casestudy's op zodanige wijze zijn geanonimiseerd dat de organisaties onherkenbaar in beeld gebracht zijn.

De gekozen onderzoeksaanpak kent nadrukkelijk ook beperkingen. Een belangrijk nadeel van de binnen de casestudy's gemaakte keuzes voor documentenonderzoek en interviews is dat we afhankelijk waren van de bereidheid van respondenten om informatie met ons te delen. Door met verschillende gesprekspartners binnen elke organisatie te spreken menen we dat dit nadeel beperkt is. Onze indruk is ook niet dat de respondenten terughoudend waren met het delen van informatie. Een belangrijker nadeel is dat wanneer bepaalde verwerkingen van persoonsgegevens die niet overeenstemmen met de eisen van de AVG en de UAVG, niet goed in beeld zijn bij de gesprekspartners, dat in het onderzoek niet aan het licht is gekomen. Wat

de gesprekspartners niet weten, hebben ze immers ook niet kunnen vertellen. In de case-study's voerden we geen 'rechercheonderzoek' of audits uit. Daarmee kan niet met zekerheid worden gesteld dat de bevindingen uit het onderzoek volledig recht doen aan de werkelijkheid. Dat is inherent aan deze aanpak waarbij niet uitvoerig is ingegaan op concrete processen, maar waarbij op basis van een beperkt aantal gesprekken een algemeen beeld van de naleving van de AVG door een negental overheidsorganisaties is geprobeerd te geven.

Expertmeeting

Aan het eind van het onderzoek hebben we acht experts uitgenodigd om met ons over de bevindingen van het onderzoek van gedachten te wisselen. Het ging hierbij om twee academici, een medewerker van de AP, twee medewerkers van de VNG en drie FG's. We hebben de bevindingen en de voorlopige analyse voorgelegd en gevraagd in welke mate het beeld herkenbaar was, of er aanvullingen waren en of onze analyse gedeeld werd. De opbrengsten van de expertmeeting zijn in de rapportage verwerkt. Informatie over de deelnemers aan de expertmeeting (naar functietype) is opgenomen in bijlage 1.

3 Juridisch kader

3.1 Inleiding

In dit hoofdstuk wordt ingegaan op het toepasselijk wettelijk kader in relatie tot overheden. Dit onderzoek ziet op de AVG. Deze verordening ziet, gelijk als zijn voorganger de Europese richtlijn 95/46/EG en de omzetting daarvan in de Wet bescherming persoonsgegevens, op de verwerking van persoonsgegevens die gebaseerd zijn op privaatrechtelijke en bestuurlijke rechtsverhoudingen. De Nederlandse wetgever heeft in de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) daar waar de verordening ruimte laat voor nationale keuzes, of met het oog op een nadere invulling daarvan, nadere regels gesteld. De AVG en de UAVG bouwen voort op het normenkader uit de Europese Richtlijn 95/46/EG en de Wet bescherming persoonsgegevens.

Voor zover overheden zich ook bezighouden met het opsporen van strafbare feiten valt dit onder het regime van de Wet politiegegevens, waarin de Europese richtlijn 2016/680 een nationale uitwerking heeft gekregen. Wat betreft het toepassingsbereik sluiten de bepalingen uit de AVG en de Wet politiegegevens elkaar wederzijds uit: waar de bepalingen voor de verwerking van persoonsgegevens uit de AVG gelden, zien deze niet op de verwerking van persoonsgegevens met het oog op de opsporing strafbare feiten.

3.2 Rollen AVG

De verwerkingsverantwoordelijke is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[9] De verwerkingsverantwoordelijke moet voor het verwerken van persoonsgegevens een rechtmatige grondslag uit artikel 6 en, indien bijzondere persoonsgegevens verwerkt worden, uit artikel 9 in samenhang bezien met de artikelen 22 tot en met 30 UAVG hebben en is verantwoordelijk dat de persoonsgegevens op een zorgvuldige wijze worden verwerkt.

Er kan ook een gezamenlijke verwerkingsverantwoordelijkheid bestaan, bedoeld in artikel 26 AVG. Dit is het geval wanneer twee of meer verwerkingsverantwoordelijken samen de doeleinden en middelen van de verwerking bepalen. Verder volgt uit artikel 26 AVG dat wanneer er sprake is van een gezamenlijke verwerkingsverantwoordelijkheid, de rollen, verantwoordelijkheden en verhouding tot betrokkenen op transparante wijze worden vastgelegd.

[9] Artikel 4, onderdeel 7, AVG.

Er kan ook sprake zijn van een derde partij die ten behoeve van een (gezamenlijke) verwerkingsverantwoordelijke persoonsgegevens verwerkt, de zogenoemde verwerker. De taken van een verwerker richting de verwerkingsverantwoordelijke moeten in een overeenkomst worden vastgelegd.[10]

3.3 Grondslagen voor het verwerken van persoonsgegevens

De AVG bepaalt dat persoonsgegevens mogen worden verwerkt voor *bepaalde, nadrukkelijk omschreven en gerechtvaardigde* doelen.[11] Een doel is gerechtvaardigd als het kan worden gebaseerd op een van de grondslagen uit artikel 6 van de AVG.

Grondslagen uit artikel 6, eerste lid, AVG:

De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

a. de betrokkene heeft *toestemming* gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de *uitvoering van een overeenkomst* waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om *te voldoen aan een wettelijke verplichting* die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de *vitale belangen* van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. de verwerking is noodzakelijk voor de vervulling van *een taak van algemeen belang* of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de *gerechtvaardigde belangen* van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

   Onderdeel f geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.

Overheden kunnen zich in beginsel slechts baseren op twee grondslagen, namelijk indien de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust dan wel dat de verwerking noodzakelijk is voor 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.

[10] Artikel 28 AVG.
[11] Artikel 5, eerste lid, sub b, AVG.

Toestemming als grondslag verhoudt zich lastig met de voorwaarden waaraan toestemming moet voldoen. Een van de voorwaarden is dat toestemming vrij[12]dient te worden gegeven. Gelet op de verhouding van de burger tot de overheid zal daaraan niet snel kunnen worden voldaan. Ook gerechtvaardigd belang zal niet snel als grondslag kunnen dienen, omdat het op grond van de verordening aan de wetgever wordt overgelaten om de rechtsgrond voor gegevensverwerking door overheidsinstanties te creëren. Overheidsinstanties mogen in het kader van de uitvoering van hun taken het verwerken van persoonsgegevens niet baseren op de rechtsgrond gerechtvaardigd belang.[13] Overheidsinstanties kunnen daarentegen andere verwerkingen, bijvoorbeeld in het kader van de reguliere toegangsbeveiliging van overheidsgebouwen wel baseren op de grondslag gerechtvaardigd belang. Evenals de verwerking door de inkoopafdeling van namen van mensen die ingehuurd worden en de contactpersonen van partijen waar mensen van ingehuurd worden. Het dient daarbij te gaan om verwerkingsactiviteit die voortvloeien uit het privaatrechtelijk handelen van een overheidsinstantie en daarmee, niet kenbaar en voorzienbaar voor de betrokken voortvloeien uit de taak van algemeen belang die bij of krachtens wet is toegekend. Van privaatrechtelijk handelen is geen sprake wanneer het gaat om de bewaking van militaire objecten, nu dit een taak van algemeen belang betreft.[14]

Het verwerken van bijzondere persoonsgegevens, zoals onder meer persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden, tenzij voor de verwerking daarvan een uitzonderingsgrond geldt.[15] In paragraaf 3.1 van de UAVG zijn uitzonderingsgronden op het verwerkingsverbod opgenomen.

De AVG spreekt naast gewone persoonsgegevens en bijzondere persoonsgegevens ook over persoonsgegevens van strafrechtelijke aard. Het verwerken van persoonsgegevens van strafrechtelijke aard is op grond van artikel 10 AVG alleen toegestaan als dat gebeurt onder toezicht van de overheid of als het specifiek bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen bevatten voor de rechten en vrijheden van betrokkenen is geregeld. Daarnaast moet de verwerking ook gebaseerd zijn op een grondslag uit artikel 6 van de AVG.

In paragraaf 3.2 van de UAVG zijn uitzonderingen opgenomen wanneer persoonsgegevens van strafrechtelijke aard mogen worden verwerkt. Artikel 32 UAVG bevat een aantal algemene uitzonderingsgronden op het verbod van verwerking van strafrechtelijke persoonsgegevens. Zo mogen persoonsgegevens van strafrechtelijke aard onder meer verwerkt worden wanneer de betrokkene uitdrukkelijke toestemming heeft gegeven, of wanneer betrokkene de persoonsgegevens kennelijk zelf openbaar heeft gemaakt. Artikel 33 bevat specifieke uitzonderingsgronden voor het verwerken van strafrechtelijke gegevens en zijn is het meest relevant in het kader van het verwerken en delen van een zwarte lijst.

[12] Artikel 4, onderdeel 11, AVG.
[13] Artikel 6, eerste lid, AVG.
[14] Rijkswet geweldgebruik bewakers militaire objecten.
[15] Artikel 9 AVG in samenhang bezien met de artikelen 22 tot en met 30 UAVG.

Ook al is er een uitzondering op het verbod om bijzondere categorieën van persoonsgegevens te verwerken van toepassing dan wel dat het is toegestaan om persoonsgegevens van strafrechtelijke aard te verwerken, dan moet er nog steeds een grondslag voor de gegevensverwerking worden gevonden in artikel 6 van de verordening. In de praktijk kunnen de uitzonderingen samenvallen met een grondslag onder artikel 6.

Vanzelfsprekend zal ook aan alle andere vereisten van de verordening moeten worden voldaan, wil er sprake zijn van een geoorloofde gegevensverwerking.

3.4 Zorgvuldige gegevensverwerking

De verwerking van persoonsgegevens moet aan de gegevensbeschermingsbeginselen uit artikel 5 AVG voldoen. Uit artikel 5 volgt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.[16] Ook moet de verwerking gebonden zijn aan specifieke doelen[17], moet er worden voldaan aan de eis van dataminimalisatie.[18] Daarnaast moet de verwerkingsverantwoordelijke maatregelen nemen om te zorgen dat de verzamelde gegevens juist zijn[19], mogen de gegevens niet langer worden bewaard worden dan nodig[20] en moeten organisatorische en technische maatregelen getroffen worden zodat gegevens goed beveiligd en vertrouwelijk blijven.[21] De verwerkingsverantwoordelijke moet ten slotte kunnen aantonen dat gegevens zorgvuldig worden verwerkt.[22] Het gaat hier om de zogenoemde verantwoordingsplicht.

3.5 Verdere verwerking

Het beginsel van doelbinding, zoals hiervoor is aangehaald, houdt in dat persoonsgegevens alleen mogen worden verzameld voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel en dat zij vervolgens niet verder op een met dat doel onverenigbare wijze mogen worden verwerkt. Als verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, is verdere verwerking toegestaan zonder inbreuk te maken op de doelbinding. Verdere verwerking van gegevens, voor een doel dat niet verenigbaar is met het doel waarvoor de gegevens zijn verzameld dient met terughoudendheid plaats te vinden. Verdere verwerking voor een niet-verenigbaar doel is op grond van artikel 6, vierde lid, uitsluitend toegestaan, indien dit berust op toestemming van de betrokkene of op een Unierechtelijke of lidstatelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, eerste lid, van de verordening bedoelde doelstellingen van algemeen belang. Met betrekking tot de verdere verwerking voor een ander verenigbaar doel bevat artikel 6, vierde lid, een aantal criteria aan de hand waarvan de verwerkingsverantwoordelijke kan toetsen of het andere doel verenigbaar is met het oorspronkelijke doel.[23]

---

[16] Artikel 5, eerste lid, sub a AVG.
[17] Artikel 5, eerste lid, sub b AVG.
[18] Artikel 5, eerste lid, sub c AVG.
[19] Artikel 5, eerste lid, sub d AVG.
[20] Artikel 5, eerste lid, sub e AVG.
[21] Artikel 5, eerste lid, sub f AVG.
[22] Artikel 5, tweede lid, AVG.
[23] *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 37.

3.6 Transparantie en rechten van betrokkenen

Transparantie van gegevensverwerkingsactiviteiten is een van de centrale beginselen. De AVG voorziet[24] in een algemene zorgplicht voor de verwerkingsverantwoordelijke om passende maatregelen te nemen opdat betrokkene de informatie in begrijpelijke vorm, zonder onredelijke vertraging en kosteloos ontvangt.[25] De artikelen 13 en 14 AVG bevatten verplichtingen tot het verstrekken van informatie aan betrokkene wanneer gegevens van de betrokkene worden verkregen respectievelijk wanneer gegevens niet van de betrokkene zijn verkregen.

Op grond van de AVG[26] komt een betrokkene een aantal rechten toe om controle te houden over hun persoonsgegevens. Zo heeft de betrokkene het recht op inzage in persoonsgegevens die van hem worden verwerkt. Een betrokkene kan de verwerkingsverantwoordelijke verzoeken om gegevens te verbeteren, aan te vullen of (onder bepaalde voorwaarden) te verwijderen. Ook heeft een betrokkene recht om zijn persoonsgegevens te verkrijgen in een gestructureerde en machine leesbare vorm. Daarnaast komt de betrokkene het recht toe om de verwerkingsverantwoordelijke te verzoeken om persoonsgegevens van de betrokkene (tijdelijk) niet te verwerken dan wel te wijzigen. Verder heeft betrokkene het recht van bezwaar. Tot slot bestaat er het recht om als betrokkene niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profilering.

Bij het verwerken van persoonsgegevens moeten systemen, processen en de organisatie zo zijn ingericht dat aan deze rechten van betrokkene kan worden voldaan.

3.7 Verplichtingen verwerkingsverantwoordelijke

Op de verwerkingsverantwoordelijke rust, mede ter uitwerking van de eerdergenoemde verantwoordingsplicht en aantoonplicht,[27,28] de algemene verplichting om passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking wordt uitgevoerd in overeenstemming met de AVG. De verwerkingsverantwoordelijke moet daarbij rekening houden met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen. De getroffen maatregelen moeten worden geëvalueerd en, indien nodig, geactualiseerd. Bij omvangrijke en risicovolle verwerkingen omvatten de hiervoor genoemde maatregelen tevens een gegevensbeschermingsbeleid. Nu overheden te maken hebben met omvangrijke en risicovolle verwerkingen geldt voor overheden dat zij een dergelijk gegevensbeschermingsbeleid dienen op te stellen.

Bij de uitwerking van de algemene verplichting om technische en organisatorische maatregelen te treffen worden twee beginselen in acht genomen die tot doel hebben om de

[24] Artikel 12, eerste lid, AVG.
[25] Artikel 12, derde tot en met vijfde lid 3, AVG.
[26] De artikelen 12 tot en met 23 AVG.
[27] Artikel 5, tweede lid, AVG.
[28] H.R. Kranenborg en L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming In Europees en Nederlands perspectief* (Mastermonografieën staats- en bestuursrecht), Wolters Kluwer: Deventer 2018 p. 226.

bescherming van persoonsgegevens in de verwerkingsactiviteiten en de technologische middelen waarmee gegevens worden verwerkt, in te bouwen. Het gaat om het beginsel van gegevensbescherming door ontwerp (*privacy by design*)[29] en het beginsel van gegevensbescherming door standaardinstellingen (*privacy by default*)[30]. Het beginsel van *privacy by design* houdt in dat de verwerkingsverantwoordelijke bij de bepaling van de verwerkingsmiddelen als ook bij de verwerking zelf passende technische en organisatorische maatregelen moet treffen. Deze maatregelen zijn erop gericht om de algemene beginselen van artikel 5 AVG op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de AVG en ter bescherming van de rechten van de betrokkenen. Het beginsel van *privacy by default* houdt in dat de standaardinstellingen bij de ontwikkeling van nieuwe systemen zodanig zijn gekozen dat de bescherming van persoonsgegevens wordt verzekerd.

De beveiligingsverplichtingen zijn algemeen[31] geformuleerd en refereren aan het 'passende' beschermingsniveau dat moet worden geboden. Het begrip 'passend' in artikel 32, eerste lid, impliceert een proportionaliteitstoets: er moet evenredigheid bestaan tussen de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen enerzijds en de getroffen beveiligingsmaatregelen anderzijds.

Om de veiligheid van de gegevensverwerking te waarborgen en te voorkomen dat een verwerking inbreuk maakt op de AVG, moet de verwerkingsverantwoordelijke de aan de verwerking inherente risico's beoordelen en op grond van een objectieve en zo concreet mogelijke risicobeoordeling passende technische en organisatorische maatregelen nemen om een beveiligingsniveau te waarborgen dat op het risico is afgestemd. Uit considerans 83 AVG volgt dat de verwerkingsverantwoordelijke daarbij verschillende factoren betrekt, zoals de stand van de techniek, de uitvoeringskosten, de aard van de verwerking, de omvang van de verwerking, de context van de verwerking, de verwerkingsdoeleinden, de ernst van de vastgestelde risico's, en de waarschijnlijkheid dat de vastgestelde risico's zich zullen verwezenlijken. De beveiligingsmaatregelen, waar passend, moeten het volgende omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens;
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Voor de overheid gelden de NEN-ISO 27001/27002 en daaraan gerelateerde overheidsnormen -zoals de Baseline Informatieveiligheid Overheid (BIO) - momenteel als de standaard baselines om te komen tot een 'adequate' beveiliging.

Verder kent de AVG – evenals de Wbp – een meldplicht om de Autoriteit Persoonsgegevens (AP) in kennis te stellen van een inbreuk in verband met persoonsgegevens. Deze meldplicht wordt ook wel de meldplicht datalekken genoemd. De verwerkingsverantwoordelijke moet, zodra hij weet dat een inbreuk in verband met persoonsgegevens heeft plaatsgevonden,

[29] Artikel 25, eerste lid, AVG.
[30] Artikel 25, tweede lid, AVG.
[31] Artikel 32, eerste lid, AVG.

zonder onredelijke vertraging en uiterlijk binnen 72 uur de toezichthouder in kennis stellen van de inbreuk.[32] Als de inbreuk waarschijnlijk een hoog risico met zich meebrengt dan moet de verwerkingsverantwoordelijke de betrokkene onverwijld van de inbreuk op de hoogte brengen.[33] De verwerkingsverantwoordelijke kan door de AP tot melding aan de betrokkene worden verplicht.[34] Een melding aan de betrokkene kan achterwege blijven in de volgende drie gevallen[35]:

- de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en toegepast, bijvoorbeeld in de vorm van versleuteling van de betrokken gegevens;
- de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het vastgestelde hoge risico voor de betrokkenen zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou de verwerkingsverantwoordelijke onevenredige inspanningen vergen.

De verwerkingsverantwoordelijke is gehouden alle inbreuken, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de genomen corrigerende maatregelen ter invulling van de verantwoordingsplicht te documenteren. Dit stelt de toezichthouder in staat de naleving van de meldingsplicht te controleren.[36]

3.8 Instrumentarium

Register van verwerkingsactiviteiten
Overheden dienen als verwerkingsverantwoordelijke een register van de verwerkingsactiviteiten bij te houden.[37] Dit register moet de verwerkingsverantwoordelijke op verzoek aan de toezichthouder kunnen laten zien.[38] Het register bevat een beschrijving van de verwerkingsactiviteiten.

Gegevensbeschermingeffectbeoordeling en de voorafgaande raadpleging
Als de verwerkingsverantwoordelijke een verwerking beoogt die een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen moet hij voorafgaand aan de verwerking een gegevensbeschermingseffectbeoordeling uitvoeren.[39] De bedoeling van een dergelijke beoordeling is om bij voorgenomen verwerkingsactiviteiten de effecten daarvan voor de betrokkene te inventariseren en te beoordelen. Op basis van die beoordeling kunnen maatregelen worden genomen om die effecten te voorkomen of te reduceren. Van een hoog risico is sprake, wanneer[40]:

- een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon

[32] Artikel 33, eerste lid, AVG.
[33] Artikel 24, eerste lid, AVG.
[34] Artikel 34, vierde lid, AVG.
[35] Artikel 34, derde lid, AVG.
[36] Artikel 33, vijfde lid. AVG.
[37] Artikel 10, eerste lid, AVG.
[38] Artikel 30, vierde lid, AVG.
[39] Artikel 35, eerste lid, AVG.
[40] Artikel 35, derde lid, AVG.

rechtsgevolgen zijn verbonden of die de persoon op vergelijkbare wijze wezenlijk treffen;
- een grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten;
- een stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De AP dient een lijst op te stellen van het soort verwerkingen waarvoor een DPIA verplicht is.[41] Daarnaast kan de AP op grond van artikel 35, vijfde lid, een lijst opstellen van het soort verwerkingen waarvoor dit niet vereist is.[42]

Als uit een gegevensbeschermingseffectbeoordeling blijkt dat het overgebleven risico, ondanks de genomen maatregelen die met het oog op de beschikbare technologie en de uitvoeringskosten redelijk zijn[43], nog steeds hoog is, moet de AP worden geraadpleegd. [44] Bij een voorafgaande raadpleging adviseert de AP de verwerkingsverantwoordelijke over hoe de risico's van de voorgenomen verwerking kunnen worden beperkt. Deze maatregelen moeten worden uitgevoerd, voordat de verwerkingsverantwoordelijke met de verwerking begint. De AP kan de verwerkingsverantwoordelijke ook adviseren om in het geheel van de verwerking af te zien.

Functionaris gegevensbescherming
Overheidsinstanties of overheidsorganen zijn verplicht om een FG aan te stellen.[45] Deze verplichting geldt voor alle organen van het Rijk, provincies, gemeenten, waterschappen, andere openbare lichamen en zelfstandige bestuursorganen. Een overheidsinstantie of overheidsorgaan kan één FG aanwijzen voor verschillende overheidsinstanties of organen, met inachtneming van hun organisatiestructuur en omvang.[46] De FG wordt aangewezen op grond van zijn professionele kwaliteiten.[47] Daarbij gaat het in het bijzonder om zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en in het bijzonder om zijn capaciteiten om de in artikel 39 AVG genoemde taken te verrichten. De FG hoeft geen personeelslid van de verwerkingsverantwoordelijke te zijn.

De FG moet naar behoren en tijdig worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.[48] Deze functionaris krijgt daarbij de nodige ondersteuning en middelen[49] voor de uitvoering van zijn taken en blijft gevrijwaard van instructies met betrekking tot zijn taken. De FG heeft daarvoor binnen de organisatie toegang tot persoonsgegevens en verwerkingsactiviteiten zodat hij zelf kan onderzoeken of in overeenstemming met de AVG wordt gehandeld.

De FG heeft een onafhankelijke positie. Hij mag geen instructies ontvangen met betrekking tot de uitvoering van zijn taken. Dit houdt onder meer in dat de verwerkingsverantwoordelijke het resultaat van een door de FG ingesteld onderzoek niet mag beïnvloeden en ook niet mag bepalen hoe een bij de FG ingediende klacht wordt afgehandeld. Ook heeft hij

[41] Artikel 35, vierde lid, AVG.
[42] Artikel 35, vijfde lid, AVG.
[43] Considerans 84 en 94 AVG.
[44] Artikel 36, eerste lid, AVG.
[45] Artikel 37, eerste lid, onderdeel a, AVG.
[46] Artikel 37, derde lid, AVG.
[47] Artikel 37, vijfde lid, AVG.
[48] Artikel 38, eerste lid, AVG.
[49] Artikel 38, tweede lid, AVG.

ontslagbescherming; voor de uitvoering van zijn taken kan hij niet worden ontslagen of gestraft. De FG brengt rechtstreeks verslag uit aan de hoogste leidinggevende. [50] Als de FG ook andere taken verricht moet de verantwoordelijke of verwerker ervoor zorgen dat dit niet tot belangenconflicten leidt.[51] Hier gaat de functie van privacy officer niet samen met die van FG. Betrokkenen kunnen contact opnemen met de FG over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten op grond van de AVG.[52] De FG heeft een verplichting tot geheimhouding of vertrouwelijkheid. Dit ook in relatie tot hetgeen vanwege een klacht of een verzoek van een betrokkene bij hem bekend is geworden.[53]

De FG heeft tot taak om de verwerkingsverantwoordelijke en de betrokken werknemers te informeren en te adviseren over hun verplichtingen onder de AVG en andere EU-rechtelijke of nationaalrechtelijke gegevensbeschermingsbepalingen, ook ziet hij toe op de naleving van de AVG en verstrekt hij op verzoek advies met betrekking tot de gegevensbeschermingseffectbeoordeling, hij werkt samen met de toezichthouder en treedt op als contactpunt, met name in geval van voorgaande raadpleging in de zin van artikel 36 AVG.[54] Hij houdt bij de uitvoering van zijn taken rekening met de aan de verwerking verbonden risico's, en met de aard, de omvang, de context en de doeleinde van de verwerking.[55]

[50] Artikel 38, derde lid, AVG.
[51] Artikel 38, zesde lid, AVG.
[52] Artikel 38, vierde lid, AVG.
[53] Artikel 38, vijfde lid, AVG en artikel 39 UAVG.
[54] Artikel 39, eerste lid, AVG.
[55] Artikel 39, tweede lid, AVG.

4 Bestaand beeld

In dit hoofdstuk presenteren we de bevindingen over het bestaande beeld van de naleving van de AVG door overheden. Als basis voor dit hoofdstuk zijn de bevindingen uit de gesprekken met de Vereniging Nederlandse Gemeenten (VNG), de Auditdienst Rijk (ADR), de Autoriteit Persoonsgegevens (AP) en een onafhankelijk expert die zich laat inhuren als extern FG samengevat.

In de opzet van het onderzoek is het bestaande beeld en ook de lacunes daarin als uitgangspunt genomen voor de aanpak in de casestudy's. De gedachte hierbij is dat de bevindingen uit de casestudy's gebruikt zouden kunnen worden om het bestaande beeld aan en in te vullen, om zo niet alleen verdiepende maar ook complementaire resultaten te kunnen gebruiken voor de uiteindelijke analyse.

In paragraaf 4.1 beschrijven we eerst de betrokken instanties die we hebben gesproken om duidelijk te krijgen hoe het beeld van de naleving van de AVG er voor dit onderzoek er uitzag. Vervolgens beschrijven we in paragraaf 4.2 enkele bevindingen uit andere onderzoeken en rapportages die van belang zijn met betrekking tot naleving door overheden in brede zin. In paragraaf 4.3 beschrijven we specifiek voor enerzijds gemeenten en anderzijds departementen, uitvoeringsorganisaties en zelfstandige bestuursorganen het beeld dat gevormd is voorafgaand aan het casestudy-onderzoek. We sluiten het hoofdstuk af met een eerste analyse van oorzaken van niet-naleving van de AVG en enkele observaties over het huidige beeld met betrekking tot het verdere onderzoek.

4.1 Betrokken instanties en hun beeld van de naleving

Voorafgaand aan het onderzoek was de verwachting dat de AP het beste beeld zou hebben van de stand van de naleving van de AVG. Deze organisatie heeft immers de wettelijke taak om toezicht te houden op de naleving van de AVG. Ook overheidsinstanties zijn verplicht om datalekken bij de AP te melden. Op die manier kan de AP direct reageren en eventueel maatregelen nemen.

Uit ons gesprek met de AP is gebleken dat het beeld van de AP van de naleving verre van compleet is. Ten aanzien van datalekken is de toezichthouder nog optimistisch over de mate waarin de signalen die de AP bereiken het totaal aantal datalekken benaderen. Hierbij vertrouwt men op de integriteit van (de FG's bij) de overheden die onder toezicht staan, te meer omdat de verwachting is dat – door de grote publieke aandacht voor het functioneren van de overheid – het moeilijk is om datalekken achter te houden voor de toezichthouder.

Dat geldt echter vermoedelijk voornamelijk voor de grotere datalekken. Het is goed voorstelbaar dat kleinere datalekken (bijvoorbeeld het opsturen van een rijbewijs naar een verouderd adres) niet zo snel de publiciteit halen en ook minder snel gemeld zouden worden. Het ondersteunend effect van media-aandacht voor de naleving van de AVG beperkt zich dus tot die overtredingen die ook nieuwswaardig zijn. Dit effect is bovendien niet van toepassing op overtredingen die alleen binnen de organisaties bekend blijven, bijvoorbeeld als het gaat om gegevensdeling tussen afdelingen of met samenwerkingspartners.

Naast het reactief toezicht op basis van signalen past de AP ook proactief toezicht toe. Voor het systeemgericht toezicht[56] zijn in totaal twintig medewerkers beschikbaar, waarvan er twee zijn toegewezen aan de sector overheid. De beschikbare capaciteit voor systeemgericht toezicht is dus zeer beperkt. Om die reden is er voor gekozen om bepaalde aandachtsgebieden te hanteren. Voor de overheid gaat het dan om de thema's 'digitale overheid' en 'beveiliging'.

Jaarlijks levert de AP per sector (dus ook voor overheid) een zogeheten 'sectorbeeld' op. Dit document is echter voor interne informatievoorziening bedoeld en is niet openbaar, noch voor onderzoekers onder voorwaarden inzichtelijk. In de rapportages die door de AP naar buiten worden gebracht, wordt niet specifiek ingegaan op naleving van de AVG door overheden, maar worden totaalbeelden gepresenteerd.

Op rijksniveau is de Auditdienst Rijk (ADR) actief op het gebied van advisering over onder meer 'informatiebeveiliging en privacybescherming'. Ook de ADR heeft daarmee een beeld van de naleving van AVG door overheidsinstanties die onder de rijksoverheid vallen. Dat beeld is gebaseerd op de indrukken die de ADR opdoet tijdens de diverse audits die de organisatie uitvoert. In aanvulling daarop is de VNG actief op het gebied van advisering van gemeenten op het gebied van AVG-compliance en de inrichting en inbedding van de privacy-organisatie. De informatiebeveiligingsdienst (IBD) van de VNG organiseert hiertoe onder meer intervisiesessies en inhoudelijke sessies over deze thema's. Door kennisdeling te stimuleren ondersteunt de VNG gemeenten bij het inrichten van processen en organisaties conform de AVG. Aan de hand van de vragen en signalen die tijdens deze sessies of ad hoc binnenkomen en aan de hand van de inbreng van de gemeenten heeft de VNG een beeld gevormd van de naleving van de AVG bij die gemeenten. De informatie die ADR en VNG hebben gedeeld over de naleving van de AVG door overheden komt hierna aan de orde in de paragrafen 4.3.1 en 4.3.2.

We moeten constateren dat het huidige beeld van de naleving van de AVG door overheden beperkt is. Om deze reden is het, met name op het gebied van decentrale overheden en zelfstandige bestuursorganen, zaak om een slag om de arm te houden met betrekking tot de compleetheid van het beeld. Bij de AP en bij VNG zijn de beelden grotendeels ontstaan uit signalen die hen bereiken. Daar kan een selectie-effect in optreden, bijvoorbeeld omdat juist gemeenten die een hoog volwassenheidsniveau hebben bereikt op het gebied van AVG-compliance meer vragen stellen en zich meer mengen in het debat binnen de VNG. Ook is het mogelijk dat de AP voornamelijk signalen ontvangt van overheden die gevorderd zijn in de naleving van de AVG. Het risico bestaat daardoor dat juist signalen van overheden die de AVG minder goed naleven beperkt doorklinken in het huidige beeld van de naleving.

[56] Systeemgericht toezicht (of systeemtoezicht) is het toezicht door de overheid dat gebruikmaakt van zelfregulerende (kwaliteits)systemen binnen organisaties of branches.

Tijdens het gesprek met de AP is ook gevraagd waar het zwaartepunt van verwerking van persoonsgegevens bij overheden wat hen betreft ligt. De gesprekspartners hebben aangegeven dat naast de uitvoeringsorganisaties van het rijk vooral gemeenten veel activiteiten ondernemen waarbij sprake is van (brede) gegevensverwerking. Op basis van deze observatie is ervoor gekozen om niet drie, maar vier decentrale overheden (waarvan drie gemeenten) te selecteren voor een casestudy.

4.2 Bevindingen uit ander onderzoek

Het onderzoeksprogramma Argos deed in 2020 onderzoek naar de uitvoering van de AVG.[57] Dat onderzoek signaleert met name problemen rond de FG's. Zij zouden niet worden betrokken in de besluitvorming, hebben vaak een uitvoerende functie naast hun controlerende functie en ondervinden weinig steun van de AP. Een deel (20%) van de FG's geeft aan actief te worden tegengewerkt door de eigen organisatie.

De positie van de FG is ook een onderwerp dat speelt bij de rijksoverheid. Meestal ziet dit niet op het hebben van voldoende kennis of een dubbeling van functies, maar wel op de omvang van het werkterrein. Ministeries gaan uit van één FG zowel voor het beleidsdepartement als voor de aangesloten uitvoeringsorganisaties. Bij onder meer het ministerie van Financiën, het ministerie van I&W en het ministerie van J&V betekent dit dat de FG op een zeer groot uitvoeringsapparaat toezicht houdt. Daarbij is het dan van belang welke structuren er gekozen zijn om een dekkende privacy-organisatie in te richten.

In september 2022 heeft het Centrum voor Informatiebeveiliging en Privacybescherming (CIP), een netwerkorganisatie van overheidsinstellingen en marktpartijen, een onderzoek gepubliceerd over de invulling van de functie van de FG in de praktijk binnen de publieke sector.[58] Hiervoor is een enquête afgenomen bij 199 FG's bij overheden. FG's geven aan dat de volwassenheid van de functie van FG in de afgelopen vier jaar sterk is verbeterd. De functie is structureler ingebed in organisaties en de focus is verschoven van advisering naar toezichthoudende activiteiten. Ook bij DPIA's zien de FG's dat hun rol meer een toezichthoudende in plaats van een adviserende is geworden. Het toezicht wordt steeds meer planmatig ingericht. De bevraagde FG's hebben ook de volwassenheid van de eigen privacy-organisatie beoordeeld. De FG's zijn kritisch op de staat van het verwerkingsregister en over de steun van het management. De tendens lijkt te zijn dat FG's vinden dat ze werknemers steeds minder goed kunnen overtuigen van het belang van privacy en naleving van de AVG. In de gesprekken met FG's tijdens de casestudy's zijn we ook verder op hun positie, de borging van hun onafhankelijkheid en hun zicht op naleving van de AVG ingegaan.

4.3 Het bestaande beeld van de naleving

[57] L. Ruizendaal, M. Poncin & D. Hielkema, 'Kwart van gemeenten neemt privacy niet serieus', *Argos* 2020, te raadplegen via vpro.nl/argos.
[58] W. van Wijk, A. Reuijl en S. Aliar, *FG-Enquête 2022. Een tweede onderzoek naar de invulling van de functie van Functionaris Gegevensbescherming in de praktijk binnen de publieke sector*, Centrum voor Informatiebeveiliging en Privacy: 2022.

Voordat we het bestaande beeld specifiek bij gemeenten en departementen en rijksoverheidsorganen behandelen, presenteren we in deze paragraaf enkele cijfers uit jaarrapportages van de AP, die een algemeen beeld schetsen van ontwikkelingen in de afgelopen jaren.

De AP publiceert jaarlijks cijfers over datalekken. Hieruit blijkt dat in het aantal meldingen dat door rijksoverheden, zelfstandige bestuursorganen en gemeenten geen grote verschillen zitten. In 2018 deden overheden – met uitzondering van politie en justitie – 3550 keer melding van een datalek. Rijksoverheden meldden in 2018 994 datalekken (28%), zelfstandige bestuursorganen ongeveer 1100 keer (31%) en gemeenten 1385 keer (39%). De overige meldingen werden onder andere door provincies en waterschappen gedaan.[59] In 2019 ontving de AP 4624 meldingen van overheden: een stijging van 27%.[60] Rijksoverheden meldden in 2019 1156 datalekken (25%), zelfstandige bestuursorganen 1757 (38%) en gemeenten 1526 (33%).[61] In 2020 werden 5275 meldingen gedaan door overheden (weer met uitzondering van politie en justitie).[62] In 2021 werden 5719 datalekken gemeld.[63] De AP geeft in haar jaarrapportages meermaals aan dat niet alle datalekken worden gemeld.[64]

4.3.1 Gemeenten

Anekdotische bevindingen

Op gemeentelijk niveau bestaan problemen rond de inzet van smart city-toepassingen, waaronder wifitracking, en online monitoring. Zogenaamde smart city-toepassingen zijn een aandachtsgebied van de AP. In juli 2021 verscheen dan ook een onderzoeksrapport van de AP.[65] Hierin definieert de AP smart city-toepassingen als 'het verzamelen en verwerken van (persoons)gegevens over of in de openbare ruimte door de inzet van sensoren, technologie of andere toepassingen om inzicht in, of analysemogelijkheden over de openbare ruimte te verkrijgen, of sturing van de openbare ruimte mogelijk te maken.'[66] Enschede kreeg in 2021 een boete wegens wifi-tracking. Daarnaast hebben Dongen en Tilburg hun wifi-netwerk uit de lucht gehaald omdat het niet voldeed aan de AVG. In het onderzoek naar smart city-toepassingen komt de AP daarnaast tot de conclusie dat FG's niet altijd de positie, middelen en zeggenschap krijgen om toereikend toezicht te houden op bijvoorbeeld smart city-toepassingen.[67]

Uit recent onderzoek blijkt dat bijna alle gemeenten openbare bronnen, zoals social media als Facebook en Twitter, op internet monitoren.[68] Een klein deel (14%) slaat hierbij ten minste maandelijks online berichten op. Een groter deel (44%) slaat jaarlijks online berichten op.[69] Hierbij worden doorgaans ook persoonsgegevens zoals IP-adressen of nicknames opgeslagen

[59] AP, *Jaarrapportage datalekken 2018*, 2019, p. 1, 7 en 8.
[60] AP, *Jaarrapportage datalekken 2019*, 2020, p. 12.
[61] AP, *Jaarrapportage datalekken 2019*, 2020, p. 12.
[62] AP, *Jaarrapportage datalekken* 2020, p. 1 en 3. In de jaarrapportage van 2020 is, in tegenstelling tot de jaarrapportages van 2018 en 2019, geen onderscheid gemaakt naar type overheidsorganisatie.
[63] AP, *Jaarcijfers Datalekken 2021*, 2022, p. 1 en 9.
[64] AP, *Jaarrapportage datalekken 2020*, 2021, p. 5 en AP, *Jaarrapportage datalekken 2021*, 2022, p. 3.
[65] AP, *Smart Cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*, 2021.
[66] AP, *Smart Cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*, 2021, p. 7.
[67] AP, *Smart Cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*, 2021, p. 31.
[68] W. Bantema, S. Westers, M. Hoekstra, R. Herregodts & S. Munneke, 'Black Box van gemeentelijke monitoring', *Politiekunde* 2021, 109, p. 44.
[69] W. Bantema, S. Westers, M. Hoekstra, R. Herregodts & S. Munneke, 'Black Box van gemeentelijke monitoring', *Politiekunde* 2021, 109, p. 78-79.

en dus verwerkt. De conclusie van dit onderzoek is dat in het merendeel van de gevallen de eisen van de AVG en het Europees Verdrag voor de Rechten van de Mens (EVRM) worden nageleefd, maar dat risico's bestaan op privacyschendingen doordat niet is vastgelegd in welke gevallen en onder welke voorwaarden mag worden gemonitord. Bovendien ontbreekt vaak het toezicht van een FG.[70]

Begin 2018 constateerde de AP dat twee gemeenten meer persoonsgegevens dan noodzakelijk verzamelen bij de beoordeling van de zorg die mensen nodig hebben. Zowel uit die onderzoeken als uit latere jaarverslagen, onderzoeken en besluiten van de AP of nieuwsbronnen blijkt niet dat dit specifieke probleem zich bij meerdere gemeenten voordoet.

Algemeen beeld van de naleving van de AVG door gemeenten
De inschatting van de AP is dat met name gemeenten veelvuldig, en breed, persoonsgegevens verzamelen en dat bij gemeenten niet altijd een duidelijk beeld bestaat van de relevante wet- en regelgeving en hoe die toegepast moet worden bij hun processen. Specifiek wordt ook gewezen op het feit dat niet alleen de AVG, maar ook de Wpg en andere wetgeving van toepassing kan zijn. Met betrekking tot de AVG bestaat soms nog steeds discussie over de verschillende rollen van verwerker en verwerkingsverantwoordelijke, en door die onduidelijkheid is de naleving van de AVG soms problematisch.

Wat hierbij complicerend werkt is de ontwikkeling dat bij decentrale overheden veelvuldig de (keten)samenwerking wordt opgezocht en dat in het kader van die samenwerking dan ook gegevensuitwisseling als voorwaarde wordt gezien voor een doeltreffende uitvoering. In de samenwerkingsverbanden is het goed denkbaar dat de rollen binnen het kader van de AVG niet goed onderscheiden of gedefinieerd worden. Er wordt nog vaak gedacht in termen van 'het mag' in plaats van 'het is noodzakelijk'. Bovendien is het door het grote aantal samenwerkingsverbanden waarin gemeenten deelnemen voor de gemeentelijke organisaties zelf moeilijk overzicht te houden. Hierdoor zijn bijvoorbeeld gegevensverwerkingsregisters over het algemeen niet volledig en niet correct bijgehouden.

Ook de DPIA's zijn, naar de indruk van de AP, bij de meeste gemeenten niet volledig op orde. De DPIA's worden wel uitgevoerd, maar vaak is het niet geborgd dat deze up-to-date worden gehouden als de wijze van verwerking verandert. Bij de inwerkingtreding van de AVG zijn projectorganisaties opgezet die tijdelijk veel werk hebben verzet op het gebied van AVG-compliance, maar het omvormen van deze processen naar de dagelijkse uitvoeringspraktijk en bijvoorbeeld het opzetten van een structurele Plan Do Check Act-cyclus (PDCA-cyclus) gebeurt slechts zelden. Dat geldt overigens ook voor departementen en andere overheden. Het algehele volwassenheidsniveau wordt door de AP voorzichtig nog steeds ingeschat als 'in ontwikkeling'.

Bij decentrale overheden kijkt de AP niet actief naar zaken als de inrichting van de privacyorganisatie, de scheiding van rollen en het budget voor FG's. Wel krijgt de AP geregeld signalen van FG's die bijvoorbeeld aangeven niet voldoende toegang te hebben tot besluitvorming, of die niet voldoende tijd of budget krijgen voor uitvoering van de taken. Dat gaat dan niet (alleen) om de capaciteit van de FG-functie, maar in belangrijke mate om bewustzijn in de

[70] W. Bantema, S. Westers, M. Hoekstra, R. Herregodts & S. Munneke, 'Black Box van gemeentelijke monitoring', *Politiekunde* 2021, 109, p. 115.

organisatie: Het is vooral van belang dat interne signalen over overtredingen van de AVG serieus worden genomen en dat een open houding wordt nagestreefd ten aanzien van interne kritiek.

De indruk van de AP is dat bij gemeenten vaak nog sprake is van geloof in data voor het bieden van allerhande oplossingen en daarbij kan een 'dominantie van de doelstelling' optreden. Zeker bij ketensamenwerking of andere processen waar aanpalende wetgeving relevant is, is het verleidelijk om privacy als belemmerende factor te zien, in plaats van te kijken naar de mogelijkheden en voorwaarden waarbinnen processen wel plaats kunnen vinden. De *tone at the top* is in deze gevallen doorslaggevend, en helaas niet altijd in positieve zin. Daarbij wordt regelmatig onvoldoende acht geslagen op het feit dat de burger ten opzichte van de gemeente een veel sterkere afhankelijkheid heeft dan ten opzichte van bijvoorbeeld bedrijven (waar men relatief eenvoudig kan besluiten geen klant te worden of blijven).

Door de Informatiebeveiligingsdienst (IBD)[71] is ook vastgesteld dat de positie van de FG een groot probleem is bij gemeenten. Regelmatig kan de FG de onafhankelijke en toezichthoudende rol niet goed vervullen vanwege de inbedding van de functionaris in de organisatie. Ook de adviserende rol komt soms onvoldoende uit de verf, wanneer de FG doorschuift naar een rol waarin verantwoordelijkheid wordt genomen voor de privacybescherming in de uitvoering, bijvoorbeeld bij het uitvoeren van DPIA's.

Bij kleine gemeenten speelt dit fenomeen van rolvermenging van de FG met die van adviseurs sterker dan bij grotere. De VNG maakt zich zorgen over externe FG's, die voor een beperkt aantal uren aanwezig zijn binnen de organisatie. Dergelijke FG's zijn in de praktijk veel minder goed in staat om op de hoogte te blijven van wat er in de organisatie gebeurt, kunnen minder goed voeling krijgen met de organisatie en staan te veel op afstand om tijdig input te leveren bij het ontwerpen van processen en projecten.

Gemeenten staan volgens de AP ook meer dan andere overheden onder druk door het sterk uitgebreide takenpakket en problemen in bijvoorbeeld de jeugdzorg. Gegevensbescherming en het opbouwen van een solide privacy-organisatie heeft in die omstandigheden minder prioriteit gekregen dan gehoopt. Daarbij speelt ook nog een rol dat veel gemeenten een kwalitatief personeelstekort kennen en niet voldoende goede mensen kunnen krijgen, ook voor wat betreft expertise en kunde op het gebied van gegevensbescherming. De AP ziet overigens geen verband tussen de grootte van de gemeente en de mate waarin de AVG-compliance op orde is. Er zijn kleine gemeenten die het heel goed doen, en grote gemeenten die het minder goed voor elkaar hebben. Bij grote gemeenten speelt dan volgens de VNG soms mee dat medewerkers in de lijn de deskundige mensen op het gebied van AVG intern niet weten te vinden, waardoor de aanwezige kennis niet goed wordt ingezet.

Het algehele beeld vanuit zowel de AP als de VNG ten aanzien van de ontwikkelingen over langere tijd is positief. Beide instanties hebben de indruk dat gemeenten stappen blijven zetten, dat gemeenten zich steeds meer bewust worden van het belang van gegevensbescherming en hoe dat geborgd moet worden. Ook op het gebied van kennisdeling worden gemeenten, ondersteund door de VNG, steeds actiever. Er wordt bijvoorbeeld gebruik gemaakt van

[71] De informatiebeveiligingsdienst is onderdeel van de VNG en ondersteunt gemeenten bij preventie, detectie, coördinatie en kennisdeling op het gebied van informatiebeveiliging. Ook biedt IBD ondersteuning bij de bescherming van persoonsgegevens.

standaard verwerkersovereenkomsten, en ook op andere gebieden wordt getracht te voorkomen dat gemeenten het wiel onnodig opnieuw uitvinden. Zo is er onder meer een IRPA-tool beschikbaar (integrale risico- en privacy-analyse) die steeds meer wordt gebruikt, en is er de ENSIA-tool (Eenduidige Normatiek Single Information Audit) waarmee de gemeenteraad beter in positie wordt gebracht om de gemeente te controleren op het gebied van onder meer naleving van de AVG. Ook de AP zegt aandacht te hebben voor de rol van de raad in het afdwingen van AVG-conform gedrag.

4.3.2 Departementen en uitvoeringsorganisaties

Anekdotische bevindingen

Van een tweetal ministeries zijn overtredingen van de AVG bekend. In november 2020 bleek dat het *Land Information Manoeuvre Centre* (LIMC), een onderdeel van de Koninklijke Landmacht, gegevens uit openbare bronnen, waaronder nieuwswebsites en sociale mediaplatforms, heeft verzameld, geanalyseerd en verwerkt in rapportages. Het doel hiervan was het in kaart brengen van aan COVID-19 gerelateerde maatschappelijk ontwikkelingen, zoals de verspreiding van desinformatie, ten behoeve van militaire en civiele besluitvorming. In dit verband werden persoonsgegevens verwerkt zonder wettelijke grondslag. De FG van Defensie deed onderzoek naar deze overtreding, waarbij een van de conclusies was dat het LIMC niet de intentie had om persoonsgegevens te verwerken. De aanbevelingen van de FG richtten zich met name op het verbeteren van het risicobewustzijn en de interne controle. Zo werd aanbevolen om een DPIA op te stellen voor Informatiegestuurd optreden, risicovolle verwerkingen te inventariseren en de AVG-organisatie te professionaliseren door AVG-coördinatoren onder te brengen bij verschillende eenheden en een Chief Privacy Officer (CPO) aan te stellen en te positioneren bij de bestuursstaf en de directie bedrijfsvoering en organisatie.[72]

De Nationaal Coördinator Terrorisme en Veiligheid (NCTV), die onder het ministerie van Justitie en Veiligheid valt, beging mogelijk eenzelfde overtreding. Bij het maken van fenomeenanalyses zoals het 'Dreigingsbeeld Terrorisme' verwerkte de NCTV persoonsgegevens om de dreiging te duiden. Deze verwerking bestond meer specifiek uit online monitoring: het in de gaten houden van personen op internet, bijvoorbeeld op social media. De NCTV paste sinds 2006 online monitoring toe. Daarbij meende de NCTV aanvankelijk dat de algemene taakstelling van de NCTV voldoende grondslag bood voor de verwerking van persoonsgegevens. Naar aanleiding van een onderzoek van het NRC begin 2021 is de NCTV echter tot het inzicht gekomen dat de verwerking van persoonsgegevens een stevigere wettelijke basis nodig heeft.[73] De voorgestelde Wet verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid zou hierin voorzien, maar de behandeling van dit wetsvoorstel ligt stil na kritiek van de AP.[74]

Ook van een aantal uitvoeringsorganisaties zijn overtredingen van de AVG bekend. De AP heeft twee boetes en een verwerkingsverbod opgelegd aan de Belastingdienst.[75] De boetes hadden respectievelijk betrekking op de onrechtmatige verwerking van de dubbele nationaliteit van aanvragers van kinderopvangtoeslag en het verwerken van persoonsgegevens in de applicatie

[72] FG Defensie, *Onderzoek naleving Algemene verordening gegevensbescherming. Experimenteeromgeving Land Information Manoeuvre Centre (LIMC)*, 2021, p. 60-61.
[73] *Kamerstukken II* 2020-2021, 32761/30821, nr. 180, p. 3.
[74] Zie AP, *Advies over het concept voor een wetsvoorstel Wet verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid*, 2021.
[75] Zie voor deze besluiten: autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties.

Fraude Signalering Voorziening in strijd met de beginselen van rechtmatigheid, doelspecificatie, juistheid en opslagbeperking. Het verwerkingsverbod had betrekking op de verwerking van het BSN in het btw-identicatienummer voor zzp'ers, waardoor derden via dit nummer, dat zelfstandigen op hun site moeten plaatsen, het BSN van de zzp'er konden achterhalen. Ook concludeerde de AP in onderzoek dat de Belastingdienst bij de bestrijding van fraude meerdere en ernstige overtredingen van de AVG en de Wbp heeft begaan, waaronder de onrechtmatige verwerking van persoonsgegevens, te langdurige opslag van gegevens, onvoldoende beveiliging en het niet-betrekken van de FG bij het uitvoeren van DPIA's. De AP heeft daarvoor geen boete opgelegd. Daarnaast heeft de AP onderzoek gedaan naar de beveiliging van informatie van de afdeling Datafundamenten & Analytics van de Belastingdienst. De Belastingdienst heeft geconstateerde beveiligingsrisico's na signalering daarvan door de AP voldoende ondervangen.[76]

De AP heeft ook een boete en een last onder dwangsom aan het UWV opgelegd.[77] De boete had betrekking op negen vergelijkbare datalekken bij het versturen van groepsberichten. Doordat steeds vergelijkbare lekken bij de UWV werden geconstateerd, bestond bij de AP het vermoeden dat de het UWV geen passende technische en organisatorische maatregelen heeft genomen om deze datalekken te voorkomen. Dat bleek inderdaad het geval te zijn, waarna een boete is opgelegd op grond van art. 13 Wbp en art. 32 AVG. De last onder dwangsom had betrekking op het ontbreken van meerfactorauthenticatie bij de toegang tot het werkgeversportaal. Daarnaast deed KPMG in opdracht van het UWV onderzoek naar het SONAR-systeem. Dit systeem bevat gegevens van werkzoekenden en wordt gebruikt om arbeidsbemiddeling door het UWV en gemeenten mogelijk te maken. De conclusie van dit onderzoek was dat het SONAR-systeem niet voldeed aan de eisen van de AVG.[78]

Uit onderzoek van de Volkskrant in 2019 bleek dat de DUO in strijd met de AVG gebruik heeft gemaakt van trackingssoftware.[79] De trackingsoftware werd gebruikt om aan te tonen dat een student een belangrijk bericht van de DUO heeft ontvangen. Bij de inzet van trackingsoftware worden meerdere persoonsgegevens verwerkt, zoals het IP-adres, het e-mailadres en tijdstip van opening. Naar aanleiding van dit onderzoek is de DUO in gesprek gegaan met de AP en gestopt met het gebruik van de software. Een overtreding is niet vastgesteld.

Daarnaast waren er meerdere (vermeende) overtredingen van de AVG bij uitvoeringsorganisaties waarbij de AP geen formeel handhavingsbesluit heeft genomen. Naar aanleiding van een gemeld datalek en berichtgeving in de media heeft de AP onderzoek gedaan naar de handel en diefstal van persoonsgegevens afkomstig uit systemen van GGD-GHOR. Vervolgens heeft de AP het toezicht op de GGD-GHOR geïntensiveerd. Van het CBR is bekend dat het in 2019 medische gegevens heeft toegevoegd aan digitale dossiers van anderen. Dit datalek is gemeld bij de AP.[80] Het COA deelde persoonsgegevens van asielzoekers met de politie, wat een extern onderzoeksbureau dat hiernaar onderzoek deed aanmerkte als een onevenredige inbreuk op de levenssfeer. [81] De Kamer van Koophandel (KvK) is door de AP aangesproken op het verkopen van namen en adressen van zzp'ers en bestuurders in het product 'Adressenbestand Online'. De AP constateerde dat de manier waarop deze gegevens verspreid werden niet

[76] AP, *Onderzoek naar Datafundamenten & Analytics*, 2021, p. 1.
[77] Zie voor deze besluiten: autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties.
[78] KPMG, *Deelonderzoek 1: SONAR*, 2020
[79] P. de Lange, 'DUO overtreedt privacyregels met volgsoftware in e-mails met studenten', *De Volkskrant* 2019.
[80] G. Pols, ´CBR erkent fout met medische dossiers: 'Dit mag echt niet gebeuren´', *Trouw* 2019.
[81] Brief van de minister van Justitie en Veiligheid en de staatssecretaris van Justitie en Veiligheid van 29 januari 2021, met kenmerk 3181786.

voldeed aan privacyregels. Hierop zijn geen handhavende maatregelen genomen, ook omdat de KvK zelf dit onderdeel van de gegevensverspreiding heeft gestopt.[82]

Algemeen beeld van naleving van de AVG

Op basis van de anekdotische bevindingen, maar ook op basis van interviews met de AP en de ADR stellen we vast dat ook bij de rijksoverheid sprake is van sterke verschillen bij de naleving van de AVG. Per departement en per afdeling of uitvoeringsorganisatie worden onafhankelijke keuzes gemaakt, soms ook op basis van verschillende uitgangspunten. Zo constateert de AP dat er twee scholen zijn ten aanzien van de rol van de FG binnen departementen: bij het ene departement meent men dat de FG alleen een rol heeft bij de processen binnen dat departement, bij het andere wordt de FG ook geacht een rol op te pakken in de wetgevingsprocessen die binnen dat departement plaatsvinden. Ook de ADR onderschrijft het belang van goede sturing vanuit de top om de naleving van de AVG goed op te zetten en vast te houden.

De AP tracht wel (deels via de FG's) om het interne toezicht bij departementen te verbeteren, maar 'dit gaat niet van harte'. Twee departementen hadden bijvoorbeeld tot voor kort een gezamenlijke FG. De AP is daar kritisch op en blijft waar mogelijk invloed uitoefenen om bewustzijn te creëren en de onafhankelijke positie van de FG's te versterken. De ADR ziet ook dat FG's in het verleden vaak werden geacht een deel van de verantwoordelijkheid voor gegevensbescherming op te pakken, terwijl dat echt bij de uitvoerende organisatie moet blijven. Dat bewustzijn is overigens in de afgelopen jaren wel gegroeid.

De ADR constateert dat het primaire proces bij departementen altijd voorrang krijgt, en dat daarbij alles zo snel en efficiënt mogelijk moet. Omdat er ook nog eens veel bezuinigingen zijn, wil men vaak niet investeren in privacybescherming. Privacy officers geven zelfs wel eens aan dat er wordt gehoopt op een privacylek of schandaal, zodat er in de nasleep meer investeringen vrijgemaakt kunnen worden voor privacybescherming.

Wat mogelijk meespeelt is dat bij de rijksoverheid soms het idee lijkt te bestaan dat men, omdat er altijd al gewerkt is in lijn met de Wet bescherming persoonsgegevens (Wbp), eigenlijk de zaken al op orde heeft voor wat betreft de AVG. Die misvatting lijkt volgens de AP nogal eens te bestaan in de gesprekken over nodige veranderingen. Toch ziet de ADR ook dat de AVG wel ontwikkelingen teweeg heeft gebracht, en dat er sprake is geweest van een mentaliteitsverandering. Bij sommige departementen worden privacy officers al in het wetgevingsproces ingezet, om zo mee te denken over proportionaliteit en noodzakelijkheid van de verwerking van persoonsgegevens. In de IT-strategie van verschillende departementen wordt meer aandacht geschonken aan gegevensbescherming, en ook in het politieke debat hebben privacy-overwegingen een belangrijkere rol gekregen. Een in de Tweede Kamer aangenomen motie schrijft voor dat alle uitvoeringsorganisaties een CPO moeten aanstellen.

Ook bij de rijksoverheid is het beeld dus hoofdzakelijk heel divers, maar ziet men over de gehele linie ook positieve ontwikkelingen ten aanzien van het bewustzijn over naleving van de AVG en het inrichten van een privacy-organisatie die daarbij goed toezicht kan houden en ondersteuning kan bieden.

[82] Kamer van Koophandel, *Kamer van Koophandel schrapt adressen-product na kritiek AP*, 12 maart 2019, te raadplegen via kvk,nl (laatst geraadpleegd op 8 november 2022).

4.4 Observaties met betrekking tot casestudy-onderzoek

We hebben geconstateerd dat, hoewel er veel anekdotische bevindingen zijn verzameld en er enkele onderzoeken naar de naleving van de AVG bij overheden zijn uitgevoerd, er geen goed beeld is van de naleving van de AVG door overheden. Dit heeft meerdere oorzaken. Ten eerste is de toezichthouder afhankelijk van rapportages en informatie vanuit de onder toezicht gestelde overheden. Op dat punt is het mogelijk dat informatie over naleving van de AVG niet volledig wordt gedeeld. Dit kan komen doordat de interne toezichthouder niet volledig op de hoogte is van wat er binnen zijn organisatie gebeurt op het gebied van gegevensverwerking. Ook is het denkbaar dat een proces waarbij sprake is van verwerking van persoonsgegevens niet als zodanig wordt herkend, en dat dus niet duidelijk is dat de AVG van toepassing is. Ten derde is de capaciteit van de toezichthouders beperkt, terwijl het toezichtsveld veel overheden en veel gegevensverwerkingsactiviteiten omvat. Er moet dus selectief worden omgegaan met de beschikbare capaciteit, en een deel van de activiteiten en overheden komt daardoor in beeld. Als laatste punt, dat vooral voor het onderhavige onderzoek van toepassing is, maakt de toezichthouder de voor het toezicht opgestelde rapportages vanuit het systeemgericht toezicht niet openbaar. Hierop kon dus voor dit onderzoek niet worden voortgeborduurd. Tegen die achtergrond hebben we gekozen voor het volgen van een brede benadering bij de selectie van casestudy's gericht op het realiseren van een spreiding over de verschillende typen overheidsorganisaties.

5 Casestudy's

5.1 Inleiding

Dit hoofdstuk bevat de verslaglegging van de casestudy's. Wij hebben ons op deze plek, omwille van de leesbaarheid, beperkt tot een verkorte weergave van de cases. Voor een uitgebreidere verslaglegging van de casestudy verwijzen wij naar bijlage 2 tot en met 10. In de verkorte weergaven van de cases gaan wij, na een korte uiteenzetting van het type organisatie en de verwerking van gegevens, in op het beleid en de organisatie-inrichting op het gebied van privacy. Vervolgens bespreken wij de uitvoering van de AVG in de praktijk. Hierbij gaan wij, afhankelijk van de casus, in op zaken als de wijze waarop binnen de organisatie kennis en bewustzijn over privacy wordt gecreëerd, de uitvoering van privacyprocessen zoals DPIA's en de feitelijke invulling van de taken op het gebied van privacy.

In meerdere casusposities werden organisaties met privacygerelateerde incidenten of vraagstukken geconfronteerd. Deze benoemen we los van de casestudy's op deze plek, omdat deze de herkenbaarheid van de betreffende casussen te groot zou kunnen maken. De kwesties betroffen een beveiligingsincident met een datalek tot gevolg, een structurele verwerking van persoonsgegevens waarvoor geen rechtsgrondslag bestond in een wettelijke taak of de introductie van een nieuwe technologie zonder dat vooraf voldoende inzicht bestond in de AVG-aspecten daarvan. Bij het aan het licht komen van deze incidenten hebben de verschillende organisaties lessen getrokken uit het incident en is het bewustzijn binnen die organisaties gegroeid. Dat heeft zijn weerslag gehad in organisatorische en technische maatregelen om dergelijke incidenten in de toekomst te voorkomen. In een casus hebben incidenten geleid tot overleg tussen overheidsorganisatie, wetgever en toezichthouder over het spanningsveld tussen de doelmatige uitvoering van wettelijke taken, de financiering van de taakuitvoering en de belangen van betrokkenen bij gegevensverwerking. Hierbij is geconstateerd dat de interpretatie van de uit te voeren taken een complexe materie kan zijn, en dat er sprake moet zijn van gezamenlijk optrekken bij het bepalen van wat wel en niet is toegestaan. Die onduidelijkheid creëert maatschappelijke druk die zich waarschijnlijk ook heeft vertaald in een groeiend bewustzijn binnen de organisatie.

De casestudybeschrijvingen hieronder zijn als volgt opgebouwd. Elke casestudy wordt eerst kort ingeleid. Vervolgens wordt gekeken naar het privacybeleid van de casestudyorganisatie. Daarna wordt ingegaan de op de organisatie-inrichting en hoe naleving van de AVG in de praktijk gestalte krijgt. Vervolgens worden de belangrijkste uitdagingen aan de orde gesteld waarna de casestudybeschrijving worden afgesloten met een met een korte analyse van de bevindingen.

5.2 Caseverslag ministerie

In deze paragraaf wordt de praktijk beschreven van de toepassing en naleving van de AVG door een ministerie. Dit ministerie kenmerkt zich als een ministerie, waarvan een zeer omvangrijke uitvoeringsorganisatie onderdeel is. Dit ministerie verwerkt voor de uitvoering van verschillende taken persoonsgegevens. Vanuit AVG-perspectief ondervindt dit ministerie meerdere uitdagingen. De privacy-organisatie is zich in de praktijk nog aan het vormen en ook het bewustzijn op het vlak van de bescherming van persoonsgegevens is nog in ontwikkeling. Daarnaast wordt er, mede ingegeven door de actualiteit, een noodzaak gevoeld om persoonsgegevens te verwerken, waarvoor de van toepassing zijnde wetgeving geen grondslag geeft.

In het kader van deze casestudy hebben wij gesproken met de AVG-coördinator, de FG voor de AVG, de FG voor de Wpg, twee teamleiders van afdelingen waarbinnen diverse persoonsgegevens worden verwerkt, het hoofd van een beleidsafdeling en een beleidsmedewerker van diezelfde afdeling. Het privacybeleid van het ministerie is bestudeerd, evenals het Model gegevensbeschermingseffectbeoordeling rijksdienst. Daarnaast zijn brieven van de minister aan de Tweede Kamer die zien op de verwerking van persoonsgegevens door dit ministerie bestudeerd.

5.2.1 Beleid

Met het van toepassing worden van de AVG heeft de staatssecretaris privacybeleid in een regeling vastgesteld. Dit document beoogt richting te geven aan hoe de organisatie om moet gaan met privacy en laat zien dat de organisatie de privacy waarborgt, beschermt en handhaaft. Dit beleid is in beginsel van toepassing op alle verwerkingsactiviteiten binnen deze organisatie, behalve voor zover bepaalde verwerkingsactiviteiten op grond van de UAVG door de minister daarvan worden uitgesloten. In de regeling wordt het AVG-beheer uiteengezet. Daarnaast wordt aandacht besteed aan de omgang met verwerkers, zijn de verplichtingen van de verwerkingsverantwoordelijke nader uitgewerkt, waaronder het register van verwerkingsactiviteiten, informatiebeveiliging en de meldplicht datalekken, en worden de rechten van betrokkenen en de inzet van de DPIA om tot risicobeheersing en controle daarop te komen, besproken.

5.2.2 Organisatie-inrichting

Het ministerie hanteert het *three lines of defence*-model; al wordt dit niet nadrukkelijk in de regeling of de toelichting daarbij benoemd.

De *eerste lijn* is de lijnorganisatie. De eindverantwoordelijkheid van het AVG-beheer ligt bij de plaatsvervangend Secretaris-Generaal. De hoofden van de dienstonderdelen zijn belast met de naleving van de AVG en de specifieke regelgeving ten aanzien waarvan verwerkingen worden gevoerd. Deze AVG-beheerders kunnen deze zorgplicht geheel of gedeeltelijk opdragen aan een AVG-onderbeheerder binnen het dienstonderdeel. De verwerkingsverantwoordelijke – zijnde de minister – blijft bevoegd de uit de AVG voortvloeiende bevoegdheden van een verwerkingsverantwoordelijke zelf uit te oefenen.

De *tweede lijn* wordt, naast de beveiligingsfunctionarissen, gevormd door de AVG-coördinatoren binnen de dienstonderdelen. Deze functionarissen fungeren als privacy officers. De AVG-coördinator wordt in veel gevallen bijgestaan door een jurist. De AVG-coördinator coördineert de uitvoering van de AVG en de specifieke wetgeving binnen het dienstonderdeel als ook de feitelijke handelingen die daarvoor nodig zijn. Begin 2023 zal ook een centrale AVG-

Coördinator worden aangesteld. Doordat een centrale AVG-coördinator niet binnen de organisatie aanwezig is, ontbreekt op dit moment een wezenlijke centrale schakel in de privacyorganisatie die mede beleidsmatige verantwoordelijkheid neemt voor het signaleren, het behandelen en implementeren van organisatiebrede privacyvraagstukken en voor het in gang zetten van algemene kennisoverdracht.

De *derde lijn* is het interne toezicht dat op grond van de AVG is belegd bij de FG. De AVG verbindt eisen aan de positionering van een FG. Zo ziet de FG onafhankelijk toe op de naleving van de AVG in de betreffende organisatie en heeft de FG toegang tot het bestuur van de organisatie. De FG is binnen de organisatie zodanig gepositioneerd dat dit recht doet aan de positie die de FG op grond van de AVG dient te bekleden. De FG heeft toegang tot de AVG-beheerders, de Secretaris Generaal en de minister. Daarnaast hanteert de FG een systematiek van toezichtjaarplannen en toezichtjaarverslagen.

5.2.3 Praktijk

De FG brengt jaarlijks een toezichtsjaarverslag aan de minister uit over de naleving van de AVG. Hetgeen leidt tot voornemens om de gedane aanbevelingen op te volgen. De opvolging daarvan lijkt in de praktijk echter onvoldoende handen en voeten te krijgen. Er wordt geen integraal beleid opgesteld om de aanbevelingen om te zetten in acties en deze in de hele organisatie door te voeren.

Uit de interviews komt naar voren dat een centrale AVG-coördinator in de rol CPO wordt gemist. De FG wordt mede daardoor vaak in de rol van adviseur op de meer AVG-beleidsmatige thema's gemanoeuvreerd, waardoor de FG onvoldoende in staat wordt gesteld om de interne toezichtrol op toereikende wijze in te vullen. Vanuit de eerste lijn wordt een CPO gemist die AVG-beleidsstandpunten kan verwoorden en op beleidsmatig vlak richting kan geven. In de praktijk blijkt volgens de geïnterviewden dat bij de lijnorganisatie (de eerste lijn) vaak veel vragen leven over de taakuitoefening in relatie tot de verwerking van persoonsgegevens, maar dat de eerste lijn vaak niet weet hoe te acteren. De eerste lijn voelt zich daarin niet altijd gehoord, waardoor escalatie naar boven in de lijn moeizaam verloopt.

Uit de interviews komt het beeld naar voren dat het privacybewustzijn binnen de organisatie relatief laag is. Als gevolg van een incident dat zich heeft voorgedaan, is er bij de dienstonderdelen wel een grotere alertheid ontstaan over de vraag of zij persoonsgegevens mogen verwerken. Dit leidt tot een kramp bij medewerkers. Dit bewustzijn hoe om te gaan met beveiligingsincidenten lijkt voort te komen uit de naleving van andere geldende strenge veiligheidsnormen en niet zozeer uit het bewustzijn over het belang van de AVG. Het vergroten van bewustzijn over de AVG ligt niet alleen bij de FG, maar is ook een taak van de AVG-beheerders. Dit wordt binnen de organisatieonderdelen opgepakt door het organiseren van interne cursussen die afgestemd zijn op de specifieke doelgroep. Ook vanuit de FG worden jaarlijks opleidingen georganiseerd om de AVG-bewustzijn te vergroten. Dit vergt echter tijd vanwege het gevoerde personeelsbeleid waardoor medewerkers veelal maar enkele jaren in een functie zitten om vervolgens te rouleren.

Een DPIA wordt geïnitieerd door de proceseigenaar van een IT-dienst of door de betrokken beleidsdirectie bij de ontwikkeling van beleid en regelgeving. De DPIA wordt conform het Model gegevensbeschermingseffectbeoordeling rijksdienst uitgevoerd. De privacycoördinator speelt hierbij een coördinerende rol. Een DPIA wordt doorgaans pas opgesteld wanneer de activiteit, waarvan de verwerking onderdeel uitmaakt, is gestart. Bij het uitvoeren van een

DPIA streeft de organisatie er naar de DPIA conform de AVG eerder in het proces uit te voeren. Op dit moment wordt te laat de vraag gesteld of en welke persoonsgegevens worden verwerkt en of de verwerking risicovol is. De rol van de FG bij het DPIA-proces lijkt meer op de achtergrond te zijn en wordt omschreven als vrij theoretisch. Dit lijkt samen te hangen met het feit dat de FG niet gaat over beleidsstandpunten.

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende verwerkersovereenkomst en de DPIA. De AVG-coördinatoren zorgen voor de registratie van de verwerkingsactiviteiten en het actueel houden van dit register.

De AVG-regeling legt de verantwoordelijkheid voor het melden van een datalek bij de AVG-(onder)beheerder dan wel de AVG-coördinator. De alertheid om dergelijke incidenten op te pakken is hoog vanwege de geldende veiligheidsnormen. Ook vanuit de top is hier veel aandacht voor. Op dergelijke incidenten wordt dan ook direct actie ondernomen.

Binnen dit ministerie wordt geworsteld met de bestaande wettelijke taken en de actuele noodzaak om bepaalde activiteiten te ontplooien die niet binnen die wettelijke taken vallen. Gezocht wordt naar een mogelijkheid om recht te doen aan die actuele noodzaak. Daarbij richt het ministerie zijn blik op de inzet van de rechtsgrond gerechtvaardigd belang. Dit geeft volgens de geïnterviewden het ministerie de mogelijkheid om verwerkingsactiviteiten te ontplooien, waarvoor een grondslag in wetgeving ontbreekt. Onduidelijk voor het ministerie is wel of op grond van de AVG gerechtvaardigd belang kan worden ingezet. Overheidsinstanties mogen op grond van artikel 6, eerste lid, AVG in het kader van de uitvoering van hun taken zich namelijk niet baseren op de rechtsgrond gerechtvaardigd belang bij de verwerking van persoonsgegevens. Overheidsinstanties kunnen andere verwerkingen die raken aan de bedrijfsvoering wel baseren van de rechtsgrond gerechtvaardigd belang. De vraag is echter volgens de geïnterviewden hoe ver die ruimte die de AVG geeft, reikt.

5.2.4 Uitdagingen

Uit de casestudy volgt dat de tweede lijn beleidsmatig en in de praktijk moet worden uitgewerkt en versterkt. Dit begint met het aanstellen van een centrale privacy-coördinator. De privacyvolwassenheid van de eerste lijn is gebrekkig. De eerste lijn worstelt met AVG-vraagstukken en voelt zich onvoldoende gehoord door de beleidsverantwoordelijken. Het ontbreken van een CPO lijkt zich hier te wreken. Een verdere inbedding van het juist doorlopen van het DPIA-proces dient vanuit de eerste lijn prioriteit te krijgen. Doordat de jaarlijkse bevindingen van de FG, ondanks voornemens daartoe, onvoldoende opvolging krijgen, lijkt uitgestraald te worden dat aan de AVG onvoldoende belang wordt toegekend.

5.2.5 Analyse

Er wordt ingezet op scholing van medewerkers over het belang van naleving van de AVG. Hiervoor worden zowel algemene als meer toegesneden opleidingen aangeboden, zowel vanuit de privacy-organisatie per organisatieonderdeel alsook vanuit de FG. Het effect hiervan lijkt niet optimaal vanwege het periodiek rouleren van medewerkers en leidinggevenden.

Bij het ontbreken van een CPO wordt de adviesrol van de tweede lijn niet centraal ingevuld, waardoor richtinggevende beleidsstandpunten door de eerste lijn worden gemist. Dit staat de verdere groei van de privacyvolwassenheid van de eerste lijn in de weg. Ook leidt het ontbreken van de CPO ertoe dat de FG onvoldoende de eigen rol kan vervullen.

De privacyvolwassenheid van de organisatie wordt als relatief laag gekwalificeerd. De normgetrouwheid lijkt vooral voort te komen uit een correcte naleving van andere normen die overeenkomen met die uit de AVG, dan dat dit is ingegeven vanuit de AVG. De AVG staat in de dagelijkse praktijk onvoldoende op het netvlies bij de medewerkers. Ook lijken de vaardigheden te ontbreken om privacyvragen te herkennen en tijdig onder de aandacht te brengen van de tweede en in de praktijk vooral de derde lijn.

De organisatie ondervindt een spanningsveld tussen het belang van de bescherming van persoonsgegevens en het belang van de centrale beleidsdoelstelling. De organisatie ervaart op dat vlak handelingsverlegenheid doordat een wettelijke taak ontbreekt om bepaalde verwerkingsactiviteiten te ontplooien die noodzakelijk worden geacht om de primaire taak te kunnen uitoefenen. De organisatie zoekt binnen de kaders van de AVG naar oplossingen en is daarbij geneigd om de juridische grenzen op te zoeken.

De Tweede Kamer heeft vanuit haar taak vanzelfsprekend invloed op de besluitvorming die binnen het ministerie plaatsvindt, waarbij de verwerking van persoonsgegevens een rol speelt. Aan wensen, geuit door de Tweede Kamer, wordt door het ministerie niet zonder meer invulling gegeven. Soms kan dit niet vanwege beperkingen die uit de AVG voortvloeien. Bijvoorbeeld omdat een grondslag op grond van de AVG ontbreekt. Indien dit zo is, wordt dit door de minister teruggegeven aan de Tweede Kamer. Op basis van de interviews ontstaat het beeld dat de Tweede Kamer zich doorgaans bewust lijkt te zijn van de specifieke positie van het departement bij de naleving van de AVG en van het feit dat het department het belang van de bescherming van persoonsgegevens nadrukkelijk bij de standpuntbepaling en besluitvorming betrekt.

Toezicht en handhaving vindt vooral plaats door middel van intern toezicht. De AP speelt bij de naleving van de AVG niet direct een rol en staat op afstand. Ook ontbreekt een vast aanspreekpunt.

5.3 Caseverslag uitvoeringsorganisatie 1

Deze casestudy betreft een agentschap. Het agentschap is zelf geen bestuursorgaan, en heeft als zodanig ook geen eigen FG. Het privacybeleid is deels gecentraliseerd onder het departement en vervolgens binnen de eigen organisatie doorvertaald en passend gemaakt voor de eigen situatie. Het agentschap verwerkt op grote schaal gegevens voor het onderhouden van contacten met betrokkenen, het voorbereiden van inspecties, onderzoeken en monitoring van bepaalde economische activiteiten.

In deze casestudy zijn gesprekken gevoerd met twee medewerkers van de interne auditdienst, de CPO van de uitvoeringsorganisatie, de CPO van het ministerie waar de organisatie onder valt en de FG van dit ministerie. Ook is het departementale privacybeleid bestudeerd.

5.3.1 Beleid

Het privacybeleid dat zicht richt op het agentschap is op departementaal niveau vastgesteld. Het is geschikt als beleid voor alle directies, uitvoerende organisaties en agentschappen, maar kan ook als raamwerk worden gebruikt indien een decentraal opgesteld privacybeleid de voorkeur heeft.

De praktijk bij de bestudeerde organisatie blijkt nog niet aan te sluiten bij de ambities zoals die in het beleid zijn beschreven. De naleving van AVG en vooral het werken volgens het principe van *privacy by design* is in de praktijk nog niet vanzelfsprekend. De voornaamste oorzaken daarvoor zijn verouderde IT-systemen en persoonlijke verschillen in opvattingen over de naleving van AVG. Een derde factor die van belang is, is dat er soms grote druk op de organisatie staat binnen de primaire processen, waardoor de aandacht voor privacyvraagstukken er soms bij inschiet.

5.3.2 Organisatie-inrichting

De privacygovernance binnen het departement is gebaseerd op het concept van *three lines of defence*, zoals dat vaker wordt toegepast. Hierbij is het lijnmanagement verantwoordelijk voor strategisch beleid, risicobeheersing en het borgen van de naleving van privacywetgeving. De tweede lijn wordt gevormd door het 'CIO-stelsel', met aan het hoofd 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 van het departement en de Auditdienst Rijk. Ook voor de privacy officers geldt dat er een departementale CPO is aangesteld, en daarnaast ook CPO's bij organisatieonderdelen. Deze zijn gezamenlijk verantwoordelijk voor het ondersteunen van lijnmanagement bij implementatie en naleving van privacybeleid.

De FG is zoals gezegd geen onderdeel van een van de *three lines of defence*, maar is een onafhankelijke, interne adviseur en toezichthouder. De gedachte hierachter is dat het departement de naleving van de AVG en Wpg zonder advies of toezicht van de FG correct uit wil (kunnen) voeren. In de praktijk van het bestudeerde agentschap staat de FG dus behoorlijk op afstand van die organisatie. De lijnen lopen in dit geval via de departementale CPO en de decentrale privacy officers. Door de FG wordt het privacyplatform op departementaal niveau als belangrijk gremium aangeduid. Dit platform vergadert structureel over actuele zaken en hulpvragen vanuit verschillende organisaties binnen het departement.

Het agentschap beschikt over een eigen CPO en privacy officers. De CPO vertaalt het departementale privacybeleid naar de eigen organisatie en is verantwoordelijk voor de dagelijkse afhandeling van privacyzaken. Samen met de privacy officers fungeert hij als vraagbaak voor het lijnmanagement en adviseren ze over risico's en mitigatie daarvan. Voor de uitvoering van het werk schakelen ze met privacyfunctionarissen binnen diverse onderdelen van de organisatie. Hierbij is geen sprake van een hiërarchische relatie, maar van een coördinerende rol richting het departement en andere overheidsorganen.

5.3.3 Praktijk

Naast door het CIO-office opgezette cursussen hebben de verschillende diensten, waaronder het agentschap, ook eigen cursussen voor medewerkers die meer toegesneden kunnen zijn op het werk binnen de organisatie. Bij aanpassingen van informatiesystemen wordt structureel een beoordeling van de veiligheidsrisico's uitgevoerd.

Voor het uitvoeren van DPIA's volgt het agentschap de departementaal voorgestelde processtappen. Er is geen specifieke procesbeschrijving voor het agentschap opgesteld. De proceseigenaar is primair verantwoordelijk voor het uitvoeren van de DPIA, en schakelt voor de uitvoering de privacycoördinator in. Ook voor verwerkersovereenkomsten wordt het

departementaal beleid gevolgd. Voor het oppakken van datalekken binnen de eigen dienst heeft het agentschap wel een eigen procedure.

Om diverse redenen, waaronder onzekerheid over de invulling van de rol van privacy officer, is een groot aantal functies van privacy officers vacant. Hierdoor zijn de op papier uitgedachte overleg- en sturingslijnen onder druk komen te staan en is de inrichting van een volwaardige privacy-organisatie met contactpunten in alle onderdelen van de organisatie vertraagd. De rol van privacy officer wordt nu vaak ingevuld door mensen die weinig expertise hebben in dit kennisgebied. Overigens heeft dat in de praktijk niet tot problemen ten aanzien van de naleving van de AVG geleid. Bij een audit is geconstateerd dat mensen in de lijn zonder duidelijke sturing toch goed conform de AVG werken (onbewust bekwaam). Het geconstateerde probleem bestaat er vooral uit dat die momenteel goed uitgevoerde processen niet overal geborgd zijn, en dat met de eventuele veranderingen van personeel de naleving van AVG alsnog onder druk kan komen te staan.

5.3.4 Uitdagingen

De eerste uitdaging bij deze organisatie betreft de beleving van het belang van naleving van de AVG. Hierin worden tussen diensten en tussen afdelingen verschillen geconstateerd. Ten tweede is geconstateerd dat het (tijdelijk) moeilijk is gebleken om de posities van decentrale privacy officers in te vullen en bezet te houden. Als gevolg hiervan kan afstemming tussen privacy- en lijnorganisatie niet optimaal ingevuld zijn of worden. Ten slotte is gebleken dat de kennis van privacycoördinatoren niet altijd is toegerust op de verantwoordelijkheden die zij hebben. Het is de vraag of de in het beleid vastgelegde verantwoordelijkheden reëel zijn, gezien de soms beperkte omvang van deze rol binnen elke afdeling.

5.3.5 Analyse

Over het algemeen zien we in deze casus een organisatie die op veel vlakken het departementale privacybeleid volgt en gebruik maakt van de mogelijkheden die de departementale privacy-organisatie biedt, en daar ook positieve ervaringen mee heeft. Onder meer op het gebied van kennisdeling en overleg over privacyvraagstukken worden vruchten geplukt. Tegelijkertijd is er aandacht voor de invulling en uitwerking van het beleid op organisatieniveau. Er is binnen de organisatie sprake van een privacy-organisatie die op papier ook binnen afdelingen is ingevuld door decentrale privacy officers en -coördinatoren. De huidige situatie wijkt tijdelijk af van die gewenste situatie, doordat een aantal privacy officers de functie heeft neergelegd. Dit komt deels voort uit een interne discussie over de invulling van deze functie, waaruit blijkt dat geen sprake is geweest van een breed gedragen, duidelijk geluid waarin alle betrokkenen zich konden vinden. Het gevolg is dat de beoogde communicatielijnen tussen privacy- en lijnorganisatie nu niet overal zijn ingevuld.

In het algemeen kan ook worden gesteld dat principes van de AVG binnen het agentschap volledig van toepassing worden geacht en dat het beleid hier ook goed op is ingericht; eventuele niet naleving van de AVG is niet te wijten aan met de wet strijdige wensen of weerstand tegen de privacywetgeving, maar eerder aan hoge werkdruk en prioriteitsstelling.

5.4 Caseverslag uitvoeringsorganisatie 2

Deze casestudy betreft een zbo die persoonsgegevens verwerkt voor de eigen organisatie met meer dan 1000 werknemers, maar ook onder andere persoonsgegevens beheert die in enkele openbare registers worden opgenomen.

In het kader van deze casestudy is gesproken met een directeur, een beleidsadviseur die zich bezig houdt met dataverwerking, de CISO en de FG. De zbo heeft het privacybeleid, het jaarrapport van de FG voor het jaar 2021, een rapport over mogelijke verbeteringen op het gebied van gegevensverwerking, de privacyverklaring en procesbeschrijvingen voor het uitvoeren van DPIA's en het melden van datalekken verstrekt.

5.4.1 Beleid

Voor het privacybeleid is enige tijd na de inwerkingtreding van de AVG een document vastgesteld, dat voor de hele organisatie van toepassing is. In dit document worden allereerst de visie op privacy, het juridisch kader en de principes met betrekking tot privacy geformuleerd. Vervolgens wordt de inrichting van de organisatie en de verdeling van verantwoordelijkheden bij bepaalde actoren beschreven, en is vastgelegd onder welke voorwaarden eventueel van het privacybeleid kan worden afgeweken.

5.4.2 Organisatie-inrichting

In het privacybeleid is voor dertien privacygerelateerde taken een beschrijving van (mede)verantwoordelijke personen of afdelingen. Er is geen beschrijving gegeven van eventuele overlegstructuren, en de verantwoordelijkheden zijn op hoofdlijnen beschreven.

Het vaststellen van het beleid is belegd bij de bestuurlijk hoofdverantwoordelijke entiteit binnen de organisatie. Deze entiteit stelt tevens de Privacyverklaring vast. Een afdeling JZ vervult een rol die we bij andere organisaties veelal bij CPO's belegd zien. Deze afdeling adviseert bij de uitvoering van DPIA's en het opstellen van verwerkersovereenkomsten, beheert het verwerkingsregister en biedt ondersteuning aan lijnafdelingen bij het invullen ervan, beantwoordt tweedelijns privacyvragen en verzorgt de afhandeling van verzoeken van betrokkenen op grond van de AVG.

Het lijnmanagement is primair verantwoordelijk voor correcte naleving van de AVG, waaronder de uitvoering van DPIA's, en de bewaking van maatregelen die eruit voortvloeien, het op peil brengen van het privacybewustzijn, het nakomen van verplichtingen ten aanzien van de documenteerplicht, vaststelling en realisering van bewaartermijnen, het zorgen voor verwerkersovereenkomsten en het bewerkstelligen van informatiebeveiliging. Bij verschillende taken zijn partijen benoemd die in de uitvoering kunnen ondersteunen, zoals een compliance-afdeling, de afdeling personeelszaken (voor opleidingen) privacy-ambassadeurs en een team voor beveiligingsincidenten. In sommige gevallen is er ook een security officer binnen de afdeling aangesteld.

De FG heeft geen directe verantwoordelijkheid bij privacygerelateerde taken. Hij dient onder meer eens per kwartaal aan de bestuursverantwoordelijke entiteit te rapporteren over de stand van zaken omtrent verwerking van persoonsgegevens in de organisatie. Hij signaleert risico's en treedt daarover in overleg met het management, houdt intern toezicht op naleving van de AVG en adviseert en ondersteunt. Een aparte rol is weggelegd voor een bestuurder die op strategisch niveau verantwoordelijk is voor de integriteit en kwaliteit van de beheerde gegevens.

In de praktijk is gebleken dat niet altijd geacteerd wordt op de adviezen van de FG en dat deze soms terzijde worden geschoven of dat maatregelen niet direct worden opgepakt. Hierbij kan een rol spelen dat men de risico's of schade voor betrokkenen waarvan persoonsgegevens zijn verwerkt als beperkt inschat. In combinatie met soms hoge werkdruk kan dit zorgen voor een lagere prioritering van correctieve maatregelen. Het privacybewustzijn is wat dat betreft nog niet optimaal, al zien gesprekspartners wel een licht positieve trend hierin.

5.4.3 Praktijk

Naleving van de AVG is primair een verantwoordelijkheid van de medewerkers zelf is. Door middel van online cursussen worden deze op de hoogte gebracht van de risico's met betrekking tot de verwerking van persoonsgegevens in hun functie. De manager van de afdeling personeelszaken draagt verantwoordelijkheid voor het opleidingsplan met betrekking tot privacykennis.

Als een voortvloeisel uit het *privacy by design*-principe wordt vooraan in het ontwerptraject van nieuwe activiteiten of processen (of aanpassingen) een check uitgevoerd of een DPIA nodig is aan de hand van een checklist. Op basis hiervan kan een JZ-adviseur tot de conclusie komt dat een DPIA inderdaad nodig is en volgt een gesprek over vervolgstappen. De uitvoering van DPIA en het documenteren ervan is de eindverantwoordelijkheid van de manager. Daarbij is gebleken dat bij DPIA's adviezen van privacyspecialisten niet altijd als leidend worden gezien.

Bij datalekken is de afdeling JZ verantwoordelijk voor de eerste interpretatie van de melding op aard en urgentie, en van de noodzaak tot melding bij de AP. De eindverantwoordelijkheid voor maatregelen ligt weer bij de verantwoordelijk directeur. Voor verwerkersovereenkomsten is een modelovereenkomst in gebruik waar alleen van kan worden afgeweken, onder verantwoordelijkheid van de lijnmanager, als er overleg is geweest met de FG en een security officer.

De FG stelt als intern toezichthouder jaarlijks een rapportage op. Hierin wordt onder meer de stand van zaken met betrekking tot datalekken, actuele vragen, privacybewustzijn, de inzet van DPIA's en het gebruik van het verwerkingsregister aan bod, waarbij ook trends over de jaren worden geschetst.

Uit de interviews die we hielden is gebleken dat de cultuur in de organisatie niet altijd en overal overeenkomt met de ambities zoals geformuleerd in het beleid. Het komt wel eens voor dat opgetekende risico's niet direct ten volle serieus worden genomen of dat maatregelen om de risico's te mitigeren geen prioriteit krijgen. Pas wanneer er reële nadelen voor de eigen organisatie dreigen komt men definitief in beweging. Hierin bestaan overigens grote verschillen tussen afdelingen en specifieke personen. In de praktijk is duidelijk geworden dat de FG vooral vanuit een adviesrol opereert, en dus geen absolute doorzettingsmacht heeft.

5.4.4 Uitdagingen

Bij deze organisatie is gebleken dat een voorname kwetsbaarheid in de cultuur van omgang met wetgeving en intern beleid zit. De naleving van de AVG is een van de factoren die in belangenafwegingen wordt meegenomen, maar geen topprioriteit. Dit is sterk afhankelijk van specifieke personen in het lijnmanagement. Er wordt nogal eens voor gekozen om eerst primaire processen op orde te krijgen alvorens aandachtspunten op het gebied van privacy op te pakken. Dit proces is dus niet geborgd in processen. Daarbij is geconstateerd dat beperkte

capaciteit op de werkvloer een negatief effect kan hebben op de aanpak van privacygerelateerde aandachtspunten.

5.4.5 Analyse

Het algehele beeld over deze organisatie is dat de organisatie veel aandacht heeft besteed aan het goed inrichten van beleid en processen met betrekking tot gegevensverwerking. Ook ten aanzien van het privacybewustzijn wordt heel serieus gehandeld, met scholing zowel bij aanvang van het dienstverband als periodiek daarna. Tot op strategisch niveau zijn privacyfunctionarissen of mensen met expertise op dit gebied in de organisatie terug te vinden. Daarbij is de rode lijn dat lijnmanagement verantwoordelijk is voor het in kaart brengen van te nemen maatregelen en uitvoering daarvan, waarbij steeds expertise kan worden ingeroepen vanuit de verschillende onderdelen van de privacy-organisatie. De grootste kwetsbaarheid zit hem in het feit dat adviezen vanuit privacyfunctionarissen nog in een afweging meegenomen moeten worden, en daarbij soms op de achtergrond raken uit doelmatigheidsoverwegingen. Daarmee wordt de naleving van de AVG soms optioneel, of wordt het in ieder geval soms op een langer plan geschoven, afhankelijk van de betrokken managers.

5.5 Caseverslag uitvoeringsorganisatie 3

Deze paragraaf beschrijft de praktijk van de naleving door een uitvoeringsorganisatie. De kerntaak van de organisatie bestaat uit het beheren van enkele registers. Deze registers bevatten met name gewone persoonsgegevens, maar kunnen ook bijzondere persoonsgegevens en strafrechtelijke gegevens bevatten. De gegevens uit de registers worden gedeeld met andere overheden; het merendeel van deze gegevensdeling verloopt geautomatiseerd. De uitvoeringsorganisatie verwerkt daarnaast ook gegevens bij het contact met burgers en als werkgever. De organisatie is ISO-gecertificeerd; in dat kader vinden externe audits plaats.

In het kader van deze casestudy is gesproken met de centrale privacy officer, twee decentrale privacy officers, een directeur, een manager van een afdeling waarbinnen veel gegevens worden verwerkt en de FG. De uitvoeringsorganisatie heeft verschillende beleidsdocumenten op het gebied van privacy en informatiebeveiliging toegezonden. Dit betreft onder andere een document met betrekking tot de privacygovernance, het gegevensbeschermingsbeleid, het leveranciersmanagementbeleid en het dataclassificatie- en sourcingsbeleid. Ook heeft de uitvoeringsorganisatie diverse werkinstructies, templates en een opleidingsplan verstrekt.

5.5.1 Beleid

De functies, taken en verantwoordelijkheden zijn uiteengezet in een governancedocument. In dit document zijn ook de richtinggevende principes voor gegevensverwerking door de organisatie uiteengezet. Daarnaast beschikt de organisatie over een gegevensbeschermingsbeleid, op grond waarvan nader beleid is geformuleerd voor specifieke onderwerpen, waaronder dataclassificatie, de uitvoering van DPIA's, datalekmeldingen en leveranciersmanagement.

5.5.2 Organisatie-inrichting

De privacy-organisatie is ingericht volgens het *three lines of defence*-model. Een bijzonderheid is dat per organisatieonderdeel een decentrale privacy officer is gepositioneerd. Daarnaast is op de verschillende afdelingen binnen een organisatieonderdeel een medewerker aangewezen als contactpersoon op het gebied van privacy. Deze contactpersonen zijn van belang voor

de informatievoorziening van de decentrale privacy officers en het creëren van bewustzijn binnen hun onderdeel.

5.5.3 Praktijk

Binnen de uitvoeringsorganisatie wordt privacybewustzijn als belangrijke factor voor naleving van de AVG beschouwd. Dit bewustzijn draagt eraan bij dat medewerkers de privacyfunctionarissen vroegtijdig bij nieuwe projecten betrekken, eerder vragen stellen en datalekken signaleren en melden. De geïnterviewden constateren dat de trainingen en e-learningmodules het privacybewustzijn hebben vergroot; ook de positionering van de decentrale privacy officers op onderdeelniveau (in plaats van concernniveau) draagt bij aan het privacybewustzijn, omdat de privacy officers beter een netwerk kunnen opbouwen en benaderbaar zijn voor medewerkers.

De uitvoeringsorganisatie heeft de processen op privacygebied, de uitvoering van DPIA's, datalekmeldingen en het sluiten en evalueren van verwerkersovereenkomsten, uitvoerig beschreven. De DPIA's worden binnen de uitvoeringsorganisatie uitgevoerd door een multidisciplinair team, bestaande uit bijvoorbeeld medewerkers in de uitvoering, ICT-medewerkers en een privacy officer of security officer (afhankelijk van het onderwerp). In de interviews komt naar voren dat een DPIA binnen de uitvoeringsorganisatie niet als invuloefening wordt beschouwd, maar dat de processen en risico's uitvoerig worden besproken en er ook aandacht is voor dataethiek. De beoordeling en finale toetsing is respectievelijk aan een privacy officer en de FG.

De functie van FG wordt binnen de organisatie fulltime uitgeoefend. De FG neemt een onafhankelijke positie in en heeft toegang tot verschillende overleggen, zowel met het managementteam als met de raad van toezicht. De organisatie heeft enkele jaren geleden een centrale privacy officer aangesteld. Deze aanstelling beoogt te voorkomen dat de FG zich te intensief met uitvoeringswerkzaamheden moet bezighouden.

5.5.4 Uitdagingen

Volgens de geïnterviewden bestaat de belangrijkste uitdaging van de organisatie uit het continu bevorderen van het privacybewustzijn. Dit bewustzijn draagt eraan bij dat beleid daadwerkelijk wordt geïmplementeerd en is een belangrijke factor in de naleving van de AVG. Naast het continu onder de aandacht brengen van privacy is van belang dat het management blijvend voorbeeldgedrag vertoont en dat er actueel beleid is. Een andere uitdaging zijn digitaliseringsprojecten en de daarmee gepaard gaande privacyrisico's. De geïnterviewden geven aan dat aan de voorkant van het project rekening wordt gehouden met deze risico's en dat de privacy-organisatie hier tijdig bij wordt betrokken. Ook op dit vlak is het van belang dat medewerkers zich bewust zijn van de privacy-aspecten van hun werkzaamheden.

5.5.5 Analyse

De taakopvatting en cultuur van de organisatie lijken een belangrijke rol te spelen bij de naleving van de AVG. Privacybescherming wordt binnen de organisatie als onderdeel van de taak, het zorgvuldig beheren van de registers, beschouwd. In het kader van zorgvuldig registerbeheer houdt de organisatie zich al langere tijd, al voor invoering van de AVG, bezig met privacy. De organisatie heeft daardoor inmiddels een hoog volwassenheidsniveau bereikt: de organisatie beschikt over gedetailleerd beleid en over voldoende capaciteit om dit beleid op de werkvloer te implementeren; de wijze waarop de privacybescherming is georganiseerd wordt regelmatig geëvalueerd.

Binnen de uitvoeringsorganisatie bestaat een hoge mate van acceptatie van de AVG. Dit kan verklaard worden vanuit de zojuist beschreven taakopvatting, waarin privacybescherming als onderdeel van het zorgvuldig beheren van registers wordt beschouwd. Doordat privacybescherming deel uitmaakt van de taak wordt ook weinig spanning ervaren tussen de taakuitoefening en de naleving van de AVG. De hoge mate van acceptatie houdt onder andere in dat de directie belang hecht aan privacybescherming en daar ook voldoende capaciteit voor beschikbaar stelt.

De uitvoeringsorganisatie hecht belang aan het vertrouwen dat zij als overheidsinstelling geniet. Dat blijkt zowel uit het gesprek met de directeur als uit het gesprek met de FG. Volgens de directeur is het voor een overheidsorganisatie van belang is dat deze het vertrouwen behoudt; de FG geeft aan dat de organisatie zijn bestaansrecht ontleent aan het zorgvuldig beheren van de registers. Vanuit dit oogpunt is het volgens beiden van belang dat de organisatie conform de privacywetgeving handelt en dat zij dit ook naar buiten toe kan verantwoorden. Om die reden laat de uitvoeringsorganisatie externe audits uitvoeren. Deze audits dragen bij aan de verdere ontwikkeling van de organisatie op het gebied van privacy.

5.6 Caseverslag uitvoeringsorganisatie 4

Deze casebeschrijving doet verslag van het onderzoek naar de naleving door een uitvoeringsorganisatie. De uitvoering van haar taken brengt mee dat de uitvoeringsorganisatie contact heeft met burgers en professionele dienstverleners. De organisatie verwerkt hierbij persoonsgegevens. Doorgaans zijn dit namen, BSN-nummers en financiële gegevens, maar het kan ook gaan om strafrechtelijke of medische gegevens. Deze gegevens worden doorgaans door professionele dienstverleners aangeleverd. Het contact met burgers vindt plaats per post; datalekken veroorzaakt door het verkeerd adresseren van brieven krijgen binnen de organisatie veel aandacht.

In het kader van deze casestudy is gesproken met de CIO, CISO, FG en een medewerker die, naast de uitvoering van reguliere werkzaamheden, binnen een afdeling van de uitvoeringsorganisatie fungeert als centraal aanspreekpunt en privacyrisico's signaleert. In het vervolg wordt deze medewerker aangeduid als 'de contactpersoon'. De uitvoeringsorganisatie heeft de volgende documenten opgestuurd: een beleidsstuk waarin de governancestructuur is vastgelegd en een aanvulling daarop, het privacyhandboek, een zogenaamd awareness-plan om de bewustwording te bevorderen en een presentatie voor een training voor contactpersonen.

5.6.1 Beleid

In 2019 heeft de uitvoeringsorganisatie de governancestructuur ten aanzien van privacy vastgelegd in een beleidsdocument (het governancedocument). In dit document zijn de rollen en verantwoordelijkheden op het gebied van privacy uitgewerkt, waarbij het *three lines of defence*-model is gevolgd. Ook is vastgelegd dat er een periodiek privacy-overleg plaatsvindt, wat hierin wordt besproken en wie hierbij aanwezig zijn en beschrijft het document in grote lijnen hoe de samenwerking met het informatiebeveiligingsteam is geregeld.

Daarnaast beschikt de uitvoeringsorganisatie over een privacyhandboek. In dit handboek is in hoofdlijnen aangegeven hoe de organisatie omgaat met persoonsgegevens, bijvoorbeeld op het vlak van dataretentie, het afsluiten van verwerkersovereenkomsten en de vernietiging van persoonsgegevens. Het privacyhandboek vormt de basis voor andere beleidsdocumenten,

zoals een richtlijn voor e-mailgebruik en de procesbeschrijvingen voor datalekken, inzageverzoeken en DPIA's. Het handboek besteedt ook aandacht aan trainingen en bewustwording op het gebied van privacy.

5.6.2 Organisatie-inrichting

De privacy-organisatie is ingericht volgens het *three lines of defence*-model. Op elke afdeling is een medewerkers als contactpersoon aangewezen. Deze contactpersoon brengt privacy-aspecten onder de aandacht en fungeert binnen de betreffende afdeling als eerste aanspreekpunt over voor privacyvraagstukken. Op het gebied van informatiebeveiliging hebben zij dezelfde rol.

De FG heeft een aantal keren per jaar overleg met de directeur van de organisatie. De CIO zit ook in het managementteam. In gevallen dat er serieus iets verkeerd gaat op het gebied van privacy het managementteam wordt geïnformeerd. De FG wordt in die gevallen in de gelegenheid gesteld om kritische vragen te stellen.

5.6.3 Praktijk

Ter bevordering van het privacybewustzijn maakt de uitvoeringsorganisaties gebruik van e-learning modules. Alle medewerkers zijn verplicht om deze modules te volgen. Contactpersonen krijgen uitgebreidere trainingen die worden verzorgd door het privacyteam en de FG. Daarnaast maakt de organisatie gebruik van diverse 'awareness-prikkels', bijvoorbeeld het versturen van nep-phishingberichten. Binnen de afdelingen spelen de contactpersonen een rol bij het creëren van privacybewustzijn.

Binnen de organisatie is veel aandacht voor datalekken. Medewerkers begrijpen wanneer sprake is van een datalek, maar het komt soms voor dat een datalek niet wordt gesignaleerd. Gesignaleerde datalekken worden altijd gemeld bij de AP, zij het niet altijd binnen de daarvoor geldende termijn van tweeënzeventig uur. Ingeval van complexere datalekken wordt een privacy officer of de FG geïnformeerd. Tijdens het privacy-overleg wordt besproken of het datalek aanleiding geeft tot het nemen van maatregelen.

De uitvoeringsorganisatie heeft langdurige relaties met leveranciers. De CIO geeft aan dat dit een risico vormt, omdat de verwerkersovereenkomsten niet altijd goed in beeld zijn en in sommige gevallen ook zijn gedateerd. Dit wordt door de CIO als risico beschouwd.

De uitvoeringsorganisatie wisselt gegevens uit met andere overheden. Afgelopen jaar heeft de uitvoeringsorganisatie gegevensuitwisselingsbeleid vastgesteld, zodat de samenwerking met andere overheden beter kan worden georganiseerd. Dit beleid bevat een checklist over de grondslag en de noodzaak van de gegevensuitwisseling. De uitvoeringsorganisatie verwerkt ook persoonsgegevens in opdracht van het ministerie van Justitie en Veiligheid. De verwerkingsverantwoordelijkheid ligt in dat geval bij het ministerie. De FG geeft aan dat hij heeft gemerkt dat het ministerie moeite heeft om deze verwerkingsverantwoordelijkheid in te vullen.

De uitvoeringsorganisatie beschikt over een externe FG die sinds zomer 2021 werkzaam is bij de uitvoeringsorganisatie. De FG geeft aan dat het van belang is om draagvlak te creëren op privacygebied. Om die reden legt hij vooralsnog niet de focus op controle-activiteiten, maar kijkt hij mee met de verschillende privacyprocessen. De ervaring van een andere

geïnterviewde is dat de FG kritische vragen stelt, kennis van zaken heeft en op enige afstand van de organisatie staat.

5.6.4 Uitdagingen

De geïnterviewden geven aan dat de uitvoeringsorganisatie steeds professioneler te werk gaat op het gebied van privacy. Desondanks wijzen zij een aantal verbeterpunten aan. In de eerste plaats is op bepaalde punten sprake van achterstallig onderhoud: in de interviews komt naar voren dat de privacyverklaring en het verwerkingsregister moeten worden bijgewerkt. Zoals eerder besproken zijn ook sommige verwerkersovereenkomsten niet goed in beeld of verouderd. In het algemeen is de evaluatie van deze documenten een punt van aandacht; hiervoor is GRC-tooling in ontwikkeling.[83]

Daarnaast spelen er technische vraagstukken die zijn verbonden met informatiebeveiliging. Een van die vragen is hoe informatie binnen de systemen van de uitvoeringsorganisatie kan worden geïsoleerd. Ook het veilig werken vanuit de Cloud is een onderwerp dat binnen de uitvoeringsorganisatie aandacht krijgt. In meer algemene zin zijn volgens één van de geïnterviewden meer inspanningen nodig om volledig aan de eisen van de BIO te voldoen.

5.6.5 Analyse

De uitvoeringsorganisatie beschikt over een redelijk goed ontwikkelde privacy-organisatie die in staat is tot zelfevaluatie. De wijze van gegevensverwerking is uitgewerkt in het beleid, de rollen op het gebied van privacy- en informatiebeveiliging zijn vastgelegd en duidelijk voor betrokken en de FG neemt een onafhankelijke positie in. De privacyfunctionarissen hebben aandacht voor de aspecten van privacybescherming die nog verder ontwikkeld moeten worden.

Binnen de organisatie is veel aandacht voor het creëren van privacybewustzijn bij medewerkers. Dit hangt mogelijk samen met de aandacht die uitgaat naar datalekken door verkeerd geadresseerde post. Het voorkomen en herkennen van deze datalekken is afhankelijk van het gedrag van de betrokken medewerkers, waardoor veel aandacht wordt besteed aan het verbeteren van het gedrag.

Op organisatieniveau is geen sprake van factoren die de naleving van de AVG negatief beïnvloeden. De taakuitoefening van de organisatie wordt niet noemenswaardig gehinderd door de regels van de AVG. De AVG wordt binnen de organisatie dan ook niet als obstakel beschouwd of anderszins als ‘lastig’ ervaren. Dat laat onverlet dat medewerkers in hun dagelijkse werkzaamheden, wegens tijdsgebrek, niet altijd prioriteit geven aan de naleving van de AVG.

5.7 Caseverslag waterschap

De onderzochte organisatie betreft een waterschap met ongeveer 300 medewerkers. Waterschappen zijn verantwoordelijk voor voldoende en schoon water en zorgen voor bescherming tegen te veel water in Nederland. Het waterschap verwerkt in heel beperkte mate gegevens van inwoners, veel minder dan bijvoorbeeld gemeenten doen. Dat komt doordat het

[83] Governance, risk and compliance (GRC)-tooling heeft tot doel het inzetten van software om compliance-processen te stroomlijnen.

waterschap de heffing van de waterschapsbelasting heeft uitbesteed aan een regionaal belastingkantoor. De gegevens die het waterschap verwerkt betreffen hoofdzakelijk informatie over eigen medewerkers, de schouw en bezwaarprocedures.

In deze casestudy is gesproken met een lid van het dagelijks bestuur, een lid van de directie, een security officer en de teamleider van de afdeling Juridische Zaken. Tijdens het uitvoeren van de casestudy was de functie van FG vacant. Het waterschap heeft het handboek voor gegevensverwerking, het privacybeleid, het privacyreglement en een toetsings- en auditplan voor privacy-audits verstrekt.

5.7.1 Beleid

Het waterschap heeft in 2016 een privacyreglement, en in 2019 privacybeleid voor de periode 2020 – 2022 vastgesteld. Het beleid wordt momenteel geactualiseerd. Het privacybeleid dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de inrichtingskeuzes van privacy en te waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt. In het beleid worden de ambities en uitgangspunten uiteengezet. Ook deelt het beleid taken en verantwoordelijkheden toe binnen de organisatie op strategisch, tactisch en operationeel niveau. De PDCA-cyclus ten aanzien van privacy en gegevensverwerking is uitgewerkt in het beleid. Het waterschap heeft de ambitie om in 2023 volwassenheidsniveau 4 van het Capability Maturity Model voor privacy bereikt te hebben. Naast het privacybeleid beschikt het waterschap over een toetsings- en auditplan privacy en AVG. In dit plan is uitgewerkt op welk niveau de toetsen moeten plaatsvinden (binnen processen, over processen heen of op organisatieniveau), wie verantwoordelijk is voor de uitvoering van de toetsen en met welke regelmaat (periodiciteit) de toetsen worden uitgevoerd.

5.7.2 Organisatie-inrichting

Het waterschap heeft een privacy-organisatie die nog in ontwikkeling is, maar al een zekere mate van volwassenheid heeft bereikt. In een landelijke audit onder waterschappen scoorde de organisatie bovengemiddeld. De privacy-organisatie is ingericht op basis van het *three lines of defence*-model. De verantwoordelijkheden zijn belegd in de lijn. In de eerste lijn is per team iemand benoemd die als eerste aanspreekpunt en vraagbaak fungeert voor privacy gerelateerde vragen. Het aanspreekpunt voert deze taak uit naast zijn of haar reguliere taken en verantwoordelijkheden. In de tweede lijn zijn twee privacy officers gepositioneerd en de FG fungeert als toezichthouder in de derde lijn. Daarnaast is er een privacydesk in het leven geroepen waaraan vertegenwoordigers van personeelszaken, juridische zaken en de privacy officer deelnemen. Hier worden actiepunten uit het jaar- en uitvoeringsplan besproken, nieuws, actualiteiten, incidenten, datalekken en nieuwe wet- en regelgeving besproken.

5.7.3 Praktijk

Het waterschap heeft een eigen e-learning ontwikkeld om medewerkers te scholen in de verschillende facetten van privacy en wat daarin hun eigen verantwoordelijkheden zijn. Daarin worden de basisprincipes over privacy en informatiebeveiliging bijgebracht, de belangrijkste do’s en don’ts en het bewustzijn dat de grootste risico’s in het menselijk handelen zitten.

De aanspreekpunten op de werkvloer binnen de verschillende teams worden als zeer waardevol gezien. Zij zijn de ambassadeurs van het privacybeleid binnen de organisatie. De aanspreekpunten zorgen voor privacy bewustzijn binnen de gehele organisatie. Hun nabijheid op de werkvloer zorgt ervoor dat wanneer er bijvoorbeeld nieuwe projecten worden gestart, ook privacy-aspecten in ogenschouw genomen moeten worden. Dat leidt ertoe dat de privacy

officer steeds in een vroeg stadium wordt betrokken in het proces. Door middel van verplichte e-learnings.

Voor bepaalde processen worden DPIA's uitgevoerd. Dat gebeurt in de tweede lijn in samenwerking tussen privacy officer en een functioneel beheerder. Door middel van een Information Security Management System (ISMS), dat wordt voorgeschreven door de Baseline Informatiebeveiliging Overheid (BIO) wordt bepaald of voor een bepaald proces een DPIA moet worden uitgevoerd.

Het gros van de datalekken betreffen verkeerd geadresseerde e-mails. De organisatie probeert binnen de organisatie te benadrukken dat fouten maken menselijk is, dat datalekken kunnen voorkomen In geval van een datalek wordt er melding gedaan bij de privacy officer die een onderzoek instelt. Met de FG wordt een afweging gemaakt of er melding gedaan moet worden bij de AP. Alle datalekken worden in een datalekregister vastgelegd. Het management wordt hier middels een jaarrapportage over geïnformeerd**.**

Het management en bestuur van het waterschap geeft nadrukkelijk prioriteit aan de naleving van de AVG. Dat komt bijvoorbeeld tot uitdrukking in de wens van het management en bestuur om op de hoogte gehouden te worden van ontwikkelingen of onderzoeken die gedaan worden. De privacy officer wordt regelmatig gevraagd om een toelichting te geven in het MT rondom aan privacy gerelateerde ontwikkelingen binnen het waterschap. De lijnen tussen de privacy officer en de security officer met het MT zijn kort, zowel op formele als informele basis.

5.7.4 Uitdagingen

De belangrijkste uitdagingen waarvoor de organisatie gesteld staat is om voldoende bewustzijn en support te ontwikkelen en te behouden, maar ook om er voldoende capaciteit voor te hebben. Dat lukt tot dusver voldoende, maar de kunst is dit ook te behouden. Privacy wordt immers soms nog steeds gezien als 'iets dat men erbij moet doen', terwijl het een integraal onderdeel van de processen moet zijn. De verantwoordelijkheden met betrekking tot privacy liggen in de lijn, maar medewerkers moeten ook in staat gesteld worden om er voldoende aandacht aan te kunnen besteden.

Een belangrijk verbeterpunt voor deze organisatie dat in de audit onder waterschappen naar voren kwam is dat het Toetsings- en auditplan privacy en AVG dat is opgesteld nu ook in de praktijk gebracht moet worden. In het toetsingsplan is vastgelegd welke toetsen op welke processen, wanneer en door wie moeten worden uitgevoerd. Daar zit een belangrijke uitdaging waaraan de organisatie momenteel werkt.

5.7.5 Analyse

Er zijn verschillende factoren die de mate van naleving kunnen verklaren. Het waterschap hecht zichtbaar belang aan het ontwikkelen van het kennisniveau en het bewustzijn rondom privacyvraagstukken. Dat komt onder meer tot uitdrukking in de scholing van medewerkers via e-learnings waarin medewerkers de basisprincipes van de AVG en privacy worden bijgebracht en wat hun eigen verantwoordelijkheden hierin zijn. De aanspreekpunten op de werkvloer vormen enerzijds een vraagbaak voor werknemers, maar zijn daarnaast ook de ambassadeurs van het privacybeleid. Hun nabijheid in de organisatie zorgt ervoor dat het bewustzijn in de organisatie van privacy ontwikkeld wordt.

Over het algemeen worden de regels van de AVG geaccepteerd binnen de organisatie. Deze verklarende factor vloeit voort uit de toegenomen kennis van de regels. Nu de medewerkers binnen de organisatie in toenemende mate kennis opdoen van de privacyregelgeving, deze verinnerlijken en gaan doorzien welk belang de AVG dient, worden volgens onze gesprekspartners de regels geaccepteerd en draagt dit bij aan de naleving. Want wanneer naleving van de AVG zou worden gezien als een lastige bijzaak waarvan men nut en noodzaak niet inziet, zal de naleving tekortschieten.

5.8 Caseverslag gemeente 1

In deze paragraaf wordt de praktijk beschreven van de toepassing en naleving van de AVG door een van de grote steden in ons land. De gemeente verwerkt een grote hoeveelheid (bijzondere) persoonsgegevens en ziet zich onder meer geconfronteerd met grote uitdagingen met betrekking tot de taakuitvoering en de samenwerking in verschillende samenwerkingsverbanden met andere (overheids)partijen. Deze gemeente loopt in Nederland voorop bij het gebruik van algoritmes, maar is daarnaast ook nog druk bezig om het inzicht in de AVG binnen de organisatie te vergroten en de AVG tijdig onderdeel te laten zijn bij beleidsvorming en de implementatie van dat beleid. Daarnaast verwerkt deze gemeente persoonsgegevens voor de eigen organisatie.

In het kader van deze casestudy is gesproken met de concerndirecteur, de concern-privacy officer en de FG. Ook is een groepsgesprek gevoerd met een privacy officer, een beleidsadviseur, een teamleider en projectleider van een afdeling waarbinnen complexe gegevensverwerkingen plaatsvinden. De gemeente heeft een beschrijving van de governancestructuur, het privacybeleid, een overzicht van de bestaande privacy-overleggen en een richtlijn voor het melden van datalekken verstrekt. Ook is het register van verwerkingsactiviteiten online geraadpleegd.

5.8.1 Beleid

Met het van toepassing worden van de AVG heeft het college van burgemeester en wethouders het privacybeleid vastgesteld. Dit document maakt de AVG-governance binnen de organisatie inzichtelijk en beoogt richting te geven aan hoe de organisatie om moet gaan met privacy en laat zien dat de organisatie de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente waarin (bijzondere) persoonsgegevens worden verwerkt.

5.8.2 Organisatie-inrichting

Deze gemeente hanteert het *three lines of defence*-model. De eerste lijn is de lijnorganisatie. Zij is verantwoordelijk voor het realiseren van de doelen van de gemeentelijke organisatie, waarvan privacy een vast onderdeel behoort te zijn. De lijnorganisatie werkt volgens het privacybeleid met relevante privacykaders en vastgestelde processen. In de eerste lijn zijn de rollen en taken van het college van burgemeester en wethouders, de burgemeester, de algemeen directeur, de concerndirectie tot aan het lijnmanagement helder beschreven. Hieronder worden twee aspecten daarvan nader uitgelicht.

Een van de concerndirecteuren draagt de concernbrede verantwoordelijkheid voor de AVG. Naast de AVG is deze concerndirecteur ook verantwoordelijk voor ICT/informatiebeveiliging

en integriteit. Hij is voorzitter van de stuurgroep privacy, die het privacybeleid handen en voeten geeft voor het hele concern. Daarin zitten ook de concern-privacy officer, de FG en vertegenwoordigingen van alle clusters. Het gaat daarbij om zowel het interne privacybeleid voor de organisatie zelf, als algemeen beleid met betrekking tot uitvoering van de publieke taken.

Binnen de afdelingen zijn de proceseigenaren verantwoordelijk voor de naleving van de privacywetgeving en het privacybeleid. De proceseigenaar legt verantwoording af aan de clusterdirectie. Binnen de afdelingen zijn privacy-ambassadeurs aangewezen. Dit zijn medewerkers die naast hun primaire taak de AVG als aandachtsgebied hebben en oog hebben voor gegevensbescherming bij beleidsvorming en implementatie van beleid.

De tweede lijn, waarin disciplines van privacy, informatievoorziening en integrale beveiliging zitten, helpt de eerste lijn door het opstellen van kaders, het geven van advies over het toepassen van de kaders, coördinatie van activiteiten waar nodig. De tweede lijn wordt gevormd door de concern-privacy officer, privacy officers, de concern informatie security officer (CISO) en decentrale informatie security officer (DISO).

De rol van de privacy officers is met name die van adviseur van het management van elk cluster/directie. Daarnaast ondersteunt de privacy officer bij het verrichten van DPIA's en overlegt waar nodig met de concern-privacy officer over nieuwe ontwikkelingen. Per cluster zijn er een of meerdere privacy officers. Deze zijn verantwoordelijk voor specifiek aan de cluster/directie gerelateerde kennis en implementatie van privacyvraagstukken. De concern-privacy officer is de linking-pin naar directies en clusters en verantwoordelijk voor de behandeling van organisatiebrede privacyvraagstukken en is verantwoordelijk voor het privacyproces. Verder heeft de concern-privacy officer volgens het privacybeleid een rol in de algemene kennisoverdracht met betrekking tot privacy en het signaleren en implementeren van organisatiebrede privacyvraagstukken.

De CISO is verantwoordelijk voor het informatiebeveiligingsproces binnen het concern. De DISO is gepositioneerd binnen een cluster en legt verantwoording af aan de CISO en de clusterdirectie. Samen houden de CISO en DISO toezicht op de informatiebeveiligingsmaatregelen die een cluster neemt om gegevens, waaronder persoonsgegevens, te beveiligen. De CISO en DISO werken hierbij nauw samen met de FG, concern-privacy officer en de privacy officers.

De derde lijn is het interne toezicht dat op grond van de AVG is belegd bij de FG. De FG valt in de organisatie onder de gemeentesecretaris. Hij heeft in deze gemeente toegang tot de gemeentesecretaris en de wethouder op het moment dat er 'iets geks' gebeurt en het niet wordt opgepakt. Bovendien, als de FG vindt dat iets 'niet door de beugel kan', dan benadrukt hij bij de desbetreffende persoon dat diegene de wethouder op de hoogte moet stellen. Als dat niet gebeurt, dan wijst de FG erop dat het dan op zijn weg ligt om dit alsnog te doen. De toegang tot de gemeentesecretaris en de wethouder en het druk uitoefenen om de wethouder te informeren zijn de enige mogelijkheden die de FG heeft om naleving af te dwingen. Hij heeft geen zogenoemde stopping power om te eisen dat bijvoorbeeld acuut een verwerking wordt beëindigd. Het is namelijk aan de verwerkingsverantwoordelijke om te beslissen wat er uiteindelijk wordt gedaan. Daarnaast doet de FG regelmatig zelf onderzoek. Deze onderzoeken hebben als achterliggend doel om bij de organisaties bewustzijn te creëren om deze aspecten ook zelf te controleren en, waar nodig, managementsystemen daarop aan te passen.

Binnen de tweede lijn en tussen de tweede en derde lijn vindt periodiek overleg plaats, zo komt naar voren uit de interviews. Om ervoor te zorgen dat alle privacy officers op hetzelfde

informatieniveau zitten, is er elke twee weken een privacy officers overleg. Daarnaast hebben de concern-privacy officer, de FG en de CISO een keer in de drie weken overleg.

5.8.3 Praktijk

De wijze waarop de FG, de concern-privacy officer en de concerndirecteur hun taak opvatten en daaraan invulling geven, vormen binnen deze gemeente een goede basis om op het vlak van privacyvolwassenheid tot een verdere groei te komen.

Binnen de *three lines of defence* vormen de lijnorganisatie, de privacy officers en de FG een driehoek die gezamenlijk, maar vanuit hun eigen rol komen tot een juiste uitvoering van de AVG. In de praktijk blijkt echter dat de eerste lijn wel wil, maar niet altijd weet wanneer of hoe ze moeten acteren. De tweede lijn ervaart onduidelijkheid over wat tweedelijns advisering precies inhoudt, waardoor de afstand tussen de eerste en tweede lijn groot is en ze niet als het ware naar elkaar worden toegezogen. Het aanwijzen van privacy-ambassadeurs en het werken met één projectverantwoordelijke zijn maatregelen die helpen deze ervaren problemen het hoofd te bieden.

Om privacybewustzijn te vergroten wordt gewerkt met basis e-learning modules en verdiepende modules voor bijvoorbeeld de ambassadeurs. Ook bestaan er plannen om een aantal mini-modules te maken ten aanzien van specifieke onderwerpen. Er bestaat al een dergelijke module voor de meldplicht datalekken, maar er wordt nu ook gekeken naar een mini-module voor inkoop. Bovendien wordt aan de hand van checklists en procesbeschrijvingen vastgelegd wanneer wie waarom moet aanhaken. Daarnaast bieden de rapporten en handhavingsacties van de AP voor de FG een podium om op specifieke onderwerpen het bewustzijn te vergroten. De aanwezigheid van ambassadeurs in organisatieonderdelen helpt om het bewustzijn te vergroten, omdat zij – indien zij over voldoende kennis beschikken – tijdig AVG-vraagstukken kunnen herkennen en bij het ontplooien van activiteiten kunnen betrekken.

Een DPIA wordt doorgaans uitgevoerd door de privacy officer, voorafgaand aan de verwerking en bij bestaande verwerkingen met een hoog risico. Bij het uitvoeren van een DPIA is het de wens dat iedereen bij elkaar komt om met elkaar de beste resultaten te bereiken. Zeker bij complexe verwerkingen, waaronder de inzet van algoritmes is het van belang dat de verschillende disciplines, waaronder security, privacy, informatiebeheer, data en ethiek, aan tafel zitten. In een enkel geval loopt dit goed en is er geleerd van eerdere ervaringen en is er het besef dat de totstandkoming van een DPIA en de beoordeling daarvan tijd vergt. Deze alertheid is nog niet in alle onderdelen van de organisatie aanwezig.

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens – dat online toegankelijk is – en de daarbij behorende verwerkersovereenkomst en het model Gegevensbeschermingseffectbeoordeling. Daarnaast houdt hij toezicht op het DPIA proces. De FG heeft een sturende rol. De eerste en tweede lijn weten waar hij op let en zorgen er ook voor dat in de DPIA's die aspecten goed worden uitgewerkt.

De gemeente heeft een Protocol Meldplicht en afhandeling van datalekken en een register om datalekken bij te houden. De individuele medewerker is verantwoordelijk voor het doen van de eerste melding. De DISO van het betreffende cluster is samen met de privacy officer verantwoordelijk voor het onderzoek naar een beveiligingsincident. De DISO is verantwoordelijk voor regie op het dichten van het lek en de privacy officer voor het oppakken ervan. Het

college is eindverantwoordelijk. Een datalek heeft altijd prioriteit bij een privacy officer en de FG. De gedane meldingen en het datalek zelf worden geëvalueerd en leiden, indien nodig, tot het treffen van maatregelen. De FG monitort de registratie van de datalekken en of de maatregelen ook daadwerkelijk zijn getroffen.

Dat de AVG een verwerking niet toelaat en de verwerking dus strijdig is met de AVG, hoeft niet te betekenen dat een beslissing niet wordt genomen. De tweede en de derde lijn zijn zich ervan bewust dat het niet aan hen is om daarover te beslissen. Dat is uiteindelijk een bestuurlijke aangelegenheid. Wel zorgen zij ervoor dat privacy als wegingsfactor in de uiteindelijke besluitvorming en de daaraan ten grondslag liggende belangenafweging wordt meegenomen. Indien blijkt dat aan bepaalde voorwaarden van de AVG niet kan worden voldaan, dan wordt een escalatieproces gehanteerd. De FG brengt in dat geval een advies uit, als dat niet wordt of kan worden opgevolgd, dan kan het geëscaleerd worden tot op het niveau van de concerndirectie.

5.8.4 Uitdagingen

Uit de interviews volgt dat de privacy officers beter in staat moeten worden gesteld om hun rol te pakken. Ook moet worden onderzocht hoe specifieke kennis kan worden verkregen en ingezet in de organisatie. De privacyvolwassenheid van de eerste lijn wisselvallig. Een concernbrede inzet om AVG automatisch als onderdeel van de taak te zien, is gewenst. Een verdere inbedding van het juist doorlopen van het DPIA-proces dient vanuit de eerste lijn prioriteit te krijgen. Dit begint met het onderkennen van het belang van het ‘nulgesprek’. Een dergelijk gesprek wordt gehouden nog voordat de verwerkingsactiviteit ontwikkeld wordt, waarbij de verschillende belangen, waaronder het voldoen aan de AVG, besproken worden. Dit vergt wel dat de juiste mensen op het juiste moment met elkaar dat gesprek aangaan. Een dergelijk nulgesprek is zeker van belang waar het gaat om de inzet van algoritmes. Lessons learned uit geslaagde projecten of projecten die anderszins leerzaam zijn geweest, kunnen helpen bij het verkrijgen van de relevante inzichten die behulpzaam zijn bij de ontwikkeling van een verwerkingsactiviteit.

5.8.5 Analyse

Er wordt structureel ingezet op scholing van medewerkers over het belang van naleving van de AVG. Hiervoor worden zowel algemene als meer toegesneden cursussen aangeboden. De inzet op dit vlak is een voortdurend punt van aandacht. Wel valt op dat de privacy officers, al dan niet vanwege gebrek aan capaciteit of onduidelijkheid in de taakopvatting, in onvoldoende mate in staat zijn hun adviesrol concernbreed op toereikende wijze vorm te geven. Dit kan de verdere groei van de privacyvolwassenheid van de eerste lijn in de weg zitten. Opvallend is dat de privacy-organisatie rapporten en boetebesluiten van de AP weet aan te wenden om aandacht te vragen voor specifieke vraagstukken en aandacht te vestigen op veranderingen in de processen die moeten worden doorgevoerd.

Binnen de gemeente wordt zeker bij grotere of complexe verwerkingen, waaronder de inzet van algoritmes, de privacycomponent als een van de aspecten gezien waar vroegtijdig aandacht aan moet worden besteed. Ook leeft het besef dat dit tijd kost, waarmee rekening moet worden gehouden in de planning. Daarbij is het behulpzaam dat het in de organisatie zeer helder is wat de FG belangrijk vindt en daarmee wat in de beoordeling van de verwerking moet worden meegenomen en wat wel of niet geaccepteerd wordt. Ook de aanwezigheid van ambassadeurs helpt hierbij. Aan de andere kant blijkt dat de AVG nog onvoldoende op het netvlies staat en dat de vaardigheden ontbreken om AVG-vraagstukken te herkennen en tijdig

onder de aandacht van de tweede en uiteindelijk derde lijn te brengen. Ook komt het voor dat verwerkingen of AVG-relateerde aspecten die niet door de beugel kunnen door de eerste lijn niet onder de aandacht van de bestuurder worden gebracht of dat bij projecten de privacyrisico's onvoldoende worden uitgelicht.

Binnen deze gemeente is er een groeiend besef dat de AVG integraal onderdeel is van de uitvoering van de wettelijke taken en bevoegdheden en wordt het voldoen aan de AVG ook belangrijk gevonden. Wanneer echter andere maatschappelijk belangen zwaarder wegen, kan het AVG-belang het onderspit delven. Ook in die gevallen wordt vervolgens getracht om voldoende waarborgen te treffen die in lijn zijn met de AVG.

Vanuit de gemeenteraad worden met regelmaat AVG-kwesties geagendeerd en dat vormt vaak een trigger om over bepaalde privacy-aspecten na te denken. Het helpt vervolgens de tweede lijn om de organisatie in beweging te krijgen. De maatschappelijke ontwikkelingen die aldus worden geagendeerd kunnen gesprekspartners helpen om binnen de organisatie het verhaal meer te laten landen. De concern-privacy officer gebruikt dit als kapstok om privacy op de kaart te krijgen. Omgekeerd geldt dat als een bepaald thema voor de raadsvergadering wordt geagendeerd en aan bepaalde vraagstukken privacy-aspecten kleven de concern-privacy officer hier doorgaans van op de hoogte wordt gesteld. Indien deze functionaris AVG-technische complicaties ziet, geeft deze geen akkoord. Deze escalatie kan ertoe leiden dat onder druk AVG-technische complicaties alsnog worden weggenomen om een thema tijdig op de agenda te krijgen.

Toezicht en handhaving vindt vooral plaats door middel van intern toezicht. Dit betekent niet dat de AP op de achtergrond geen rol speelt. Er wordt, indien noodzakelijk, met de toezichthouder contact gezocht.

5.9 Caseverslag gemeente 2

Deze casestudybeschrijving doet verslag van het onderzoek naar de naleving van de AVG in een middelgrote gemeente met iets minder dan 100.000 inwoners en een ambtelijke organisatie met ruim 600 werknemers. Binnen de gemeente worden veel gegevens verwerkt van inwoners. Dat gebeurt bijvoorbeeld door het raadplegen van de Basisregistratie Personen (BRP) bij de uitgifte van paspoorten en rijbewijzen, bij het verlenen van omgevingsvergunningen, alcoholvergunningen en evenementenvergunningen. Het zwaartepunt van gegevensverwerking binnen de organisatie ligt binnen het sociaal domein. Daar wordt nogal eens wordt geworsteld met soms conflicterende belangen bij de naleving van de AVG. Van grootschalige datalekken of calamiteiten is de afgelopen jaren geen sprake geweest.

5.9.1 Beleid

Het privacybeleid is neergelegd in het Privacybeleid 2020 – 2024. De gemeente heeft in het huidige privacybeleid de bewuste keuze gemaakt om meer in te zetten op risico gestuurd toezicht. De gedachte die daaraan ten grondslag ligt is dat voor het vaststellen van risico's een objectieve beoordeling nodig is. Er dient gekeken te worden naar de waarschijnlijkheid dat zich iets ernstig zich voordoet. Het risico wordt bepaald door zowel de kans op als de impact van bepaalde negatieve gevolgen van fouten. Een grote kans op een kleine impact kan dus resulteren in een risico met score 'midden'. Tegelijk kan een zeer kleine kans op een groot

risico ook resulteren in score 'midden'. De risico-inschatting wordt gemaakt met medewerkers die nauw bij het nieuwe project, de beleidsontwikkeling of het proces betrokken zijn.

In het kader van deze casestudy is gesproken met de privacy officer, de FG, de manager bedrijfsvoering en een teamleider Sociaal Domein. Het privacybeleid van de gemeente is bestudeerd.

5.9.2 Organisatie-inrichting

De privacy-organisatie is ingericht op basis van het *three lines of defence*-model. De derde lijn wordt ingevuld door de FG. Hij bekleedt een zelfstandige positie binnen de organisatie en is met een aantal taken belast. Zo informeert en adviseert hij over de werking van de AVG, overige wetgeving en het gemeentelijke privacybeleid, houdt toezicht op naleving van het privacybeleid, vervult een ombudsfunctie bij privacygerelateerde klachten, adviseert bij privacy-incidenten binnen de organisatie, hij ziet toe op het beheer het register van verwerkingen (artikel 30 AVG). Hij helpt het privacybeleid uit te dragen en bewustzijn te creëren en hij is het contactpunt voor de landelijke toezichthouders, waaronder de AP. De tweede lijn wordt gevormd door de privacy officer en het PIT. De privacy officer is de verbindende schakel tussen de organisatie en de FG. Hij/zij ondersteunt vanuit de tweede lijn bij vraagstukken omtrent de bescherming van persoonsgegevens. Het PIT is een overlegorgaan waaraan functionarissen op het gebied van privacy en informatiebeveiliging vertegenwoordigd zijn. Dit team overlegt periodiek en op afroepbasis als daar aanleiding toe is.

5.9.3 Praktijk

De gemeente probeert door middel van opleiding en training het privacybewustzijn binnen de organisatie te versterken. Het maken van de vertaalslag van de juridische werkelijkheid van de AVG naar de praktische realiteit op de werkvloer is een lastige opgave die bovendien nog onvoldoende geborgd is binnen de organisatie. Dat heeft onder meer te maken met de beperkte tijd die de privacy officer heeft aangezien zij de gehele organisatie moet bedienen. Een belangrijke uitdaging die wordt gevoeld is de toon waarop het 'AVG verhaal' wordt verspreid binnen de organisatie. Momenteel wordt privacy vaak nog als iets extra's en belastend gezien binnen eigen werkprocessen, niet als een waarde of belang dat behartigd moet worden omdat deze kunnen botsen met andere belangen. Dat speelt bijvoorbeeld binnen het sociaal domein privacybelangen en spoedeisende (cliënt)belangen nogal eens lijken te kunnen botsen. Daarover uitleg geven op de juiste toon is nodig om het belang van privacy te verinnerlijken bij de medewerkers. Het PIT zou hier volgens gesprekspartners ook een nadrukkelijker rol in kunnen nemen, die is vaak nog te passief en meer gericht op audits en beoordelingen achteraf.

Het uitvoeren van de DPIA's wordt gebruikt ter inventarisatie van risico's bij het verwerken van persoonsgegevens. Een compleet overzicht van processen waar een DPIA moet worden uitgevoerd is er niet. Idealiter beslist de proceseigenaar of een DPIA nodig is, maar in de praktijk is het momenteel vooral de privacy officer die daartoe adviseert of het initiatief neemt. Als de lijnmanager al dan niet onbewust nalaat aan te geven dat een DPIA moet worden uitgevoerd, blijft dit buiten beeld. Ook komt het nog voor dat er geen DPIA is uitgevoerd, terwijl achteraf blijkt dat dit wel had gemoeten. De praktijk is daardoor nog niet in overeenstemming met het beleid.

Alle gemelde datalekken en wijze van afhandeling, worden in een register bijgehouden. De procedure die moet worden gevolgd is voor medewerkers te vinden op het intranet. Er is een meldformulier die medewerkers hiervoor kunnen gebruiken. De privacy officer neemt

vervolgens contact op met de melder en beoordeelt of het datalek dermate ernstig dat hiervan melding moet worden gedaan bij de AP. De handelswijze wordt achteraf wel altijd besproken in het PIT. De meldingsbereidheid van medewerkers fluctueert, zo is de ervaring. Over het algemeen durven medewerkers een datalek dat zijzelf veroorzaakt hebben wel te melden bij de privacy officer. Er wordt bewust aan gewerkt om de drempel te verlagen om een datalek te melden. Dat wordt gedaan door actief duidelijk te maken binnen de organisatie dat er in principe niet bestraffend opgetreden zal worden bij een datalek.

Vanuit management komt steeds meer steun en aandacht voor het belang van naleving van de AVG. De nieuwe gemeentesecretaris heeft daar een belangrijke impuls aan gegeven. Toch voelt het voor de privacy officer nog steeds als een strijd die gevoerd moet worden binnen de organisatie om medewerkers te doordringen van het belang van naleving van de AVG. Dat kost veel energie. De steun vanuit het management is er, maar zou nog sterker benadrukt kunnen worden. Het management zelf worstelt met de opgave de privacybelangen op de juiste wijze te vertalen binnen de organisatie.

5.9.4 Uitdagingen

De belangrijkste uitdagingen van de organisatie is om de ambities die de gemeente heeft op het gebied van privacy op concrete wijze handen en voeten te geven in de organisatie. Zo krijgen de periodieke rapportages van FG serieuze aandacht in het MT en is hun steun en gevoelde urgentie zeker aanwezig en groeiende. Hoe die steun en urgentie vervolgens te vertalen in operationele acties, procedures en werkwijzen blijkt echter lastig. Daar komt bij dat de beperkte capaciteit van de ondersteuning voor de primaire afdelingen in de vorm van de privacy officer beperkt is, terwijl die een cruciale rol kan spelen in het maken van de vertaalslag van ambitie naar praktijk. Met de beschikbare tijd en middelen worden de ambities dus mogelijk niet waargemaakt.

5.9.5 Analyse

Er zijn verschillende factoren die de mate van naleving binnen deze gemeente kunnen verklaren. Zo draagt de kennis van regels bij aan de naleving van de AVG. Daar wordt aan gewerkt middels trainingen, e-learnings en door organisatiebrede inspanningen van privacy officer. Het privacybewustzijn neemt toe, maar is geen eenvoudige opgave. Het wel of niet naleven kan in bepaalde gevallen worden verklaard in termen van een kosten-baten analyse. Wanneer naleving veel tijd kost en de kosten daarvan in de ogen van een medewerker daar niet tegen opwegen tegen de baten leidt dat tot niet-naleving. Dat mechanisme kan bijvoorbeeld optreden bij het al dan niet uitvoeren van een DPIA. De mate van acceptatie van de regel beïnvloedt eveneens het nalevingsgedrag. Wanneer bijvoorbeeld binnen het sociaal domein de belangen van de inwoner/cliënt botsen met het belang van naleving van de AVG kan dat in de praktijk tot gevolg hebben dat er ‘losjes’ met de bepalingen uit de AVG wordt omgegaan omdat men vindt dat in bepaalde situaties het belang van de inwoner/cliënt prevaleert door bijvoorbeeld onrechtmatig gegevens toch te delen.

5.10 Caseverslag gemeente 3

Deze casestudy betreft een kleine gemeente die te maken heeft gehad met een incident op het gebied van informatiebeveiliging, waarbij potentieel gegevens van medewerkers en inwoners zijn gelekt. De gemeente is een belangrijke verwerker van persoonsgegevens. Het zwaartepunt van de gemeentelijke gegevensverwerking ligt in het sociaal domein. De gemeente is

ten slotte ook een werkgever met meer dan 200 werknemers, waarvan ook gegevens worden verwerkt.

In de casestudy is gesproken met de directeur, een concern-controller, de FG en een juridisch medewerker. De juridisch medewerker was lid van de kerngroep AVG. Deze kerngroep is belast met de monitoring van de kwaliteit van de privacybescherming binnen de gemeente. De gemeente heeft een document over de privacy-governance, het privacybeleid en een viertal rapportages met betrekking tot het beveiligingsincident verstrekt.

5.10.1 Beleid

In 2019 heeft de gemeente het privacybeleid vastgesteld. In dit document is beschreven hoe werkprocessen worden georganiseerd conform de AVG, wordt in grote lijnen de privacy-organisatie beschreven, wordt het juridisch kader voor verwerking van persoonsgegevens beschreven, worden rechten van betrokkenen en de omgang met de uitoefening daarvan beschreven. Ook wordt er ingegaan op algemeen te verwachten zaken zoals het verwerkingsregister, informatiebeveiliging, bewaartermijnen en de omgang met datalekken.

5.10.2 Organisatie-inrichting

In het governancedocument is vastgelegd dat de bestuurlijke en ambtelijke verantwoordelijkheid respectievelijk bij het college van B&W en bij de gemeentesecretaris liggen. Ook is vastgelegd dat de afdelingsmanagers als eigenaren van de persoonsgegevens verantwoordelijk zijn voor integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens.

Naast de lijnorganisatie is een aantal specifieke privacyfunctionarissen beschreven. De FG heeft een rol op de achtergrond: hij adviseert en informeert omtrent gegevensverwerking, en ziet toe op naleving van de AVG en gerelateerde wet- en regelgeving. De CISO is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid en het coördineren van de uitvoering van het beleid. De rol van privacy officer is gericht op de uitvoering en de naleving van de privacywetgeving, waarbij hij adviseert over privacybescherming, vaak vanuit een juridische invalshoek. Binnen de gemeente is een kerngroep AVG in het leven geroepen.

In het governancedocument is verder vastgelegd hoe verantwoordelijkheden met betrekking tot privacy zijn belegd. Zo is voor verschillende taken steeds aangegeven wie verantwoordelijk is voor de deeltaken die daaronder vallen. Hier valt op dat het nogal eens voorkomt dat (deel)taken bij verschillende partijen belegd zijn, zonder dat verder gespecificeerd wordt welke functionaris in welke situatie verantwoordelijk is. In de praktijk heeft de FG ook wel meegeschreven aan beleidsstukken op het gebied van privacy en is aangegeven dat de FG en de CPO veel samenwerken en daarbij soms pragmatisch taken verdelen. De kerngroep AVG is door natuurlijk verloop na verloop van tijd leeggelopen en bestaat nu alleen nog uit de FG en CPO.

De FG heeft (samen met de privacy officer) de mogelijkheid om het managementteam (MT) te adviseren. Het is geen uitzondering dat een advies van de FG niet volledig of niet direct wordt opgevolgd. Dat heeft er wel eens toe geleid dat er een hernieuwd advies vanuit de FG aan het MT is gericht.

5.10.3 Praktijk

Met name vlak na de inwerkingtreding van de AVG is in de hele gemeente veel aandacht besteed aan de AVG. Dit is in de jaren daarna iets afgenomen. Er is een training ontwikkeld voor nieuwe medewerkers en ook in herhaalcursussen wordt aandacht geschonken aan de AVG.

Direct na het beveiligingsincident is het bewustzijn in de organisatie met name ten aanzien van de technische aspecten van gegevensbeveiliging aanzienlijk toegenomen. Medewerkers werden zich veel bewuster van wat hun verantwoordelijkheden waren en wat de risico's waren van onvoorzichtige gedragingen. Toch is dit niveau van bewustzijn na verloop tijd ook iets gedaald. Daarnaast is geconstateerd dat de naleving van de AVG in brede zin door een groot deel van de organisatie los wordt gezien van de noodzaak van beveiliging van gegevens en systemen.

Voor DPIA's, verwerkersovereenkomsten en de afhandeling van datalekken is vastgelegd dat het afdelings- en teammanagement primair verantwoordelijk is voor de coördinatie, uitvoering, opstellen en afhandelen van zaken. De FG en privacy officer ondersteunen en adviseren, eventueel ook (indien een IT-voorziening onderdeel is van het nieuwe proces) samen met de CISO.

Bij de bestudeerde gemeente heeft zich een beveiligingsincident voorgedaan waarbij potentieel sprake was van het grootschalig lekken van persoonsgegevens. Naar aanleiding hiervan is het bewustzijn bij medewerkers door verschillende maatregelen aanzienlijk vergroot. Ten aanzien van het nadenken over gegevensbescherming zijn minder grote stappen gemaakt.

In het beleid is het interne toezicht conform de AVG vastgelegd in de functie van de FG. Het externe toezicht wordt gedaan door de AP. Voor deze grootschalige lekken is gebleken dat het contact met de AP niet naar tevredenheid is verlopen. Het meldingsproces bleek niet goed ingericht op de grootschaligheid van het (mogelijke) lek.

5.10.4 Uitdagingen

De privacy-organisatie is op een aantal punten nog niet optimaal ingericht of ingebed. Zo wordt de FG nog te weinig als adviseur en sparring partner ingezet, maar meer als toezichthouder achteraf. Er is een kerngroep AVG ingesteld, maar inmiddels is deze om praktische redenen niet meer actief, terwijl er wel officieel verantwoordelijkheden zijn belegd. Hierdoor vallen extra taken op de schouders van de FG en de privacy officer, wat een smalle basis is. Een laatste punt betreft de afhankelijkheid van de FG van het MT. De adviezen worden door het MT niet altijd overgenomen, maar er worden meer subjectieve afwegingen gemaakt waardoor privacy-aspecten minder hoge prioriteit kunnen krijgen onder druk van werkprocessen of de roep om doelmatigheid.

5.10.5 Analyse

Het beveiligingsincident heeft een behoorlijke indruk gemaakt op de organisatie. Inmiddels is het bewustzijn groot ten aanzien van de technische beveiliging van toegang tot gegevens en het bestrijden van risico's op lekken. Toch staat de gemeente onder grote druk om met beperkte middelen een groot takenpakket uit te voeren. Daarmee bestaat een prikkel om doelmatig te werken en te focussen op het doelmatig opzetten en uitvoeren van werkprocessen. Er ontstaat daardoor een prikkel om AVG-aspecten geen voorrang te geven. Adviezen vanuit de FG aan het MT worden niet altijd direct opgevolgd. Dit alles wil niet zeggen dat men niet doordrongen is van het belang van naleving van de AVG. Die wordt zonder meer

onderschreven. Door tijdsdruk kan de prioritering van werkzaamheden echter wel richting primaire processen verschuiven. Privacy-aspecten worden daardoor niet altijd als integraal onderdeel van het opzetten van processen gezien.

6 Vergelijkende Analyse

6.1 Inleiding

In dit hoofdstuk vergelijken we de bevindingen uit de negen casestudy's. Door de cases met elkaar te vergelijken bouwen we een beschrijving en verklaring op van de naleving van de AVG bij de bestudeerde overheidsorganisaties. Het in paragraaf 2.2 geschetste kader gebruiken we daarbij als kapstok. De dimensies van spontane naleving en de drieslag 'weten, willen en kunnen' indachtig, letten we daarbij onder meer op beleid en organisatie (par. 6.3 en 6.4), kennis en bewustzijn (par. 6.5) en het gebruik van het AVG-instrumentarium, zoals de meldplicht datalekken en de werkwijze die daarbij wordt gevolgd, het gebruik van het verwerkingsregister en het uitvoeren van DPIA's (par. 6.6). De negen overheidsorganisaties zijn op basis van diverse kenmerken geselecteerd met het oog op het bereiken van een spreiding over de totale populatie overheidsorganisaties. Daarmee is geen representativiteit bereikt, maar hebben we wel een dwarsdoorsnede van de Nederlandse overheid kunnen bekijken. Op basis daarvan kunnen uitspraken gedaan worden over de naleving van de AVG met meer algemene geldigheid, zonder dat de pretentie kan bestaan dat daarmee de totale variatie in beeld is gebracht. Door een vergelijking te maken tussen de negen cases en te zoeken naar overeenkomsten en verschillen kunnen we wel een beeld geven van een aantal belangrijke onderwerpen die spelen bij de naleving van de AVG. Op basis daarvan is het mogelijk tot een overzicht van knelpunten en verbeterpunten te komen, zonder de pretentie van volledigheid.

Dit hoofdstuk is als volgt opgebouwd. Allereerst staan we in paragraaf 6.2 stil bij de negen casestudy's, de algemene kenmerken van de overheidsorganisaties en de verschillen en overeenkomsten daartussen. Daarna beschrijven we in paragraaf 6.3 het door de overheidsorganisaties vastgestelde beleid over de bescherming van persoonsgegevens. In paragraaf 6.4 staat de organisatie-inrichting centraal die bij de overheden is gekozen voor de privacy-organisatie. Paragraaf 6.5 concentreert zich op wat de overheden doen aan het vergroten en bestendigen van kennis en bewustzijn van de regels over de bescherming van persoonsgegevens en in paragraaf 6.6 komen de instrumenten van de AVG, zoals de DPIA en de meldplicht datalekken, aan de orde en de wijze waarop overheden daarmee werken. In paragraaf 6.7 staan we stil bij de knelpunten en verbeterpunten als het gaat om de naleving van de AVG door overheden, ook benoemen we in die paragraaf een aantal *good p*ractices. Het hoofdstuk besluit in 6.8 met een korte conclusie.

6.2 De cases

Voor het onderzoek selecteerden we overheidsorganisaties die werkzaamheden verrichten op verschillende niveaus binnen de gedecentraliseerde eenheidsstaat. We voerden onderzoek uit op een departement, bij vier uitvoeringsorganisaties, drie gemeenten en een waterschap. Daarmee hebben we in ieder geval een deelselectie gemaakt van overheidsorganisaties die variëren op belangrijke kenmerken. We kozen niet voor een provinciale organisatie omdat we op voorhand veronderstelden dat die relatief weinig werken met (bijzondere) persoonsgegevens. Dat geldt ook voor het waterschap dat we selecteerden, dus van de keuze van een provincie verwachtten we daarnaast weinig toegevoegde waarde. De uitvoeringsorganisaties werken alle vier op landelijk niveau. Ze verschillen op ten minste drie kenmerken van elkaar: schaal, beleidsterrein en relatie met het departement. We selecteerden een kleine uitvoeringsorganisatie, een grote organisatie met bijna 3.000 medewerkers en twee middelgrote met ca. 1.500 medewerkers. Schaal lijkt niet onbelangrijk te zijn voor de manier waarop de AVG wordt nageleefd. Aan de ene kant omdat de privacy-organisatie bij een kleinere organisatie herkenbaarder is en functionarissen met een bepaald takenpakket daarbinnen gemakkelijker gevonden lijken te worden. Aan de andere kant heeft een grotere organisatie in personele zin meer mogelijkheden om gekwalificeerde medewerkers aan te trekken en aan zich te binden, en dat blijkt voor de naleving van de AVG van belang te zijn zoals we verderop zullen zien. Drie van de uitvoeringsorganisaties zijn zelfstandige bestuursorganen. Voor de bescherming van persoonsgegevens betekent dit dat ze volledig zelf verantwoordelijk zijn voor de inrichting van hun privacy-organisatie en dat er op dat punt geen relatie met het departement is. Bij de uitvoeringsorganisaties die gelieerd zijn aan een moederdepartement is de FG op het departement gestationeerd. Dat geeft andere verhoudingen, waarop we hierna terugkomen. Tot slot hebben we de uitvoeringsorganisaties op verschillende beleidsdomeinen geselecteerd. We zien niet direct een verband tussen kenmerken van het beleidsterrein enerzijds en de naleving van de AVG anderzijds. Wel maakt het type werkzaamheden uit, zoals we hierna verder uitwerken. In het casestudy-onderzoek lijken de overheidsorganisaties die werken met bijzondere persoonsgegevens zich sterker bewust te zijn van het belang van de AVG. Deze organisaties hebben steeds een goed uitgewerkte privacy-organisatie ingericht. Een andere bevinding in het onderzoek is dat *the tone at the top* van belang is en mogelijk van grotere invloed dan de inrichting van de privacy-organisatie op de wijze waarop bij de uitvoering in de eerste lijn van de organisatie de AVG wordt nageleefd. Daarbij gaat het om de wijze waarop in de besluitvorming rekening wordt gehouden met de AVG, om de wijze waarop door bestuur en management over de AVG wordt gesproken en over het gedrag van de top van de organisatie als het gaat om AVG-compliance.

We selecteerden drie gemeenten in verschillende groottecategorieën: een van de grote steden, een 100.000+ gemeente en een gemeente van 35.000 inwoners. Ook hier zien we verschillen die met schaal te maken hebben. De casestudy van een kleinere gemeente bevestigt het beeld dat kleinere gemeenten meer moeite hebben goed gekwalificeerde medewerkers aan te trekken en vast te houden.[84] Net als op andere terreinen worden door kleinere gemeenten FG's en privacy officers vaker extern ingehuurd. Gemeenten verschillen van de andere organisaties door de intensieve wijze waarop ze persoonsgegevens en ook bijzondere persoonsgegevens van inwoners verwerken. Daarbij gaat het met name om de taken die gemeenten op het sociaal domein uitvoeren. Opvallend is dat daarbij ook – meer en intensiever dan bij andere overheidsorganisaties – sprake is van samenwerking en dus gegevensdeling

[84] Op basis van de Personeelsmonitor gemeenten 2021, uitgevoerd door het A&O fonds Gemeenten, zie: https://www.binnenlandsbestuur.nl/carriere/kleinere-gemeenten-ontberen-personeel

met andere organisaties (denk aan zorgpartijen, onderwijs en andere gemeenten), maar ook met verschillende andere onderdelen binnen de gemeentelijke organisatie (denk aan openbare orde en veiligheid).

In paragraaf 6.8 staan we stil bij het onderscheid tussen de uitvoeringsorganisaties enerzijds en de gemeenten en het departement anderzijds. Dat onderscheid, hoe grofmazig ook, kan getypeerd worden als het onderscheid tussen meer technische uitvoering enerzijds en meer politieke beleidsvorming anderzijds. Uitvoeringsorganisaties die in de dagelijkse werkzaamheden minder direct met politiek-bestuurlijke afwegingen te maken hebben, richten zich sterker op de kwaliteit van de uitvoering en zijn meer bezig met de randvoorwaarden die daarbij van belang zijn. De bescherming van persoonsgegevens is zo'n randvoorwaarde en het belang dat daaraan werd gehecht zagen we bij verschillende uitvoeringsorganisaties duidelijk terug. Bij ministeries en gemeenten troffen we een andere situatie aan. Daar staan politiek-bestuurlijke afwegingen meer centraal. Het lijkt er dan op dat de bescherming van persoonsgegevens eerder onderdeel wordt van een belangenafweging en daardoor een minder prominente plaats krijgt.

6.3 Beleid

Alle organisaties die we bestudeerden hebben expliciet vastgesteld beleid voor de bescherming van persoonsgegevens. Vaak zijn ter uitwerking van dat beleid werkinstructies of andere nadere regels, of zelfs een privacyhandboek, opgesteld. Enkele van de overheidsorganisaties zijn ISO-gecertificeerd; in dat verband is er sprake van externe audits. Veelal zijn in het beleid uitgangspunten neergelegd voor de wijze waarop de organisatie de AVG implementeert en worden op strategisch, tactisch en operationeel niveau de taken en rollen op het vlak van de bescherming van privacy in de organisatie toegedeeld. De beleidsstukken die we hebben bezien zijn over het algemeen actueel en gelden voor een in de tijd afgebakende periode. In een enkel geval waar die periode is afgelopen of binnenkort afloopt was sprake van een lopende of binnenkort komende actualisatieslag.

In de beleidsstukken en de uitwerking daarvan in nadere documenten is er veelal aandacht voor het verwerkingsregister, het uitvoeren van DPIA's, de informatiebeveiliging, de rechten van betrokkenen, de bewaartermijnen en de omgang met datalekken. Soms kennen organisaties richtlijnen voor het omgaan met e-mails. Ook is er in de documenten meestal aandacht voor het juridische kader dat geldt voor de omgang met persoonsgegevens.

Soms zijn het privacybeleid – over de inhoudelijke kant van de bescherming van persoonsgegevens – en de privacygovernance – over de organisatorische inrichting van de zorg voor privacy – neergelegd in afzonderlijke beleidsstukken, meestal staat informatie over die onderwerpen allemaal in een document.

De uitvoeringsorganisatie die onderdeel is van het departement werkt met het door het departement vastgestelde beleid.

6.4 Organisatie

De inrichting van de privacy-organisatie van alle bestudeerde organisaties komt in feite steeds neer op het *three lines of defence*-model. Ook tijdens de expertmeeting was er consensus dat dit model zich in de praktijk ook op het vlak van privacy heeft bewezen. Vaak is dit model redelijk uitgewerkt in het beleid en wordt die term ook expliciet gebruikt. Soms is de organisatie-inrichting van de bescherming van persoonsgegevens minder expliciet op schrift gesteld, maar wordt in de praktijk van de organisatie op hoofdlijnen die indeling in drie niveaus wel gevolgd. We hebben bij enkele organisaties gezien dat het soms lastig is om de posities op elk van de drie niveaus van de privacy-organisatie in te vullen vanwege de krapte op de arbeidsmarkt. Dan improviseren de organisaties en is de invulling van de functies wat minder rolvast. We zien enkele keren een vermenging van de derde en de tweede lijn in die zin dat de FG ook taken van de privacy officer uitvoert. Dat is strijdig met de bedoeling van de AVG en met de onafhankelijke positie van de FG.

Volgens de AVG is het bestuur van de organisatie de verwerkingsverantwoordelijke. Die AVG-verantwoordelijkheden zijn gemandateerd in de lijnorganisatie, waarbij in de praktijk afdelingsmanagers en medewerkers binnen die afdelingen de taak hebben de AVG in de praktijk toe te passen en bij de invulling van hun taak en bij de uitoefening van bevoegdheden de AVG in acht te nemen. Verschillende organisaties kennen in de eerste lijn, vaak per afdeling of ander organisatieonderdeel, een contactpersoon, een taakaccenthouder of een andere functionaris die fungeert als aanspreekpunt en vraagbaak en die risico's signaleert en bewustzijn creëert.

De tweede lijn bestaat uit de privacy officer en de CPO die om advies kunnen worden gevraagd door de eerste lijn en die ondersteunende werkzaamheden verrichten, bijvoorbeeld bij het uitvoeren van DPIA's, een taak die in beginsel in de eerste lijn wordt uitgevoerd. Privacy officers en CPO's zijn ook verantwoordelijk voor het formuleren van het privacybeleid. Soms vervult de afdeling juridische zaken deze rol. Verder zijn in de tweede lijn de security officer en de CIO te vinden, die verantwoordelijk zijn voor het informatievoorzienings- en digitaliseringsbeleid en het beheer van de informatiesystemen. De invalshoek daarbij is vooral de informatiebeveiliging. Het *three lines of defence*-model geeft in de tweede lijn dus zowel aandacht aan informatiebeveiliging (technisch) als aan de bescherming van persoonsgegevens (inhoudelijk). Dit sluit aan bij de verplichtingen van de verwerkingsverantwoordelijke om technische en organisatorische maatregelen te treffen om aan de AVG te voldoen.

De derde lijn bestaat uit de FG die toeziet op de wijze waarop de eerste en tweede lijn invulling geven aan hun verantwoordelijkheden. Bij uitvoeringsorganisaties die vallen onder een moederdepartement is de minister de verwerkingsverantwoordelijke en houdt de FG op het departement toezicht op de verwerkingen in dat kader, dus ook voor de verwerkingen door de uitvoeringsorganisatie. Dat betekent dat de FG nog steeds de derde lijn is, maar dat er een zekere afstand is tot de uitvoeringsorganisatie. In die gevallen is de tweede lijn wat steviger georganiseerd. Kritiek die in dat verband wel is opgetekend is dat door die afstand de FG niet goed weet wat er speelt binnen de uitvoeringsorganisatie. Goede overlegstructuren en open communicatie tussen tweede en derde lijn zijn dus van groot belang in deze situaties.

In een tweetal overheidsorganisaties die we bestudeerden werd de FG op inhuurbasis door de organisatie ingeschakeld. In een van deze gevallen hing dat samen met de nadruk die de organisatie legde op het onafhankelijke functioneren van de FG, dat door externe inhuur beter gewaarborgd zou zijn. In een ander geval speelden vooral wervingsproblemen een rol.

6.5 Kennis en bewustzijn

In de casestudy's valt de grote aandacht voor kennisontwikkeling en het belang van houding en gedrag sterk op. In elke organisatie worden cursussen en trainingen verzorgd om het kennisniveau en het privacybewustzijn te vergroten. In vrijwel alle organisaties wordt gewerkt met e-learning modules en verdiepende modules. In een van de kleinere organisaties is het voor alle medewerkers verplicht daaraan deel te nemen en een certificaat te halen. Sommige organisaties verzorgen verdiepende modules voor de medewerkers in de eerste lijn die aanspreekpunt of contactpersoon zijn. Tijdens de expertmeeting werd opgemerkt dat niet te snel moet worden aangenomen dat het vergroten van kennis binnen organisaties direct leidt tot een sterker bewustzijn van het belang van privacy. Kennis van het onderwerp is weliswaar een belangrijke voorwaarde voor het creëren van bewustzijn, maar ook slechts een eerste stap. Verschillende organisaties werken met prikkels om het bewustzijn te stimuleren in de vorm van 'nep-phishing' berichten. Ook wordt in een aantal organisaties structureel aandacht geschonken aan naleving van de AVG tijdens reguliere overleggen.

Behalve kennis en bewustzijn moeten bij de naleving van de AVG houding en gedrag worden onderscheiden. Uiteraard is er geen directe causale relatie tussen beide: kennis en bewustzijn kunnen houding en gedrag wel beïnvloeden, maar de AVG-normconformiteit van het handelen van medewerkers wordt door meer variabelen beïnvloed. In de casestudy's worden in dat verband tijdsdruk en de dominantie van beleidsdoelen genoemd als verstorende factoren. 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.

De mate waarin de FG's bij de bestudeerde organisaties zich actief bezighouden met het vergroten van privacybewustzijn loopt nogal uiteen. Dat heeft ook veel te maken met de vaak parttime invulling van de functie en het van buitenaf betrekken van een FG. Bij organisaties met een fulltime FG is deze vaak actief, ook bij het vergroten van bewustzijn in de organisatie. In die organisaties lukt het de FG veelal ook om een stempel te drukken op wat de FG belangrijk vindt in een DPIA of aan welke specifieke onderwerpen binnen de organisatie extra aandacht moet worden gegeven. Op de werkvloer weet men dat en houdt men daar dan ook expliciet rekening mee. Parttime aangestelde FG's en FG's van buiten hebben het op dit punt aanmerkelijk lastiger, ook omdat ze minder goed in staat zijn de AVG-naleving op dagelijkse basis in de gaten te houden.

Er is in het algemeen relatief veel aandacht bij bestuur en management voor het belang van privacy en de naleving van de AVG. De geïnterviewden zien op dat punt ook een positieve ontwikkeling. Duidelijk is dat een enkele persoon in het bestuur of de directie met affiniteit met het onderwerp, die het belang daarvan onderstreept veel verschil kan maken. We zien dat de AVG-verantwoordelijkheid ook binnen het hogere management expliciet wordt belegd, bijvoorbeeld bij een concerndirecteur of een plaatsvervangend SG. Er is bij de meeste organisaties sprake van periodieke rapportage aan bestuur en management. Een enkele keer blijken vervolgacties die uit rapportages voort zouden moeten vloeien nog wel eens achterwege te blijven.

De gesprekspartners zien een ontwikkeling waarbij het belang van privacy bij de gemiddelde medewerker van de organisatie steeds meer op het netvlies staat, maar sommigen beschrijven

het tussen de oren krijgen van het belang van naleving van de AVG toch ook als een 'strijd' die veel energie kost. Het versterken van privacybewustzijn wordt gezien als een lastige opgave die veel tijd kost, die soms maar beperkt beschikbaar is. Bij enkele organisaties wordt het privacybewustzijn als 'relatief laag' getypeerd; andere organisaties doen het volgens de geïnterviewden mogelijk beter. In het algemeen lijken de meer eenvoudige AVG-verplichtingen, zoals de meldplicht, aardig tussen de oren te zitten, maar komt het doorvertalen van de AVG in het beleid nog onvoldoende tot wasdom. Niet altijd worden AVG-vragen en uitdagingen door de eerste lijn herkend, of dat gebeurt vaak pas laat in het proces. De experts die we spraken wijzen er in lijn hiermee op dat vaak de vraag of een bepaalde gegevensverwerking überhaupt noodzakelijk of wenselijk is niet wordt gesteld. Daardoor is het uitgangspunt van *privacy by design* doorgaans niet te realiseren.

In enkele casestudy's wordt in de organisatie een verschil geconstateerd tussen het belang van technische beveiligingsmaatregelen en bewustzijn enerzijds en het belang van naleving van de AVG en het nalevingsgedrag dat daarbij hoort anderzijds. In reactie op incidenten die zich hebben voorgedaan richt de aandacht in de bestudeerde organisaties zich soms sterk op de (meer technische) informatiebeveiligingskant. De kennis van de AVG kan in scholingsprogramma's prioriteit hebben gekregen, maar dat betekent niet dat de naleving van de AVG dan ook meteen als prioriteit wordt gezien.

6.6 AVG-instrumenten

De verantwoordelijkheid voor het uitvoeren van DPIA's ligt bij de eerste lijn. De privacy officers adviseren en ondersteunen, maar dat doen ze alleen op verzoek of wanneer ze – soms min of meer toevallig – op de hoogte raken van de noodzaak om een DPIA op te stellen. Dat betekent dat niet altijd wanneer dat zou moeten een DPIA wordt uitgevoerd. Hier ligt uiteraard een duidelijke relatie met privacybewustzijn, maar meer nog met houding en gedrag. Soms wordt de taak van het uitvoeren van een DPIA door een multidisciplinair team uitgevoerd. Een enkele keer stapt de privacy officer uit de adviserende rol en wordt de verantwoordelijkheid voor het uitvoeren van een impact assessment overgenomen – afhankelijk van de capaciteit en vaardigheid die in de eerste lijn te vinden is. Ook tijdens de expertmeeting is opgemerkt dat de eerste lijn niet altijd voldoende kennis heeft om kwalitatief goede DPIA's uit te voeren. Daarmee ontstaat dan een prikkel om mensen met meer expertise zoals privacy officers in te zetten, terwijl die daarmee eigenlijk buiten hun rol in de privacy-organisatie stappen. In een enkele organisatie is de verantwoordelijkheid voor de ondersteuning bij het uitvoeren van een DPIA neergelegd bij de FG. Soms wordt ook pas een DPIA uitgevoerd wanneer de activiteit waarvan de gegevensverwerking onderdeel is, al is gestart. Dat is niet in overeenstemming met de AVG, die stelt dat de DPIA dient te worden uitgevoerd voordat de gegevensverwerkingsactiviteiten starten.

De meeste organisaties hebben een duidelijke procedure en vaak een formulier voor het melden van een datalek. Die procedure is neergelegd in een protocol en vaak ook op het intranet te vinden. De indruk van de geïnterviewden is dat medewerkers die te maken hebben met een datalek daarvan ook melding doen. De casestudy-organisaties hebben registers waarin datalekken worden bijgehouden. Gemelde datalekken worden door privacy officers onderzocht. Bij sommige organisaties wordt in overleg met de FG bepaald of een datalek bij de AP moet worden gemeld, andere melden elk datalek bij de toezichthouder. In de casestudy's tekenden

we op dat op een van de gemeentelijke organisaties na, een geconstateerd datalek altijd wordt gevolgd door de afweging van de noodzaak van een verbeteractie.

6.7 Knelpunten en verbeterpunten

In deze paragraaf beschrijven we wat de belangrijkste knelpunten zijn die bij een vergelijking tussen de casestudy's bij de naleving van de AVG door overheden naar voren komen.

De meeste organisaties waar we onderzoek deden, investeren tijd in de bewustwording bij de medewerkers van nut en noodzaak van de AVG. Dat doen ze door te investeren in training en opleiding. Verschillende organisaties bieden meerdere e-learning modules aan voor nieuwe medewerkers, bestaande medewerkers en voor leidinggevenden. Tegelijkertijd realiseert iedereen zich dat een AVG-conforme nalevingscultuur niet vanzelfsprekend is. Niet bij alle organisaties is daarvan in voldoende mate sprake. Achterblijvend nalevingsgedrag heeft te maken met ontbrekende of gebrekkige kennis, maar ook met het belang dat bestuur en management uitdragen. De aandacht voor AVG-naleving varieert en komt bijvoorbeeld tot uitdrukking in het soms pas achteraf betrekken van privacy officers bij projecten en het – mede daardoor – niet altijd uitvoeren van DPIA's waar dat wel noodzakelijk is. Privacy heeft niet altijd prioriteit bij de bestudeerde organisaties, veelal 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 aandachtspunt bij. Dan zijn belangrijke keuzes vaak al gemaakt, waardoor AVG-naleving lastig is. Tijdens de expertmeeting is breed aandacht gevraagd voor de rol van politiek en bestuur bij het prioriteren van de naleving van de AVG. Pas als op dat niveau het besef bestaat dat gegevensverwerking als kernactiviteit van overheden moet worden gezien verbetert de naleving van de AVG volgens de experts.

Een ander knelpunt dat we bij meerdere organisaties zijn tegengekomen is de bezetting van posities. De krappe arbeidsmarkt speelt daarbij een rol, waarbij dat specifiek geldt voor de functies van FG, privacy officers en functies op het vlak van informatiebeveiliging. Bij verschillende organisaties zijn posities niet ingevuld of worden bepaalde werkzaamheden uitgevoerd door functionarissen die dat niet in hun takenpakket hebben. Dat leidt tot rolverwarring, die we regelmatig tegenkwamen bij FG's die eerder adviseur dan interne toezichthouder zijn. Meer algemeen is de afbakening van de functies van privacy officer en FG een kwestie die aandacht vraagt. Tijdens de expertmeeting is ook aandacht gevraagd voor het vergroten van kennis van de AVG. Sleutelposities binnen de privacy-organisatie lijken regelmatig moeilijk te vullen; de poel waarin wordt gevist is betrekkelijk klein. Door betere scholing van de al aangewezen privacyfunctionarissen, of door het opleiden van nieuwe privacyfunctionarissen zou deze krapte verholpen kunnen worden. Daarbij zou ook gedacht kunnen worden aan beroepskwalificaties voor privacyfuncties, zodat beter kan worden gestuurd op expertise binnen de organisatie.

Sommige organisaties laten een sterke focus op techniek zien, waarbij het treffen van passende maatregelen in de sfeer van informatiebeveiliging aandacht krijgt, maar de nadruk minder ligt op de bescherming van persoonsgegevens en het waarborgen van dat belang in de processen binnen de organisatie. Soms is de achtergrond daarvan een incident dat zich bij die organisaties heeft voorgedaan op het vlak van informatiebeveiliging, zoals een hack of een datalek.

De voorgaande knelpunten leiden tot een aantal verbeterpunten die op grond van dit onderzoek bij overheidsorganisaties onder de aandacht worden gebracht. Daarbij ligt de nadruk op de eerste lijn, de lijn, of het primaire proces. Daar wordt het werk uitgevoerd dat kan leiden tot het optreden van privacyrisico's. We constateren dat overheidsorganisaties relatief veel inzet plegen op het vergroten van de kennis van de privacyregels en -standaarden. Dat die kennis vervolgens ook in het werk wordt toegepast is een kwestie van houding en gedrag. Daarbij speelt het management een belangrijk rol. Wanneer het management het belang van de bescherming van persoonsgegevens expliciet benoemt en daarin ook voorbeeldgedrag laat zien, kan de nalevingscultuur van de organisatie positief worden beïnvloed.

Een tweede verbeterpunt is van organisatorische aard. Overheidsorganisaties hebben in hun beleidsdocumenten veelal een duidelijke inrichting van de privacy-organisatie vastgelegd, in veel gevallen het *three lines of defence*-model. In de praktijk krijgt die organisatie-inrichting echter niet altijd consequent invulling. Soms is sprake van gebrek aan rolvastheid en niet zelden ook van niet bezette functies. Het is van belang dat dit punt goed wordt bewaakt. Dat is een duidelijke verantwoordelijkheid van management en bestuur.

Een derde suggestie betreft de nadruk op informatiebeveiliging. De indruk bestaat dat vaak de nadruk ligt op de aanpak van eenvoudige risico's in de sfeer van informatiebeveiliging, zoals het vergrendelen van usb-sticks en laptops met wachtwoorden, het introduceren van 2-staps verificatie of het beveiligd versturen van e-mails. Overheidsorganisaties moeten er voor waken dat de naleving van de AVG niet verwordt tot uitsluitend een kwestie van bedrijfsvoering. Privacy moet een plaats hebben binnen de PDCA-cyclus in de organisatie, in de kwaliteitsborging, zodat een volwassen privacy-organisatie ontstaat.

6.8 Conclusie

De AVG trad ruim vier jaar geleden in werking. Het is onmiskenbaar dat de komst van de AVG veel veranderingen heeft gebracht op het terrein van de gegevensbescherming, ook bij Nederlandse overheden. Critici zeggen daarover dat dit bijzonder is gelet op het feit dat de normen van de AVG inhoudelijk niet ingrijpend verschillen van de normen waaraan overheden zich ook voordien hadden te houden. Dat neemt niet weg dat de AVG in brede zin geldt als een 'game changer', zowel nationaal als Europees. Een deel van de 'soft power' van de Europese Unie, waar de Unie normen stelt die ook buiten de lidstaten juridische betekenis hebben vanwege de economische macht van de Unie, is erop gebaseerd. Duidelijk is dat ook de Nederlandse overheid privacybescherming serieuzer is gaan nemen. Deze conclusie begint dan ook met een positieve toon: de AVG heeft veel veranderingen gebracht en de naleving van de AVG door overheden is gaandeweg daadwerkelijk op gang gekomen.

Dat neemt niet weg dat er tegelijkertijd ook nog een weg te gaan is. De casestudy's laten zien dat verschillende knelpunten zijn geconstateerd. Een aantal daarvan heeft een bredere strekking en komt bij meer organisaties voor, andere beperken zich tot een of enkele overheidsorganisaties. We hebben bij het beschrijven en analyseren van de casestudy's geput uit twee inspiratiebronnen: de Tafel van Elf over dimensies van spontane naleving en handhaving en de meer globale benadering van 'weten, willen en kunnen'. Hierop grijpen we op deze plaats terug.

We maken een belangrijke opmerking vooraf. We bestudeerden negen overheidsorganisaties waarin we de naleving van de AVG in beeld hebben gebracht. We constateerden een belangrijk verschil tussen de aard van de overheidsorganisatie die centraal stond, waarbij er een belangrijk onderscheid gemaakt moet worden tussen 'politieke' overheidsorganisaties en 'technische' overheidsorganisaties. Met die eerste categorie doelen we op overheidsorganisaties waar politiek-bestuurlijke afwegingen over uitgangspunten van beleid en de uitvoering daarvan gemaakt worden. De tweede categorie zijn de uitvoeringsorganisaties die zich over het algemeen minder met beleidsmatige afwegingen bezighouden. Uiteraard is zo'n tweedeling een sterke versimpeling van de werkelijkheid en gaat het om twee uitersten van een breed spectrum. Dat neemt niet weg dat een departement of een gemeente een overheidsorganisatie is waarin het politieke bestuur een sterke invloed heeft. Daar staan uitvoeringsorganisaties tegenover waarbij vooral de techniek, in de zin van de doelmatigheid en effectiviteit van de uitvoering, voorop staat. Dat onderscheid komt in de casestudy's in die zin naar voren dat de uitvoeringsorganisaties op een meer vanzelfsprekende manier de normen van de AVG naleven, terwijl de naleving van privacynormen bij de gemeenten en het departement in sterkere mate afhankelijk is van een afweging van belangen. Daarbij is de dominantie van beleidsdoelen veel groter en dat laat zich verklaren door de nabijheid van de politiek binnen die organisaties. Bij gemeenten en departementen spelen daadwerkelijk ook meer en uiteenlopende belangen, waardoor de te maken afwegingen in de praktijk complexer zijn. Naleving van de AVG door die organisaties lijkt daarmee minder vanzelfsprekend en in ieder geval veel lastiger. Op dit punt komen we later nog terug, maar het lijkt als algemene aftrap wel van belang.

Kennis van de AVG bij overheidsorganisaties is de afgelopen jaren sterk verbeterd. In de casestudy's komt dat tot uiting door de inspanningen die overheden plegen op het vlak van kennisbevordering. Verschillende overheden bieden interne scholingsactiviteiten aan, huren externen in en hebben een contract voor de afname van e-learning modules waaraan medewerkers en leidinggevenden periodiek deel moeten nemen. Op deze manier wordt de kennis binnen de organisatie van de AVG en de instrumenten van privacybescherming vergroot en het bewustzijn aangewakkerd. Dat het gemiddelde kennisniveau is verbeterd wil overigens nog niet zeggen dat de kennis overal op orde is. Vaak is kennis bij een beperkt aantal medewerkers aanwezig, maar ontbreekt die bij anderen die ook met persoonsgegevens werken. Bovendien – zo kwam in veel gesprekken en ook tijdens de expertmeeting naar voren – is het gegevensbeschermingsrecht een ingewikkeld rechtsgebied. Als gevolg van algemene beginselen die in de AVG centraal staan, zoals doelbinding (in beginsel mag informatie die met een bepaald doel is verzameld niet voor een ander doel worden gebruikt) en noodzakelijkheid (ook wel dataminimalisatie genoemd: het verwerken van persoonsgegevens moet noodzakelijk zijn voor het doel waarvoor dat wordt ingezet), kunnen antwoorden op vragen niet altijd eenvoudig gevonden worden.

Hoewel het met de kennis van de AVG redelijk goed lijkt te gaan, is het niet zo dat naleving van de AVG altijd vanzelfsprekend is. Wanneer naleving tekort schiet is dat overigens niet altijd een bewuste keuze. Soms ontbreekt voldoende besef dat het beoordelen van AVG-aspecten vooraf moet gaan aan een verwerking van persoonsgegevens. Dat uit zich dan in DPIA's die pas achteraf worden uitgevoerd, waardoor correcties in processen die nodig zijn achterwege blijven of met veel extra inzet gepaard gaan. Er is dan sprake van een zichzelf versterkend effect, want juist daardoor krijgt de AVG en het waarborgen van privacybescherming een slechte naam. Een enkele keer is expliciet sprake van een keuze om niet na te leven, en is de beleidsdoelstelling dominant ten koste van naleving van de AVG. Dan zou echt gesproken kunnen worden van tekortkomingen op 'willen'. Maar dat zijn eerder de uitzonderingen die de

regel, dat het steeds beter gaat met de naleving van de AVG, bevestigen. Als dat aan de orde is klinkt *the tone at the top* onvoldoende helder en luid. Privacybescherming staat dan onvoldoende op de besluitvormingsagenda, rapportages van FG's worden niet besproken of blijven zonder vervolgacties en voorbeeldgedrag ontbreekt. Is dat aan de orde dan sneeuwt het privacybelang soms onder in de belangenafweging.

Als de kennis op orde is en er is sprake van nalevingsbereidheid, moeten er ook voldoende middelen zijn om de AVG-instrumenten toe te passen. Belangrijke randvoorwaarde daarvoor is de organisatie-inrichting: medewerkers moeten weten wat hun verantwoordelijkheden zijn en waar ze te rade kunnen gaan om advies. Bij overheidsorganisaties is het *three lines of defence*-model breed ingevoerd. Die organisatie-inrichting functioneert over het algemeen ook naar tevredenheid. Kanttekening is dat door personeelstekorten of wisselingen in de formatie, de posities niet altijd bezet zijn, waardoor met name de derde en de tweede lijn soms door elkaar gaan lopen. Verder zien we bij de organisaties, zeker waar in het verleden een incident aan de orde was, een focus op het realiseren van adequate informatiebeveiliging. Soms blijft het belang van naleving van de AVG in de processen binnen de organisatie vergeleken daarmee wat achter.

7 Conclusie

7.1 Inleiding

In dit hoofdstuk geven we de antwoorden op de onderzoeksvragen. Dat doen we in paragraaf 7.2. In paragraaf 7.3 besluiten we het onderzoeksrapport met een slotbeschouwing. We hebben in dit onderzoeksrapport een beschrijving gegeven van de naleving van de AVG door de overheid. We realiseren ons dat we een ambitieuze onderzoeksvraag proberen te beantwoorden. Dé overheid bestaat natuurlijk niet. Omdat de AVG geldt voor alle gegevensverwerkingen door alle overheden is de nalevingsvraag niet eenvoudig te beantwoorden. Bij de veelheid aan overheidsorganisaties is immers sprake van een variatie aan kenmerken zoals schaal, beleidsterrein, politiek-bestuurlijke afwegingsruimte en uitvoeringscomplexiteit. Ook de vraag of overheden werken met bijzondere persoonsgegevens doet ertoe, evenals de mate waarin overheden met elkaar samenwerken en gegevens delen. We hebben dan ook niet de pretentie in dit rapport een volledig beeld te schetsen van de variatie die zich bij al die verschillende overheden voordoet als het gaat om de naleving van de AVG.

We kozen er voor met behulp van een casestudy-design de onderzoeksvraag te beantwoorden, waarbij we de wijze hebben bestudeerd waarop een negental overheden, die variëren op een aantal kenmerken, de AVG naleven. De casestudy's hebben we uitgevoerd aan de hand van documentenonderzoek en interviews. Daarmee hebben we een beeld verkregen van de toepassing van de AVG op papier en bezien door de ogen van enkele respondenten bij de overheden. We hebben dus niet zelf kunnen observeren hoe binnen de bestudeerde organisaties de naleving van de AVG verloopt. De wijze waarop de instrumenten van de AVG – zoals het uitvoeren van een DPIA voor een gegevensverwerking of het melden van een datalek – binnen de bestudeerde overheden precies worden toegepast, hebben we niet zelf kunnen vaststellen, maar bezien we door de ogen van de gesprekspartners en op basis van wat daarover aan het papier is toevertrouwd. Dat betekent dus ook, zoals in de onderzoeksaanpak in paragraaf 2.3 al werd aangestipt, dat wanneer verwerkingen van persoonsgegevens binnen de organisaties niet in overeenstemming zijn met de AVG en de UAVG, en dat niet in beeld is bij de privacyorganisatie, deze in dit onderzoek dus ook niet aan het licht zijn gekomen.

De voorgaande opmerkingen nemen niet weg dat we menen met deze rapportage een redelijk getrouw beeld van de naleving van de AVG bij overheden te hebben geschetst. Door de praktijk binnen de negen organisaties met elkaar te vergelijken ontstaat een aantal regelmatigheden op punten als beleid, organisatie-inrichting en kennisontwikkeling. Door die voor te leggen aan deelnemers aan een expertmeeting, tegen de achtergrond van een aantal verdiepende interviews met onder andere medewerkers van de VNG, de Auditdienst Rijk en de Autoriteit Persoonsgegevens, denken we dat die regelmatigheden meer algemene gelding hebben. Het

onderzoek voerden we uit aan de hand van een tweetal conceptuele modellen, 'weten, willen en kunnen' en de Tafel van Elf. Die fungeerden als zoeklichten met behulp waarvan we de regelmatigheden in de nalevingspraktijk hebben opgespoord. Bij 'weten' hebben we gelet op de kennis binnen de organisatie over de regels en instrumenten van de AVG. Die kennis kan worden bevorderd door scholing en training. We richtten ons niet alleen op kennis, maar ook bewustzijn van het belang van de AVG en van naleving van de bepalingen van de wet in de organisatie. Daaraan verwant is 'willen', waarbij we na zijn gegaan in hoeverre de organisatie gemotiveerd is de AVG na te leven. Het gaat dan om de prioriteit die de organisatie geeft aan de naleving van de AVG in verhouding tot de uitvoering van haar kerntaken. Een belangrijk element daarbij is de opstelling die bestuur en management kiezen. Is de bescherming van persoonsgegevens een belangrijk uitgangspunt of wordt dat afgewogen tegen andere belangen? We hebben bijvoorbeeld gekeken in hoeverre de naleving van de AVG op de besluitvormingsagenda staat en of rapportages van de FG de bestuurstafel bereiken. Tot slot keken we naar 'kunnen': welke mogelijkheden heeft de organisatie om de AVG na te leven? Hoe is de privacy-organisatie ingericht? Zijn de posities bezet? Hoe staat het met de beveiliging van persoonsgegevens en zijn de technische randvoorwaarden vervuld?

Hierna grijpen we – veelal impliciet – terug op deze elementen om tot een beschrijving en analyse van de naleving van de AVG bij overheden te komen. Dat verdiepen we door daarbij de dimensies van spontane naleving uit de Tafel van Elf te betrekken. Die gaan over kennis van de regels, de kosten en de baten van de naleving, de mate van acceptatie van de normen van de AVG, de normgetrouwheid van de overheidsorganisatie en de maatschappelijke controle door bijvoorbeeld gebruikers van een overheidsdienst. Al deze elementen hebben gehanteerd bij het beschrijven van de bevindingen uit de casestudy's. Dat leidde per casestudy in hoofdstuk 5 tot een analyse. In dit concluderende hoofdstuk beantwoorden we in paragraaf 7.2 de onderzoeksvragen die we in hoofdstuk 1 formuleerden aan de hand van een 'between-case-vergelijking'.

7.2 Onderzoeksvragen

7.2.1 Huidig beeld

In deze subparagraaf beantwoorden we de deelvragen bij onderzoeksthema I, verkenning van het huidig beeld. Die luiden als volgt:

1. *Op welke manier kunnen overtredingen door overheidsorganisaties in beeld komen?*
2. *Welke instanties zijn betrokken bij het in beeld krijgen van deze overtredingen?*
3. *Wat is het huidige beeld van de naleving van de AVG en gerelateerde wet- en regelgeving?*
4. *Wat zijn mogelijke lacunes in de kennis van de naleving?*
5. *Welke selectie van cases geeft de beste kansen om tot een actueel beeld te komen van overtredingen door overheidsinstanties en de onderliggende redenen?*

Overtredingen door overheidsorganisaties kunnen op verschillende manieren aan het licht komen. De AVG kent in art. 33 een meldplicht wanneer sprake is van een datalek. Binnen 72 uur moet een datalek worden gemeld, tenzij niet waarschijnlijk is dat een inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De afgelopen jaren ontving de Autoriteit Persoonsgegevens jaarlijks ongeveer 25.000

meldingen per jaar, waarvan 15-20% afkomstig van overheidsorganisaties. Lang niet alle datalekken worden gemeld bij de AP, zo kan uit een vragenlijstonderzoek onder FG's worden afgeleid.[85]

De AP ontvangt behalve van gegevensverwerkers ook signalen van betrokkenen, dus individuen waarvan persoonsgegevens zijn verwerkt, dat sprake is van een datalek. De toezichthouder voert op eigen initiatief slechts beperkt onderzoek uit naar (niet gemelde) datalekken, vooral omdat daarvoor onvoldoende capaciteit beschikbaar is. De verwachting bij de AP is dat als gevolg van de publieke aandacht voor het functioneren van de overheid, ook via de media, signalen van mogelijke problemen bij het verwerken van persoonsgegevens onder de aandacht zullen worden gebracht.

Namens de toezichthouder zijn twee medewerkers belast met het proactieve, systeemgerichte toezicht op overheden. Daarmee is sprake van beperkte capaciteit voor het toezicht op de naleving van de AVG door overheden. De focus van het toezicht legt de AP daarbij op 'de digitale overheid' en op 'beveiliging'.

De ADR constateert een ontwikkeling waarbij FG's steeds nadrukkelijker een onafhankelijke positie als toezichthouder innemen. Als gevolg van capaciteitsproblemen komt het wel voor dat FG's in een adviesrol terechtkomen, waardoor deze toezichthouder op het eigen werk kan worden. Medewerkers van de VNG constateren dat het ook bij gemeenten steeds beter gaat met de onafhankelijke positie van de FG.

Bij de AP bestaat het beeld dat bij decentrale overheden de DPIA's niet op orde zijn. Ook gegevensverwerkingsregisters zijn niet volledig. In algemene zin typeert de AP de naleving van de AVG door overheden als 'in ontwikkeling'. Wat bij gemeenten een belangrijke rol speelt in de ogen van de toezichthouder is het geloof in data als oplossing voor veel vraagstukken. Daarmee kan gemakkelijk dominantie van beleidsdoelen optreden en dat risico is er zeker wanneer overheden in ketens met elkaar samenwerken en gegevens delen. De toezichthouder is verder van oordeel dat het kennisniveau bij gemeenten van het gegevensbeschermingsrecht niet op orde is. Dat klemt temeer tegen de achtergrond van de (keten)samenwerkingsverbanden waarin gemeenten zich begeven en waarbij gegevensuitwisseling een voorwaarde is voor doeltreffende uitvoering.

Bij verschillende gemeenten hebben zich de afgelopen jaren incidenten rond gegevensverwerking en -beveiliging voorgedaan. Gemeenten hebben de regels een aantal keren geschonden bij de inzet van *smart city*-toepassingen, waaronder wifitracking en online monitoring. Bijna alle gemeenten monitoren openbare bronnen op internet zonder dat daarvoor een juridische grondslag bestaat.

Dat neemt niet weg dat het algehele beeld van zowel de AP als de VNG over de AVG-naleving positief is; gemeenten zetten zeker stappen en zijn zich steeds meer bewust van het belang van gegevensbescherming en de borging daarvan. Ook op het gebied van kennisdeling worden gemeenten, ondersteund door de VNG, steeds actiever. Er wordt bijvoorbeeld gebruik

[85] Heinrich Winter, Thijs Drouen e.a., *Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en boetebevoegdheid*, Groningen/Den Haag 2022, p. 66.

gemaakt van standaard verwerkersovereenkomsten, en ook op andere gebieden wordt getracht te voorkomen dat gemeenten het wiel onnodig opnieuw uitvinden.

Bij enkele ministeries (Defensie en JenV) deden zich de afgelopen jaren incidenten voor rond de verwerking van persoonsgegevens zonder dat daarvoor een wettelijke grondslag bestond. Ook bij uitvoeringsorganisaties waren er problemen, waarvan die bij de Belastingdienst het meest bekend zijn als gevolg van de Kinderopvangtoeslagaffaire. Ook bij UWV, CBR, KvK en DUO zijn (mogelijke) problemen met gegevensverwerking gesignaleerd.

Afgezien van de incidenten die zich voor hebben gedaan is de algemene indruk dat de naleving op rijksniveau zich in positieve richting ontwikkelt. Bij sommige departementen gaat dat sneller dan bij andere. Verschillende incidenten hebben de urgentie van gegevensbescherming bevorderd. Er is een ontwikkeling waarbij privacy officers worden gevraagd mee te denken aan de tekentafel bij de voorbereiding van gegevensverwerkingen. Het bewustzijn van het belang van privacy neemt dus toe volgens onze gesprekspartners. Ook de secretarissen-generaal sturen nadrukkelijker op het belang van privacy. Tegelijkertijd wordt geconstateerd dat capaciteit en middelen een probleem kunnen zijn. Het primaire proces heeft altijd voorrang en het moet allemaal snel en efficiënt; investeren in privacybescherming is daardoor niet altijd vanzelfsprekend.

Het algemene beeld dat uit diverse bronnen en uit gesprekken met een aantal organisaties zoals de ADR, de VNG en de AP, voort is gekomen laat zien dat er signalen zijn van een positieve ontwikkeling. Dat neemt niet weg dat onvoldoende informatie bestaat over hoe de privacy-organisatie bij overheden is ingericht, wat overheden precies doen om de naleving van de AVG te bevorderen en hoe ze de instrumenten van de AVG in de praktijk hanteren. Om daarop meer greep te krijgen is gekozen voor het uitvoeren van een aantal casestudy's bij overheidsorganisaties. Daarbij is zowel gekozen voor het bestuderen van organisaties die te maken hadden met incidenten rond het verwerken van persoonsgegevens als voor organisaties waarvan op dat punt geen signalen bekend waren.

7.2.2 Casestudy's

In een negental casestudy's hebben we de lacunes die in het algemene beeld van de naleving van de AVG bestonden getracht in te vullen. De volgende vragen waren daarbij leidend:

6. *Hoe luidt het privacybeleid bij de bestudeerde overheidsorganisaties en hoe is de privacy-organisatie ingericht?*
7. *Welke onduidelijkheden, problemen en risico's kunnen binnen de bestudeerde overheidsorganisaties worden onderscheiden bij de naleving van de AVG?*
8. *Hoe werken de interne toezichtsmechanismen op de naleving van de AVG door deze overheidsorganisaties en hoe was de rol van de functionaris voor gegevensbescherming (FG) in het proces geborgd?*

De casestudy's laten zien dat de overheden serieus werken aan de naleving van de AVG. Alle bestudeerde overheidsorganisaties hebben beleid vastgesteld over de AVG en over de inrichting van de privacy-organisatie. Het *three lines of defense-model* is de gangbare wijze waarop de privacy-organisatie bij de overheden wordt vormgegeven. Al met al is bij de bestudeerde overheden sprake van positieve ontwikkelingen als het gaat om de naleving van de AVG. Het casestudy-onderzoek laat ondertussen wel zien dat bij die conclusie ook kanttekeningen moeten worden geplaatst.

Overtredingen van de AVG die bij de bestudeerde overheidsorganisaties aan de orde waren vonden telkens hun oorsprong in onvoldoende bewustzijn van het belang van het gegevensbeschermingsrecht. Dat had tot gevolg dat persoonsgegevens werden verwerkt zonder wettelijke grondslag bedoeld in artikel 6, eerste lid, AVG of dat onvoldoende sprake was van beveiligingsmaatregelen, bedoeld in artikel 32 AVG, waardoor een datalek ontstond of dat het verwerken van persoonsgegevens al was gestart zonder dat een DPIA was opgesteld. In algemene zin was het belang van de bescherming van persoonsgegevens onvoldoende aanwezig in de processen binnen de organisatie waar uiteindelijk overtredingen aan het licht kwamen. In juridische zin betekent dit dat in die gevallen de verwerkingsverantwoordelijkheid van artikel 24 AVG onvoldoende is ingevuld.

De achterliggende oorzaak daarvan moet vooral worden gezocht in het tekortschieten van het bewustzijn dat de bescherming van privacy een door de overheidsorganisatie te waarborgen belang is. In de casestudy's kwamen we ook andere, meer praktische verklaringen van het tekortschieten van de privacybescherming tegen. Een belangrijk punt is dat bij sommige overheden posities binnen het *three lines of defence*-model niet ingevuld zijn, mede als gevolg van arbeidsmarktvraagstukken. De consequentie daarvan is dat de derde lijn in het model, de FG, adviserende werkzaamheden gaat verrichten, waarmee deze functionaris als het ware uit de toezichthoudende rol stapt en daardoor niet of in mindere mate in staat is om de taken bedoeld in artikel 39 AVG op onafhankelijke wijze in te vullen.

7.2.3 Analyse

De bevindingen van de casestudy's zijn in hoofdstuk 5 beschreven en individueel geanalyseerd. Vervolgens is in hoofdstuk 6 een casevergelijking uitgevoerd. Dat levert antwoorden op de volgende vragen op:

9. *Welke overeenkomsten zijn er te vinden in de cases?*
10. *Welke verschillen zijn geconstateerd? Wat zijn de verklarende factoren voor deze verschillen?*
11. *In hoeverre zijn de bestudeerde cases naar verwachting representatief voor de situatie bij overheidsorganisaties in het algemeen?*
12. *Wat zegt bovenstaande over de algemene situatie (uitgesplitst naar de vragen 6 - 8)?*
13. *Welke lacunes bevat het opgestelde beeld van de algemene situatie? Hoe zijn deze eventueel nog in te vullen?*

Een belangrijk verschil tussen de bestudeerde cases is dat tussen uitvoeringsorganisaties, belast met meer technische uitvoeringstaken enerzijds en overheden met politiek-bestuurlijke aansturing anderzijds. In die laatste categorie vallen de casestudy's van de gemeenten en het departement. In de eerste categorie vallen de uitvoeringsorganisaties die we bestudeerden. Het valt op dat de uitvoeringsorganisaties die werken met grote databestanden en registraties een groot bewustzijn aan de dag leggen dat ze persoonsgegevens verwerken, hetgeen de nodige zorgvuldigheid met zich mee behoort te brengen. Die zorgvuldigheid zien we vervolgens terug in de veiligheidswaarborgen die in technische zin binnen deze organisaties worden nagestreefd en in de mate waarin AVG-eisen in de werkprocessen binnen die organisaties zijn geborgd. De AVG wordt binnen de bestudeerde uitvoeringsorganisaties zoveel mogelijk aan de voorkant bij besluitvorming betrokken. Het belang dat binnen departementen en gemeenten wordt gehecht aan de bescherming van persoonsgegevens wordt in vergelijking met de uitvoeringsorganisaties sterker bepaald door politiek-bestuurlijke afwegingen. Daarbinnen hebben de AVG-eisen een minder vanzelfsprekende plaats: binnen de weging van belangen delft het privacybelang dan soms het onderspit. De dominantie van beleidsdoelstellingen leidt

ertoe dat soms op een (te) laat moment aandacht aan privacywaarborgen wordt besteed waardoor de verwerking van gegevens al aan de orde is zonder dat de vraag naar de verwerkingsgrondslag afdoende is beantwoord, of zonder dat een DPIA is opgesteld of de verwerking in het verwerkingsregister is opgenomen. Sommige van deze gebreken zijn herstelbaar, maar dat is niet altijd het geval.

Er zijn ook overeenkomsten tussen de casestudy's geconstateerd. Om te beginnen doen alle bestudeerde organisaties het een en ander aan kennisbevordering. Daarbij moet wel aangetekend worden dat de kennisbevordering gericht is op het op orde krijgen en houden van de basis. Verder hebben ze allemaal beleid, dat ook meestal redelijk actueel is. Daarnaast volgens ze alle het *three lines of defence*-model.

Het lukt de organisaties niet allemaal even goed de organisatie-inrichting die op papier is bedacht voor de privacy-organisatie ook in de praktijk invulling te geven; de privacy-organisatie is ook niet altijd bij iedereen binnen de organisatie bekend. Overwegend liggen daaraan arbeidsmarktvraagstukken ten grondslag, maar het is ook niet helemaal uit te sluiten dat de mate waarin de privacy-organisatie prioriteit krijgt een verklaring daarvoor vormt. De gevolgen zijn wel serieus. Anders dan de AVG stelt is de consequentie daarvan dat de derde en de tweede lijn in elkaar overvloeien: de FG komt dan in een adviserende rol terecht, en wanneer dat structureel het geval is komt dat op gespannen voet te staan met de toezichthoudende rol. Maar ook van belang is dat privacyvraagstukken dikwijls door de medewerkers in de eerste lijn niet als zodanig worden herkend; het gevolg is dan dat de tweede lijn ook niet om advies wordt gevraagd.

De algemene indruk is dat het op dit moment beter gesteld is met de naleving van privacynormen 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 is gesteld met de waarborgen voor zorgvuldige omgang met persoonsgegevens door overheden. Dat neemt echter niet weg dat er nog een weg te gaan is; verdere verbetering is zeker mogelijk. Vooral het in de werkprocessen binnen overheidsorganisaties, en dan met name de gemeenten en departementen, opnemen van privacywaarborgen zou meer vanzelfsprekend moeten zijn. Privacy behoort aan de voorkant bij de verwerking van data aandacht te krijgen en niet pas nadat de belangrijkste beslissingen reeds genomen zijn. Daarvoor is bewustwording een kernpunt. Dat gaat ook over *the tone at the top* en het geven van het goede voorbeeld door het bestuur en het topmanagement. Door aandacht te geven aan belangenafwegingen rond de AVG en dilemma's die daarbij spelen kunnen bestuur en management het bewustzijn bij de rest van de organisatie bevorderen. Behalve over de manier waarop over de AVG wordt gesproken gaat het bij *tone at the top* dus ook om daadwerkelijk gedrag.

Omdat slechts negen overheidsorganisaties zijn bestudeerd, is niet zeker dat een representatief beeld is verkregen van de naleving van de AVG door overheden. Dat neemt niet weg dat wel sprake is van spreiding over een aantal belangrijke kenmerken van de organisaties, zoals het type organisatie (uitvoeringsorganisatie of politiek-bestuurlijke aansturing), centrale overheid of decentrale overheid en schaal. Verder is sprake van spreiding over beleidsdomeinen en over het land. Er zijn vooralsnog geen redenen om te twijfelen aan meer algemene geldigheid van het geschetste beeld, maar dat neemt niet weg dat terughoudendheid op dat punt is geboden.

De belangrijkste kanttekening die bij de bevindingen van het onderzoek moet worden geplaatst heeft te maken met de aard van het uitgevoerde onderzoek. Met de toegepaste methode van casestudy-onderzoek was het niet mogelijk in te zoomen op individueel gedrag van medewerkers binnen organisaties. Door te focussen op beleid, organisatie-inrichting, kennisbevordering en de algemene instrumenten van de AVG is wel inzicht in algemene mechanismen ontstaan, maar welk gedrag individuele medewerkers precies vertonen is daarmee nog niet inzichtelijk geworden. Daarvoor is aanvullend onderzoek nodig gericht op het individueel handelingsperspectief.

7.3 Slotbeschouwing

Vier jaar na de inwerkingtreding van de AVG is er bij overheden veel gedaan op het vlak van de bescherming van persoonsgegevens. De situatie is verbeterd in vergelijking met die van een aantal jaren geleden. Tegelijkertijd geldt dat er weliswaar veel is gebeurd, maar dat er ook nog veel te doen is. Veelal zijn organisaties nog bezig met het op orde krijgen en houden van de basis. Daarbij gaat het bijvoorbeeld om duidelijkheid over de juridische grondslag voor verwerkingsactiviteiten. In deze paragraaf beantwoorden we de laatste onderzoeksvraag:

14. *Welke aanbevelingen kunnen worden gedaan om de naleving van de AVG door overheidsorganisaties te verbeteren?*

Op basis van de bevindingen van dit onderzoek kunnen we een aantal aanbevelingen doen, gebaseerd op de *good practices* die we bij verschillende overheidsorganisaties in het onderzoek hebben gezien. In algemene zin geldt dat ook anderen dergelijke *good practices* zouden kunnen delen. Daarbij denken we met name aan de toezichthouder en aan de ministeries van JenV en BZK die op het terrein van de bescherming van persoonsgegevens een bijzondere verantwoordelijkheid hebben.

Op rijksniveau vraagt het versterken van het privacybelang bij gegevensverwerking en besluitvorming daarover om een rol voor het ministerie van Justitie en Veiligheid, in het bijzonder voor de minister voor Rechtsbescherming, die met het taakveld bescherming persoonsgegevens is belast. Dezelfde rol dient het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, in de persoon van de minister van BZK, te vervullen richting de decentrale overheden. Hoewel veel is gedaan in de afgelopen jaren, zijn verdere investeringen bij overheidsorganisaties nodig om privacy-organisaties steviger te funderen en het privacybewustzijn sterker te verankeren. Beide ministeries kunnen daarbij een stimulerende rol spelen door aandacht te blijven vragen voor het rechtsstatelijke belang van de bescherming van persoonsgegeven, maar ook door het delen van *good practices*, via handreikingen of andere communicatieproducten.

Aandacht is nodig voor het tijdig betrekken van privacybelangen bij de ontwikkeling van projecten die gepaard zullen gaan met verwerking van persoonsgegevens. Dat betekent dat functionarissen uit de privacy-organisatie vanaf de start daarvan daarbij worden ingezet. Bij een van de gemeenten kwamen we in dat verband de *good practice* van het ‘nulgesprek’ tegen, waarbij privacy officers met medewerkers en management van de eerste lijn samen nagaan wat de privacy-implicaties van een bepaalde verwerking zouden kunnen zijn. Dat vraagt om toegenomen bewustzijn bij medewerkers in de eerste lijn, dus bij vakafdelingen en binnen projectorganisaties, dat privacy-aspecten aan de orde (kunnen) komen. Van *privacy by design*

kan alleen wat worden verwacht wanneer het belang van privacy vanaf de start van een gegevensverwerking wordt meegewogen.

Het invullen van de verwerkingsverantwoordelijkheid door het uitvoeren van een DPIA moet niet als een afvinklijstje worden behandeld, maar als een serieus gesprek over de relevante processen en risico's, waarbij er ook aandacht is voor data-ethiek. 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.

Uiteraard is voor het invullen van de privacy-organisatie in het *three lines of defense*-model voldoende capaciteit vereist. Dat geldt ook voor de ontwikkeling, actualisatie en evaluatie van het privacybeleid. Er is in de casestudy's op dit punt een duidelijk arbeidsmarktvraagstuk naar voren gekomen; dat vraagt ten eerste om gerichte investeringen in bestaande medewerkers om de deskundigheid te bevorderen. Daarnaast zou gekeken kunnen worden naar de mogelijkheden om meer in te zetten op de aanbodkant van de arbeidsmarkt door het opleiden van deskundigen te stimuleren.

Voldoende aandacht en capaciteit voor het belang van privacy binnen de overheidsorganisatie staat of valt – zo laten de casestudy's zien – met de prioriteit die bestuur en directie aan het onderwerp geven. Voorbeeldgedrag, maar ook aandacht voor het waarborgen van de bescherming van privacy en de zichtbaarheid daarvan in de afweging tegen beleidsdoelstellingen helpen daarbij. Daarbij hoort ook dat oog bestaat voor de dilemma's die naleving van de AVG soms met zich mee kan brengen en de toegevoegde waarde van het voeren van een expliciet gesprek daarover.

De toezichthouder, de Autoriteit Persoonsgegevens, heeft een bijzondere verantwoordelijkheid. In het onderzoek bij overheden merkten we een duidelijke behoefte aan meer communicatie, voorlichting en sturing door de AP – naast de handhavende taak die de toezichthouder nu vooral prioriteit lijkt te geven. Diverse FG's van de bestudeerde overheidsorganisaties gaven aan behoefte te hebben aan (informeel) contact met de AP. Concreet gaat het daarbij om contact om verwerkingen met een grote impact en specifieke zorgen op privacygebied te kunnen bespreken met de AP. De AP heeft weliswaar een helpdesk die FG's toegang biedt, maar dat levert geen oordelen op over specifieke situaties. De FG's geven aan dat actief meedenken door de AP wordt gemist. Er zijn bij de AP zogenaamde voorafgaande raadplegingen bij hoge restrisico's mogelijk, maar deze gaan niet over de vraag of in een bepaalde situatie een voldoende juridische grondslag bestaat voor verwerking – die vraag heeft de organisatie in de DPIA die aan de voorafgaande raadpleging moet worden opgesteld al moeten beantwoorden. De terughoudendheid van de AP op deze punten kan wel worden verklaard uit het klassieke dilemma van de toezichthouder die terughoudend moet zijn als adviseur om de eigen toezichtstaak niet uit te hollen. De AP beroept zich echter vooral op capaciteitsgebrek. Er ligt al langere tijd een verzoek tot uitbreiding van de organisatie bij het ministerie van JenV. Die uitbreiding is ook in het vooruitzicht gesteld, mogelijk biedt dat op dit punt soelaas.

Een ander punt betreft de meldplicht datalekken. Verschillende keren gaven de bestudeerde organisaties aan dat de AP geen terugkoppeling geeft van bij de toezichthouder ingediende

meldingen. Een reactie zou volgens de overheidsorganisaties vooral nuttig zijn wanneer ze regelmatig vergelijkbare meldingen doen.

Ook het systeemtoezicht van de AP komt voor versterking in aanmerking. De organisatie rapporteert voor de hele overheidssector slechts twee medewerkers beschikbaar te hebben voor het houden van toezicht. Die zeer beperkte capaciteit vraagt om investeringen in de organisatie. Maar de AP zou ook beter gebruik kunnen maken van het bestaande netwerk van FG's, door hun kennis te gebruiken en vanuit de AP hulplijnen in de richting van de FG's te leggen.

Bijlage 1: Bronvermelding

Literatuur

E. Appelbaum, T. Bailey, P. Berg, & A. Kalleberg, *Manufacturing advantage: Why high- performance work systems pay off*, Cornwell University Press: Ithaca 2000

W. Bantema, S. Westers, M. Hoekstra, R. Herregodts & S. Munneke, 'Black Box van gemeentelijke monitoring', *Politiekunde* 2021, 109

H.R. Kranenborg & L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming In Europees en Nederlands perspectief* (Mastermonografieën staats- en bestuursrecht), Wolters Kluwer: Deventer 2018, p. 226

H.B. Winter, T. Drouen, e.a., *Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en boetebevoegdheid*, Groningen/Den Haag 2022

W. van Wijk, A. Reuijl en S. Aliar, FG-Enquête 2022. *Een tweede onderzoek naar de invulling van de functie van Functionaris Gegevensbescherming in de praktijk binnen de publieke sector*, Centrum voor Informatiebeveiliging en Privacybescherming, Amsterdam 2022

Parlementaire stukken

Kamerstukken II 2017/18, 34 851, nr. 3

Brief van de minister van Justitie en Veiligheid en de staatssecretaris van Justitie en Veiligheid van 29 januari 2021, met kenmerk 3181786

Aanhangsel Handelingen II 2020/2021, nr. 2287

Kamerstukken II 2020/21, 32761/30821, nr. 180, p. 3

Nieuwsberichten

M. Kuiper & R. van der Poel, 'Grapperhaus erkent: delen van gegevens asielzoekers met politie was onrechtmatig', *NRC* 18 januari 2021

Kamer van Koophandel, *Kamer van Koophandel schrapt adressen-product na kritiek AP*, 12 maart 2019, te raadplegen via kvk.nl (laatst geraadpleegd op 8 november 2022)

P. de Lange, 'DUO overtreedt privacyregels met volgsoftware in e-mails met studenten', *De Volkskrant* 7 augustus 2019

NOS, 'Privacywaakhond legt Enschede boete op van 600.000 euro vanwege wifitracking', 29 april 2021, te raadplegen via nos.nl.

G. Pols, 'CBR erkent fout met medische dossiers: 'Dit mag echt niet gebeuren'', *Trouw* 15 augustus 2019

E. Rosenberg & K. Berkhout, 'Hoe defensie de eigen bevolking in de gaten houdt', *NRC* 15 november 2020

L. Ruizendaal, M. Poncin & D. Hielkema, 'Kwart van gemeenten neemt privacy niet serieus', Argos 2020, te raadplegen via vpro.nl/argos.

RTL Nieuws, 'Illegale handel in privégegevens miljoenen Nederlanders uit coronasystemen GGD', 25 januari 2021, te raadplegen via rtlnieuws.nl

Rapportages

AP, *Jaarrapportage datalekken 2018,* 2019

AP, *Onderzoek naar Datafundamenten & Analytics*, 2019

AP, *Jaarrapportage datalekken 2019,* 2020

AP, *Jaarrapportage datalekken 2020,* 2021

AP, *Advies over het concept voor een wetsvoorstel Wet verwerking persoonsgegevens in het kader van coördinatie en analyse terrorismebestrijding en nationale veiligheid*, 2021

AP, *Smart Cities. Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*, 2021

AP, Jaarcijfers datalekken 2021, 2022

FG Defensie, *Onderzoek naleving Algemene verordening gegevensbescherming. Experimenteeromgeving Land Information Manoeuvre Centre (LIMC)*, 2021

KPMG, *Deelonderzoek 1: SONAR*, 2020

KPMG, *Onderzoek taken en financiële middelen bij AP*, 2020

Bijlage 2: Lijst met gesprekspartners

Huidig beeld

- Directeur Systeemtoezicht en Technologie, AP
- Senior Inspecteur Systeemtoezicht, AP
- Senior beleidsadviseur, ministerie van Justitie en Veiligheid
- Privacy adviseur, VNG
- Privacy adviseur, VNG
- Onafhankelijk expert, tevens FG van diverse organisaties

Ministerie

- AVG-coördinator
- Beleidsmedewerker
- FG voor de AVG
- FG voor de Wpg
- Hoofd beleidsafdeling
- Twee teamleiders

Uitvoeringsorganisatie 1

- CPO van de uitvoeringsorganisatie
- CPO van het ministerie
- FG van het ministerie
- Twee medewerkers van de interne auditdienst

Uitvoeringsorganisatie 2

- Beleidsadviseur op het gebied van dataverwerking
- Directeur
- CISO
- FG

Uitvoeringsorganisatie 3

- Centrale privacy officer
- Twee decentrale privacy officers
- Directeur
- Manager afdeling

Uitvoeringsorganisatie 4

- CIO
- CISO
- FG
- Medewerker in die fungeert als centraal aanspreekpunt en privacyrisico's signaleert

Waterschap

- Lid van het dagelijks bestuur
- Lid van de directie
- Security officer
- Teamleider afdeling Juridische Zaken

Gemeente 1

- Beleidsadviseur
- Concerndirecteur
- Concern-privacy officer
- FG
- Privacy officer
- Projectleider
- Teamleider

Gemeente 2

- FG
- Manager bedrijfsvoering
- Privacy officer
- Teamleider sociaal domein

Gemeente 3

- Concern-controller
- Directeur
- FG
- Juridisch medewerker

Expertmeeting

- Hoogleraar Gegevensbescherming en privacyrecht
- Hoogleraar Onderwijsinnovatie, datadelen en communicatierecht
- FG van een G4-gemeente
- FG van een grote gemeente
- FG van een kleine gemeente
- Senior inspecteur Systeemtoezicht, AP
- Privacy adviseur, VNG
- Privacy adviseur, VNG

Bijlage 3: Interviewprotocol casestudy's

Introductie

- Toelichting onderzoek

Onderwerp 1: De inrichting van de organisatie, met een nadruk op actoren rondom gegevensverwerking en gegevensbescherming

- Welke privacy-rollen zijn er, waar zijn ze belegd, en waar bestaan de werkzaamheden uit?
- Hoe wordt elke functionaris betrokken bij privacyvraagstukken?
- Hoe wordt geborgd dat verschillende onderdelen van de organisatie hetzelfde doen op het gebied van privacy?
- Hoe wordt geborgd dat medewerkers in de lijn met de AVG werken?
- Op welk moment in primaire werkproces(sen) worden privacyfunctionarissen betrokken bij vraagstukken, wie initieert dat, en welke overwegingen worden gemaakt om dit te doen?

Onderwerp 2: De FG binnen de organisatie

- Op welke wijze geeft de FG invulling aan de rol?
- Hoe vindt communicatie tussen de FG en de overige privacyrollen plaats?
- Wat is de verantwoordingsstructuur van de FG? Hoe zijn de verhoudingen met de privacy officer?

Onderwerp 3: Processen van verwerving en borging van kennis over de (U)AVG en andere regelgeving

- Hoe is borging van (bij)scholing geregeld?
- Wat wordt gedaan aan kennisoverdracht op dit gebied?
- Zijn er interne werkinstructies, protocollen en andere documenten over het verwerken van gegevens?
- Op welke manier kunnen medewerkers gebruik maken van de kennis van de privacy-organisatie?
- Hoe worden medewerkers uit de primaire processen betrokken bij het opstellen en uitwerken van privacybeleid?
- Welke onduidelijkheden over wet- en regelgeving zijn er?

Onderwerp 4: Ervaringen in de praktijk met naleving van de AVG in het algemeen

- Hoeveel prioriteit heeft gegevensbescherming binnen de dagelijkse praktijk en processen?

- Hoe goed kan de organisatie in het algemeen overweg met de (U)AVG? Waar loopt u tegenaan?
- Hoe wordt de rechtmatigheid van verzameling, verwerking en verstrekking van persoonsgegevens geborgd?
- Hoe wordt geborgd dat de technische implementatie (ICT) van processen conform de relevante AVG-bepalingen geschiedt?
- Welke problemen zijn er bij de naleving van de AVG?
- In hoeverre liggen deze aan de (U)AVG zelf?
- Beschikt de organisatie over voldoende capaciteit (mensen en middelen) om voldoende aandacht te besteden aan gegevensbescherming?
- Hoe zijn die problemen te categoriseren (inrichting organisatie, competenties en bevoegdheden, beleidsdominantie, gebrek aan kennis etc)
- Hoe wordt hiermee omgegaan? Hoe wordt getracht deze problemen aan te pakken?

Onderwerp 5: Overtredingen van de AVG (in het geval er overtredingen zijn geconstateerd)

- Wat is het project of besluit waarbij een overtreding is geconstateerd?
- Welke bepalingen uit de AVG zijn overtreden, hoe (en eventueel waarom) is dit zo gelopen?
- Hoe verliep de implementatie van informatiesystemen die voor gegevensverwerking gebruikt zijn?
- Hoe, wanneer en door wie werd de overtreding geconstateerd?
- Hoe functioneerden intern en extern toezicht hierbij?
- Bij een datalek: is een melding daarvan gedaan, en zo ja, wanneer? Zijn gedupeerden ingelicht?
- Welke reactie en/of ingrijpen heeft plaatsgevonden?
- Hoe is de (zelf)evaluatie verlopen? Wat waren de resultaten?
- Hoe verklaart de organisatie zelf de geconstateerde overtredingen?
- Wat zijn (achterliggende) oorzaken voor de geconstateerde overtredingen?
- Welke stappen zijn ondernomen om deze oorzaken te bestrijden? Welke (nog) niet en waar loopt men tegenaan bij het ondernemen van acties om herhaling te voorkomen?

Afsluiting

Bijlage 4: Opzet expertmeeting

Introductie

- Toelichting van aanleiding en opzet onderzoek
- Bespreking bevindingen op basis van het bestaande beeld
- Besprekingen bevindingen uit de casestudy's

Thema 1: Beleid en organisatie

- Bespreking bevindingen
- Stelling 1: ondanks het feit dat de rolinvulling in de praktijk nog niet conform de theorie is, is het *three lines of defense*-model het ideale model voor de inrichting van een privacy organisatie.
- Stelling 2: de FG wordt onvoldoende actief bevraagd en benut om privacyvraagstukken op te lossen.

Thema 2: Kennis en bewustzijn

- Bespreking bevindingen
- Stelling 1: De behoefte van overheden om 'slimme oplossingen' op basis van dataverwerking op te zetten, verhoudt zich slecht tot het principe van dataminimalisatie.
- Stelling 2: Overheden doen in het algemeen voldoende om privacybewustzijn te creëren en in stand te houden.

Thema 3: AVG-instrumenten

- Bespreking bevindingen
- Stelling 1: Het achterwege blijven van DPIA's is een privacybewustzijnsvraagstuk, geen organisatievraagstuk.

Thema 4: Knel- en verbeterpunten

- Bespreking bevindingen
- Stelling 1: De *tone at the top* is cruciaal voor het naleving van de AVG door de organisatie.
- Stelling 2: Zolang privacy niet als integraal onderdeel van het functioneren van een overheidsorganisatie wordt gezien, zal de naleving van de AVG onvoldoende zijn.

Afsluiting

- Wat zijn de belangrijkste aanbevelingen die u de ministers mee wilt geven?

Bijlage 5: Caseverslag ministerie

Inleiding

In dit verslag wordt de praktijk beschreven van de toepassing en naleving van de AVG door een ministerie. Dit ministerie kenmerkt zich als een ministerie, waarvan een zeer omvangrijke uitvoeringsorganisatie onderdeel is. Dit ministerie verwerkt voor de uitvoering van verschillende taken persoonsgegevens. Vanuit AVG-perspectief ondervindt dit ministerie meerdere uitdagingen. De privacy-organisatie is zich in de praktijk nog aan het vormen en ook het awareness bewustzijn op het vlak van de bescherming van persoonsgegevens is nog in ontwikkeling. Daarnaast wordt er, mede ingegeven door de actualiteit, een noodzaak gevoeld om persoonsgegevens te verwerken, waarvoor de van toepassing zijnde wetgeving geen grondslag geeft.

In het kader van deze casestudy hebben wij gesproken met de AVG-coördinator, de FG voor de AVG, de FG voor de Wpg, twee teamleiders van afdelingen waarbinnen diverse persoonsgegevens worden verwerkt, het hoofd van een beleidsafdeling en een beleidsmedewerker van diezelfde afdeling. Het privacybeleid van het ministerie en het Model gegevensbeschermingseffectbeoordeling rijksdienst is bestudeerd. Evenals brieven van de minister aan de Tweede Kamer die zien op de verwerking van persoonsgegevens door dit ministerie.

Gegevensverwerking door de organisatie

Dit ministerie verwerkt voor de uitvoering van verschillende taken persoonsgegevens. Vanuit AVG-perspectief ondervindt dit ministerie meerdere uitdagingen. De privacy-organisatie is zich in de praktijk nog aan het vormen en ook het bewustzijn op het vlak van de bescherming van persoonsgegevens is nog in ontwikkeling. Daarnaast wordt er, mede ingegeven door de actualiteit, een noodzaak gevoeld om persoonsgegevens te verwerken, waarvoor de van toepassing zijnde wetgeving geen grondslag geeft. Dit ministerie worstelt met de vraag of de grondslag gerechtvaardigd belang hierin kan voorzien.

Interne organisatie

Beleid

Met het van toepassing worden van de AVG heeft de staatssecretaris privacybeleid in een regeling vastgesteld. Dit document beoogt richting te geven aan hoe de organisatie om moet gaan met privacy en laat zien dat de organisatie de privacy waarborgt, beschermt en

handhaaft. Dit beleid is in beginsel van toepassing op alle verwerkingsactiviteiten binnen deze organisatie, behalve voor zover bepaalde verwerkingsactiviteiten op grond van de UAVG door de minister daarvan worden uitgesloten.

In de regeling wordt het AVG-beheer uiteengezet. Daarnaast wordt aandacht besteed aan de omgang met verwerkers, zijn de verplichtingen van de verwerkingsverantwoordelijke nader uitgewerkt, waaronder het register van verwerkingsactiviteiten, informatiebeveiliging en de meldplicht datalekken, en worden de rechten van betrokkenen en de inzet van de DPIA om tot risicobeheersing en controle daarop te komen, besproken. In de toelichting bij de regeling is geen visie of ambitie verwoord die ziet op het komen tot naleving van de AVG.

Privacy-organisatie

De privacy-organisatie van het ministerie is, zoals hiervoor is weergegeven, vastgelegd in een Privacyregeling. Hieronder worden alle relevante stakeholders en hun plaats binnen het privacybeleid en de organisatie besproken. Het ministerie hanteert, zoals naar voren kwam in de interviews, het *three lines of defenc*e-model; al wordt dit niet nadrukkelijk in de regeling of de toelichting daarbij benoemd.

De *eerste lijn* is de lijnorganisatie. Zij is verantwoordelijk voor het realiseren van de taken, waarvan privacy een vast onderdeel behoort te zijn. Met de lijnorganisatie worden de hierna genoemde actoren bedoeld.

De eindverantwoordelijkheid van het AVG-beheer ligt bij de *plaatsvervangend Secretaris-Generaal*. De *hoofden van de dienstonderdelen* zijn belast met de naleving van de AVG en de specifieke regelgeving ten aanzien waarvan verwerkingen worden gevoerd. Deze *AVG-beheerders* kunnen deze zorgplicht geheel of gedeeltelijk opdragen aan een *AVG-onderbeheerder* binnen het dienstonderdeel.

Elk organisatieonderdeel heeft zijn eigen privacy-organisatie ter ondersteuning van de AVG-beheerder. De AVG-beheerder kan een of meerdere *AVG-coördinatoren* aanwijzen Daarnaast zijn AVG-aanspreekpunten binnen verschillende onderdelen aangewezen die AVG werkzaamheden veelal in neventaak verrichten

De verwerkingsverantwoordelijke – zijnde *de minister* – blijft bevoegd de uit de AVG voortvloeiende bevoegdheden van een verwerkingsverantwoordelijke zelf uit te oefenen, indien dit in voorkomend geval wenselijk mocht zijn en om als AVG-beheerder ten aanzien van bepaalde gegevensverwerkingen te voorzien in een bijzondere aanwijzing.

De *tweede lijn* wordt, naast de beveiligingsfunctionarissen, gevormd door de AVG-coördinatoren binnen de dienstonderdelen. Deze functionarissen fungeren als privacy officers. De AVG-coördinator wordt in veel gevallen bijgestaan door een jurist. De AVG-coördinator coördineert de uitvoering van de AVG en de specifieke wetgeving binnen het dienstonderdeel als ook de feitelijke handelingen die daarvoor nodig zijn. Begin 2023 zal ook een centrale privacycoördinator bij de Bestuursstaf worden aangesteld. Een centrale AVG-coördinator in de rol van een CPO op dit moment niet aanwezig binnen het ministerie. Doordat een centrale AVG-coördinator niet binnen de organisatie aanwezig is, ontbreekt op dit moment een wezenlijke centrale schakel in de privacy-organisatie die mede beleidsmatige verantwoordelijkheid neemt voor het signaleren, het behandelen en implementeren van organisatiebrede privacyvraagstukken en om te komen tot een algemene kennisoverdracht. Ook lijkt de *Directie Juridische Zaken*,

gelet op hetgeen in de interviews naar voren is gebracht, een adviseursrol in te nemen die passend is bij de taakuitoefening binnen de tweede lijn.

De *derde lijn* is het *interne toezicht* dat op grond van de AVG is belegd bij *de FG*. De AVG verbindt eisen aan de positionering van een FG. Zo ziet de FG onafhankelijk toe op de naleving van de AVG in de betreffende organisatie en heeft de FG toegang tot het bestuur van de organisatie.

De FG is binnen de organisatie zodanig gepositioneerd dat dit recht doet aan de positie die de FG op grond van de AVG dient te bekleden. De FG heeft toegang tot de AVG-beheerders, de Secretaris Generaal en de minister (als verwerkingsverantwoordelijke). Daarnaast hanteert de FG een systematiek van toezichtjaarplannen en toezichtjaarverslagen.

De overlegstructuur binnen dit ministerie is als volgt. Er is een AVG-coördinatoren overleg, waarbij ook de FG's aanzitten. In dit overleg vindt kennisoverdracht plaats en worden activiteiten afgestemd. De verwachting is dat zodra de rol van CPO is ingevuld er een breder privacy platform zal worden ingericht, waarbij bijvoorbeeld ook Wpg functionarissen en stafjuristen aansluiten. Vanuit de FG en de FG in het kader van de Wet politiegegevens wordt jaarlijks de week van de beveiliging & privacy geïnitieerd ten behoeve van de privacybewustwording. De themaweek is bedoeld voor AVG-coördinatoren, AVG-aanspreekpunten en beveiligingsfunctionarissen. Daarnaast vinden separate overleggen met AVG-beheerders en AVG-coördinatoren plaats zonder structureel karakter.

Uit de interviews komt naar voren dat een CPO wordt gemist. De FG wordt mede daardoor vaak in de rol van adviseur op de meer AVG-beleidsmatige thema's gemanoeuvreerd, waardoor de FG onvoldoende in staat wordt gesteld om de interne toezichtrol op toereikende wijze in te vullen. Vanuit de eerste lijn wordt een functionaris gemist die AVG-beleidsstandpunten kan verwoorden en op beleidsmatig vlak richting kan geven. In de praktijk blijkt volgens de geïnterviewden dat bij de eerste lijn vaak veel vragen leven over de taakuitoefening in relatie tot de verwerking van persoonsgegevens, maar dat de eerste lijn vaak niet weet hoe te acteren. De eerste lijn voelt zich daarin niet altijd gehoord, waardoor escalatie naar boven in de lijn moeizaam verloopt.

Inbedding privacy in de organisatie

De FG brengt jaarlijks een toezichtsjaarverslag aan de minister uit over de naleving van de AVG. Hetgeen leidt tot voornemens om de gedane aanbevelingen op te volgen. De opvolging daarvan lijkt in de praktijk echter onvoldoende handen en voeten te krijgen. Er wordt geen integraal beleid opgesteld om de aanbevelingen om te zetten in acties en deze in de hele organisatie door te voeren. In de interviews wordt de verwachting uit gesproken dat met de komst van een CPO de opvolging van de aanbevelingen en de zorg voor gegevensbescherming binnen de organisatie beter wordt opgepakt.

Uit de interviews komt het beeld naar voren dat het privacybewustzijn binnen de organisatie relatief laag is. Als gevolg van een incident dat zich heeft voorgedaan, is er bij de dienstonderdelen wel een grotere alertheid ontstaan waar het gaat om de vraag of er een grondslag is om persoonsgegevens te mogen verwerken. Volgens de geïnterviewden leidt dat tot een kramp bij medewerkers. De verwerkingsgrondslag is vanwege dat incident een terugkomend thema in overleggen. Vervolgens is voor de beheerders niet altijd duidelijk wie bepaalt wat er wel en niet binnen de kaders van de AVG mogelijk is.

Het bewustzijn over hoe bijvoorbeeld moet worden omgegaan met een verloren laptop is hoog. Dit bewustzijn lijkt echter vooral voort te komen uit de naleving van andere geldende strenge veiligheidsnormen en niet zozeer uit het bewustzijn over de AVG op dat vlak.

Praktijk

Opleiding en training

Het vergroten van bewustzijn over de AVG ligt niet alleen bij de FG, maar is ook een taak van de AVG-beheerders. Bij hen ligt de eerste verantwoordelijkheid om de verplichtingen op grond van de AVG breed uit te dragen. Dit wordt binnen de organisatieonderdelen opgepakt door het organiseren van interne cursussen die afgestemd zijn op de specifieke doelgroep. Ook vanuit de FG worden jaarlijks opleidingen georganiseerd om het AVG- bewustzijn te vergroten. Uit de interviews komt naar voren dat het vergroten van de kennis en bewustzijn tijd vergt. Dit heeft te maken met het gevoerde personeelsbeleid dat maakt dat medewerkers en ook leidinggevenden veelal maar enkele jaren in een functie zitten om vervolgens te rouleren naar een ander organisatieonderdeel.

In het kader van opleiding en training wordt opgemerkt dat het behulpzaam zou zijn, indien Rijksbreed opleidingen en instructies voor handen zouden zijn, waarbij de ministeries kunnen aansluiten. Het ontbreken daarvan wordt gezien als een groot gemis.

Processen

DPIA's

Een DPIA wordt geïnitieerd:

a. door de proceseigenaar van een IT-dienst bij de ontwikkeling van een IT-dienst waarmee verwerking van persoonsgegevens is gemoeid die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen; of

b. door de betrokken beleidsdirectie bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien.

De DPIA wordt conform het Model gegevensbeschermingseffectbeoordeling rijksdienst uitgevoerd. Na het doorlopen van de DPIA wordt het advies ingewonnen van de FG.

Een DPIA wordt uitgevoerd binnen het dienstonderdeel, waarbij de privacycoördinator een coördinerende rol speelt. Waar op grond van de AVG een DPIA voorafgaand aan de verwerking wordt uitgevoerd, wordt doorgaans een DPIA pas opgesteld wanneer de activiteit, waarvan de verwerking onderdeel uitmaakt, is gestart. Bij het uitvoeren van een DPIA streeft de organisatie ernaar om de DPIA conform de AVG eerder in het proces uit te voeren. Op dit moment wordt te laat de vraag gesteld of en welke persoonsgegevens worden verwerkt en of de verwerking risicovol is. De rol van de FG bij het DPIA-proces lijkt meer op de achtergrond te zijn en wordt omschreven als vrij theoretisch. Dit lijkt samen te hangen met het feit dat de FG niet gaat over beleidsstandpunten.

De DPIA's zien op zowel nieuwe als reeds bestaande verwerkingen. DPIA's op bestaande verwerkingen worden gedaan, indien bijvoorbeeld een nieuwe techniek wordt toegepast. Soms worden ook DPIA's uitgevoerd in de inkoopfase.

Register van verwerkingsactiviteiten
De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende verwerkersovereenkomst en de DPIA. De AVG-coördinatoren zorgen voor de registratie van de verwerkingsactiviteiten en het actueel houden van dit register.

Datalekken
De AVG-regeling legt de verantwoordelijkheid voor het melden van een datalek bij de AVG-(onder)beheerder dan wel de AVG-coördinator. Een kopie van de melding wordt naar de FG gezonden. De alertheid om dergelijke incidenten op te pakken is hoog vanwege de geldende veiligheidsnormen. Ook vanuit de top is hier veel aandacht voor. Op dergelijke incidenten wordt dan ook direct actie ondernomen.

Weging belangen, waaronder privacy
Binnen dit ministerie wordt geworsteld met de bestaande wettelijke taken en de actuele noodzaak om bepaalde activiteiten te ontplooien die niet binnen die wettelijke taken vallen. Gezocht wordt naar een mogelijkheid om recht te doen aan die actuele noodzaak, nu volgens de geïnterviewden de wetgeving op dit vlak achterblijft. Daarbij richt het ministerie zijn blik op de inzet van de rechtsgrond gerechtvaardigd belang. Dit geeft volgens de geïnterviewden het ministerie de mogelijkheid om verwerkingsactiviteiten te ontplooien, waarvoor een grondslag in wetgeving ontbreekt. Onduidelijk voor het ministerie is wel of op grond van de AVG gerechtvaardigd belang kan worden ingezet. Overheidsinstanties mogen op grond van artikel 6, eerste lid, AVG in het kader van de uitvoering van hun taken zich namelijk niet baseren op de rechtsgrond gerechtvaardigd belang bij de verwerking van persoonsgegevens. Overheidsinstanties kunnen andere verwerkingen die raken aan de bedrijfsvoering wel baseren van de rechtsgrond gerechtvaardigd belang. De vraag is echter volgens de geïnterviewden hoe ver die ruimte die de AVG geeft, reikt. Uitleg door bijvoorbeeld het ministerie van Binnenlandse Zaken of de AP over de reikwijdte van de rechtsgrond gerechtvaardigd belang op dit punt zou volgens de geïnterviewden gewenst zijn.

Controle en toezicht

Zie toelichting derde lijn van de *three lines of defence*.

Uitdagingen

De tweede lijn moet beleidsmatig en in de praktijk worden uitgewerkt en versterkt. Dit begint met het aanstellen van een centrale privacy-coördinator. In de regeling is het aanwijzen van een AVG-coördinator een kan-bepaling en daarmee een keuze van de AVG-beheerder. Het is aan te raden om het hebben van een dergelijke coördinator te verplichten en de keuze te laten of er een of meerdere AVG-coördinatoren per dienstonderdeel worden aangewezen. Daarnaast kan in regeling het hebben van een CPO worden geëxpliciteerd.

De privacyvolwassenheid van de eerste lijn is wisselvallig. De eerste lijn worstelt met AVG-vraagstukken en voelt zich onvoldoende gehoord door de beleidsverantwoordelijken. Het ontbreken van een CPO lijkt zich hier te wreken. Een verdere inbedding van het juist doorlopen van het DPIA-proces dient vanuit de eerste lijn prioriteit te krijgen. Dit begint met het

onderkennen van het belang van het 'nulgesprek'. Een gesprek voorafgaande aan het ontwikkelen van een nieuwe verwerkingsactiviteiten waarin alle belangen, waaronder gegevensbescherming, besproken worden. Dit vergt wel dat de juiste mensen op het juiste moment met elkaar in gesprek gaan. Doordat de jaarlijkse bevindingen van de FG, ondanks voornemens daartoe, onvoldoende opvolging krijgen, lijkt uitgestraald te worden dat aan de AVG onvoldoende belang wordt toegekend. Dit is niet behulpzaam bij het verbeteren van de privacyvolwassenheid in de organisatie.

Analyse

Het volwassenheidsniveau op het gebied van privacy van de organisatie is laag. Er lijkt in de dagelijkse praktijk – ondanks de investeringen die op het vlak van scholing worden gedaan – onvoldoende kennis te zijn van de normen uit de AVG. Richtinggevend beleid op dat vlak is onvoldoende ontwikkeld. Dit lijkt mede samen te hangen met het ontbreken van een centrale privacy-coördinator, waardoor de tweede lijn in de three lines of defense niet tot wasdom komt. Ook de omstandigheid dat de jaarlijkse bevinden van de FG onvoldoende opvolging krijgen, lijkt aan het verbeteren van de privacyvolwassenheid niet bij te dragen.

Dimensies van spontane naleving

Kennis van regels
Er wordt ingezet op scholing van medewerkers over het belang van naleving van de AVG. Hiervoor worden zowel algemene als meer toegesneden opleidingen aangeboden, zowel vanuit de privacy-organisatie per organisatieonderdeel alsook vanuit de FG. Vanwege het rouleren van medewerkers en leidinggevenden vergt het vergroten van kennis tijd.

Bij het ontbreken van een CPO wordt de adviesrol van de tweede lijn niet centraal ingevuld, waardoor richtinggevende beleidsstandpunten door de eerste lijn worden gemist. Dit staat de verdere groei van de privacyvolwassenheid van de eerste lijn in de weg.

Kosten en baten
De AVG staat in de dagelijkse praktijk onvoldoende op het netvlies bij de medewerkers. Ook lijken de vaardigheden te ontbreken om privacyvragen te herkennen en tijdig onder de aandacht te brengen van de tweede en in de praktijk vooral de derde lijn. Ook komt het voor dat verwerkingen en daaraan gerelateerde AVG-risico's niet of te laat onder de aandacht van de Secretaris-Generaal of de minister worden gebracht dan wel dat privacyrisico's onvoldoende worden onderkend.

De organisatie ondervindt een spanningsveld tussen het belang van de bescherming van persoonsgegevens en het belang van het garanderen van de nationale veiligheid. De organisatie ervaart op dat vlak handelingsverlegenheid doordat een wettelijke taak ontbreekt om bepaalde verwerkingsactiviteiten te ontplooien die noodzakelijk worden geacht om de primaire taak te kunnen uitoefenen. De organisatie zoekt binnen de kaders van de AVG naar oplossingen en is daarbij geneigd om de juridische grenzen op te zoeken.

Mate van acceptatie
De privacyvolwassenheid van de organisatie wordt als relatief laag gekwalificeerd. De normgetrouwheid lijkt vooral voort te komen uit een correcte naleving van andere normen dan

AVG-normen. Zo is de organisatie alert op inbreuken op de verwerking van persoonsgegevens (datalekken). Dit wordt echter niet primair ingegeven door de AVG, maar door veiligheidsnormen die op basis van andere wettelijke verplichtingen op de organisatie rusten.

Maatschappelijke controle

De Tweede Kamer heeft vanuit haar taak vanzelfsprekend invloed op de besluitvorming die binnen het ministerie plaatsvindt, waarbij de verwerking van persoonsgegevens een rol speelt. Aan wensen, geuit door de Tweede Kamer, wordt door het ministerie niet zonder meer invulling gegeven. Soms kan dit niet vanwege beperkingen die uit de AVG voortvloeien. Bijvoorbeeld omdat de grondslag op grond van de AVG ontbreekt. Indien dit zo is, wordt dit door de minister teruggegeven aan de Tweede Kamer. Op basis van de interviews ontstaat het beeld dat de Tweede Kamer zich doorgaans bewust lijkt te zijn van de eigen positie omtrent de naleving van de AVG. Het belang van de bescherming van persoonsgegevens wordt steeds nadrukkelijker bij de standpuntbepaling en besluitvorming betrokken.

Handhavingsdimensies

Toezicht en handhaving vindt vooral plaats door middel van intern toezicht. De AP speelt bij de naleving van de AVG niet direct een rol en staat op afstand. Uit de interviews komt het beeld naar voren dat ervaren wordt de AP onvoldoende kennis heeft van het werkveld van de organisatie. Ook ontbreekt een vast aanspreekpunt.

Bijlage 6: Uitvoeringsorganisatie 1

Inleiding

In deze tekst beschrijven we de situatie met betrekking tot naleving van de AVG door een agentschap. Dit agentschap verwerkt persoonsgegevens voor de eigen organisatie, maar het zwaartepunt van de verwerking van persoonsgegevens ligt in de verzamelde gegevens voor relatiebeheer in het kader van inspecties en toezicht. Het agentschap is zelf geen bestuursorgaan, en heeft als zodanig ook geen eigen FG. Het privacybeleid is deels gecentraliseerd onder het departement en vervolgens binnen de eigen organisatie doorvertaald en passend gemaakt voor de eigen situatie.

In deze casestudy zijn gesprekken gevoerd met twee medewerkers van de interne auditdienst, de CPO van de uitvoeringsorganisatie, de CPO van het ministerie waar de organisatie onder valt en de FG van dit ministerie. Ook is het departementale privacybeleid bestudeerd.

Gegevensverwerking door de organisatie

Het agentschap verwerkt op grote schaal gegevens voor het onderhouden van contacten met betrokkenen, het voorbereiden van inspecties, onderzoeken en monitoring van bepaalde economische activiteiten. Ook is er in een aantal gevallen sprake van deling van gegevens met andere organisaties. Soms worden binnen het agentschap gegevens verwerkt op basis van wet- en regelgeving die onder de Wpg valt.

Het agentschap is ook een grote werkgever met meer dan duizend werknemers, waarvan ook gegevens worden verwerkt ten behoeve van personeelszaken en dergelijke.

Interne organisatie

Beleid

Het privacybeleid dat zicht richt op het agentschap is op departementaal niveau vastgesteld. Het is geschikt als beleid voor alle directies, uitvoerende organisaties en agentschappen, maar kan ook als raamwerk worden gebruikt indien een decentraal opgesteld privacybeleid de voorkeur heeft. In dit specifieke geval is dit niet gebeurd, en is het centrale beleid dus van toepassing op het agentschap. Naast dit document is de rijksbrede Handreiking Naleving AVG van toepassing, waarin het normen- en toetsingskader voor privacy is vastgelegd.

In het document wordt de scope waarop het beleid van toepassing is gedefinieerd, wordt de relevante wet- en regelgeving benoemd, worden de privacy-uitgangspunten gedefinieerd en wordt de governancestructuur beschreven, inclusief de verschillende rollen die bestaan en de overlegstructuren die tussen deze rollen zijn opgezet.

Deze uitgangspunten zijn in grote mate gebaseerd op de principes die vrijwel altijd worden aangehaald. Hierbij valt te denken aan verwerking conform de privacywetgeving, transparantie, waarborging van rechten van betrokkenen en borging van beveiliging. In het beleid is ook expliciet opgeschreven dat binnen het departement *privacy by design* wordt toegepast, en dan ook in het bijzonder bij projecten met een grote ICT-component.

Uit de interviews is gebleken dat de praktijk bij de bestudeerde organisatie nog niet aansluit bij de ambities zoals die in het beleid zijn beschreven. De naleving van AVG en vooral het werken volgens het principe van *privacy by design* is in de praktijk nog niet vanzelfsprekend. Hiervoor is een aantal oorzaken specifiek benoemd. Zo wordt er gebruik gemaakt van IT-systemen die voor de inwerkintreding van de AVG ontworpen zijn, waardoor de scheiding van gegevens verwerkt onder AVG dan wel Wpg nog niet voldoende is. Dit is gesignaleerd door interne privacytoezichthouders, maar nog niet opgelost. Ten tweede is geconstateerd dat er persoonlijke verschillen in opvattingen over de naleving van AVG bestaan, ook binnen afdelingen en diensten. Er lijkt nog niet één lijn gekozen te zijn voor bepaalde onderwerpen, waardoor soms discussie blijft bestaan over de interpretatie en bewegingsvrijheid omtrent AVG-voorschriften. Een derde factor die van belang is, is dat er soms grote druk op de organisatie staat binnen de primaire processen, waardoor de aandacht voor privacyvraagstukken er soms bij inschiet.

Privacy-organisatie

De privacygovernance binnen het departement is gebaseerd op het concept van *three lines of defence*, zoals dat vaker wordt toegepast. Hierbij is het lijnmanagement verantwoordelijk voor strategisch beleid, risicobeheersing en het borgen van de naleving van privacywetgeving. De tweede lijn wordt gevormd door het 'CIO-stelsel', met aan het hoofd de CIO, een centraal aangestelde functionaris. De derde lijn wordt gevormd door interne toezichthouders van het departement en de Auditdienst Rijk. De FG maakt expliciet geen onderdeel uit van deze derde lijn. De gedachte hierachter is dat het departement de naleving van de AVG en Wpg zonder advies of toezicht van de FG correct uit wil (kunnen) voeren.

In het privacybeleid wordt een aantal rijksbrede en departementale functionarissen benoemd, met daarbij hun takenpakket. Zo wordt de Privacy Adviseur Rijk als coördinator en adviseur bij rijksbrede privacyvraagstukken genoemd. Op departementaal niveau is de CIO belast met ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringsbeleid en met de ontwikkeling en het beheer van de informatiesystemen conform dit beleid. Hiertoe is een departementaal CIO-stelsel ingericht, waarin niet alleen een CIO-office een plaats heeft, maar ook decentrale CIO's die binnen organisatieonderdelen zijn gepositioneerd. De CIO ontwikkelt beleid dat voldoende aandacht schenkt aan onder meer privacy en informatiebeveiliging.

Ook voor de privacy officers geldt dat er een departementale CPO is aangesteld, en daarnaast ook CPO's bij organisatieonderdelen. Deze zijn gezamenlijk verantwoordelijk voor het ondersteunen van lijnmanagement bij implementatie en naleving van privacybeleid. De taken van de CPO zijn in het beleid niet-limitatief opgesomd, en hierbij wordt onder meer genoemd: ontwikkeling, coördinatie van privacybeleid en ondersteuning bij implementatie en naleving, het opzetten van het CPO-stelsel, monitoring van privacyrisico's, monitoren van (en ondersteunen bij) het vergroten van bewustzijn met betrekking tot privacy, het ontwikkelen en

coördineren van gegevensbeschermingsactiviteiten en het ondersteunen en adviseren van diverse actoren zoals de CIO-organisatie en interne auditors zoals de ADR en de Algemene Rekenkamer.

De FG is zoals gezegd geen onderdeel van een van de *three lines of defence*, maar is een onafhankelijke, interne adviseur en toezichthouder. In het privacybeleid wordt zijn rol beschreven conform de artikelen 37 t/m 39 van de AVG. Hij moet onder meer de ambtelijke leiding, diensthoofden en medewerkers adviseren en informeren, toezien op naleving van de AVG en de Wpg (dit is bij het departement samengebald in één persoon), adviseren over DPIA's en toezien op de uitvoering ervan, en fungeren als contactpersoon naar zowel burgers en medewerkers als naar de AP. Ook dient hij te overleggen met FG's van andere departementen. In de praktijk van het bestudeerde agentschap staat de FG dus behoorlijk op afstand van die organisatie. De lijnen lopen in dit geval via de departementale CPO en de decentrale privacy officers.

Het agentschap beschikt over een eigen CPO en privacy officers. De CPO vertaalt het departementale privacybeleid naar de eigen organisatie en is verantwoordelijk voor de dagelijkse afhandeling van privacyzaken. De CPO en privacy officers fungeren als vraagbaak voor het lijnmanagement voor vragen op dit gebied, en kunnen daarvoor overleggen met gespecialiseerde juristen. Ze monitoren mogelijke privacyrisico's en adviseren hierover aan het management. Voor de uitvoering van het werk schakelen ze met privacyfunctionarissen binnen diverse onderdelen van de organisatie. Hierbij is geen sprake van een hiërarchische relatie, maar van een coördinerende rol richting het departement en andere overheidsorganen.

Tot slot zijn er binnen het departement juridische adviseurs die als taak hebben om te adviseren bij beleidsvorming, wetgevingsprocessen en besluitvorming op het gebied van privacy.

In het beleid is op drie niveaus beschreven welke overleggremia er zijn: interdepartementaal, concernbreed en op dienstenniveau. Op concernbreed (departementaal) niveau is sprake van meerdere structurele overleggen tussen functionarissen op het gebied van onder meer privacybeleid, privacygerelateerde juridische zaken en datalekken. Welke overlegvormen op dienstenniveau moeten bestaan is verder niet ingevuld en dus aan de diensten zelf overgelaten. Door de FG wordt het privacyplatform op departementaal niveau als belangrijk gremium aangeduid. Dit platform vergadert structureel over actuele zaken en hulpvragen vanuit verschillende organisaties binnen het departement.

Hoewel de privacy-organisatie in het beleid goed is vastgelegd en breed is belegd bij diverse actoren, blijkt dat het voornemen om decentrale privacy officers bij diverse afdelingen te plaatsen op praktische problemen stuit. Om diverse redenen, waaronder onzekerheid over de invulling van de rol van privacy officer, is een groot aantal functies van privacy officers vacant. Hierdoor zijn de op papier uitgedachte overleg- en sturingslijnen onder druk komen te staan. Hiermee is het voorgenomen proces vertraagd om met de inwerkingtreding van de AVG ook een volwaardige privacy-organisatie met contactpunten in alle onderdelen van de organisatie te beschikken. De rol van privacy officer wordt nu vaak ingevuld door mensen die weinig expertise hebben in dit kennisgebied. Dat heeft tot gevolg dat bijvoorbeeld bij het opstellen van verwerkersovereenkomsten vaak specifieke kennis ontbreekt en meer dan beoogd gebruik wordt gemaakt van tweedelijns privacyfunctionarissen.

Overigens heeft dat in de praktijk niet tot problemen ten aanzien van de naleving van de AVG geleid. Veel processen verlopen naar tevredenheid. Bij een audit is geconstateerd dat dit ook

in grote mate komt omdat mensen in de lijn zonder duidelijke sturing toch goed conform de AVG werken (onbewust bekwaam). Het geconstateerde probleem bestaat er vooral uit dat die momenteel goed uitgevoerde processen niet overal geborgd zijn, en dat met de eventuele veranderingen van personeel de naleving van AVG alsnog onder druk kan komen te staan omdat nieuwe medewerkers niet persé dezelfde werkwijze ten aanzien van gegevensverwerking hanteren.

Inbedding privacy in de organisatie

Zoals gezegd heeft de FG van het departement een rol op afstand van de privacy-organisatie. De adviserende rol is beperkt, in die zin dat ook voor intern advies en toezicht nog andere functionarissen in stelling zijn gebracht. Doordat de FG op departementaal niveau is gepositioneerd, is bovendien zijn onafhankelijkheid binnen de diensten goed geborgd.

In het beleid is ook vastgelegd hoe beleidsdocumenten (van strategisch tot uitvoerend) tot stand komen en hoe de verschillende privacyrollen daarbij betrokken worden. Een afdeling onder aansturing van de CIO coördineert de afstemming op dit vlak, met onder meer de FG maar ook met andere stakeholders.

Praktijk

Opleiding en training

Op het gebied van het privacybewustzijn wordt jaarlijks een meting uitgevoerd, die verplicht is voor alle medewerkers. Bij deze meting worden vragen gesteld over privacy en informatiebeveiliging. Dat levert een beeld op van het algemene niveau van kennis. Mocht het kennisniveau onvoldoende zijn, dan kunnen de CPO en privacy officers maatregelen respectievelijk adviseren om hierin verbetering aan te brengen. Op het intranet is een informatiepagina over privacy ingericht waar ook kennis wordt gedeeld.

Vanuit het CIO-office worden cursussen aangeboden op het gebied van privacy. Het gaat dan om basistrainingen over de AVG tot aan cursussen die specifiek voor privacy officers zijn ontwikkeld. De basiscursus wordt intern gegeven, waardoor het ook beter mogelijk is om feedback vanuit de organisatie op te halen over het kennis- en begripsniveau van de medewerkers. Voor een aantal cursussen worden ook externe opleiders ingehuurd. Naast deze centraal opgezette cursussen hebben de verschillende diensten, waaronder het agentschap, ook eigen cursussen voor medewerkers die meer toegesneden kunnen zijn op het werk binnen de organisatie. Met enige regelmaat worden proef-phishingmails in de organisatie rondgestuurd om het bewustzijn over de daaraan gerelateerde risico's te vergroten.

Bij aanpassingen van informatiesystemen wordt structureel een beoordeling van de veiligheidsrisico's uitgevoerd, waardoor ook op dit vlak de kennis scherp wordt gehouden. Naar het oordeel van interne auditfunctionarissen van het departement is het bewustzijn bij het agentschap door al deze maatregelen redelijk goed op peil.

Processen

DPIA's

Voor het uitvoeren van DPIA's volgt het agentschap de departementaal voorgestelde processtappen. Er is dus geen specifieke procesbeschrijving voor het agentschap opgesteld. In de

procesbeschrijving wordt eerst beschreven dat moet worden vastgesteld of er sprake is van verwerking van persoonsgegevens, vervolgens worden in een vooronderzoek de risico's van onder meer deze verwerking in kaart gebracht. Bij een groot risico wordt het DPIA-proces opgestart, dat uitmondt in een rapportage die ter advisering wordt voorgelegd aan de FG. Binnen het lijnmanagement (de 'procesverantwoordelijke') wordt de verantwoordelijkheid belegd om eventuele maatregelen te plannen en te implementeren, waarna volgens het principe van de PDCA-cyclus het implementatieplan periodiek wordt geëvalueerd.

In de procesbeschrijving staan de taken en verantwoordelijkheden per rol beschreven. Zo is de proceseigenaar primair verantwoordelijk voor correcte verwerking van persoonsgegevens bij de eigen processen, en als gevolg daarvan ook voor het uitvoeren van de DPIA. Daarvoor wordt de privacycoördinator van de betreffende eenheid ingezet, eventueel met ondersteuning van extra mensen die door de proceseigenaar worden toegewezen. Deze coördinator zorgt voor tijdige uitvoering van de DPIA en het implementatieplan, en voor de vastlegging hiervan in de juiste documentatie. De FG heeft een adviserende rol ten aanzien van verwerkingen en DPIA's. De CPO van het agentschap kan eventueel worden ingeschakeld voor advies over het DPIA-proces en het rapport dat daaruit resulteert.

Vanuit de interviews wordt aangegeven dat de uitvoering van DPIA's in de praktijk goed aansluit op het voorgeschreven proces. De FG heeft binnen het DPIA-proces de vrijheid om zelf te beoordelen in hoeverre een adviserende of een meelezende rol gepast is. In de praktijk heeft dit tot gevolg dat hij niet bij alle DPIA's adviseert, en zich soms alleen op de hoogte stelt van de DPIA-rapportages.

Datalekken
Voor het oppakken van datalekken binnen de eigen dienst heeft het agentschap zelf een procedure ontwikkeld. Mocht er sprake zijn van datalekken die meerdere organisaties of het departement betreffen, dan kan een speciaal team voor datalekken de afhandeling ervan oppakken.

Twee keer per jaar wordt een rapportage opgevraagd bij alle organisaties onder het departement, waarin onder meer wordt gevraagd naar het aantal datalekken. Dit is informatie die al op organisatieniveau wordt verzameld en dus eenvoudig verzameld en doorgespeeld kan worden.

Verwerkersovereenkomsten
Zoals gezegd hebben de privacycoördinatoren in sommige gevallen onvoldoende kennis in huis om zelfstandig de verwerkersovereenkomsten op te stellen, waardoor de tweede lijn vaker dan bedoeld wordt ingeschakeld. Tijdens een interview is ook aangegeven dat het mogelijk niet reëel is dat de benodigde kennis op een dergelijk decentraal niveau in stand wordt gehouden; vaak is er ook sprake van dat het invullen van de rol van de privacycoördinator slechts een klein deel van het takenpakket van de betreffende medewerker betreft. Het is dan niet doelmatig om een duurzaam hoog kennisniveau bij deze functionaris te verwachten. Het is realistischer om ervoor te zorgen dat de privacycoördinator weet wat hij moet vragen, aan wie, en hoe er goed samengewerkt kan worden met de tweede lijn in de privacy-organisatie.

Samenwerking met derden

Ook op dit vlak geldt het departementale privacybeleid. Hierin is vastgelegd dat de grootste zorgvuldigheid en terughoudendheid moet worden betracht bij het verstrekken van persoonsgegevens aan derden. Dit houdt onder meer in dat voordien altijd de rechtmatigheid van de gegevensdeling moet worden getoetst en dat passende afspraken gemaakt moeten worden om de zorgvuldige omgang met persoonsgegevens te borgen.

Processen waarbij sprake is van gegevensdeling of samenwerking worden geregistreerd in het verwerkingsregister, en indien nodig worden samenwerkingsovereenkomsten of -protocollen vastgelegd en in het register opgenomen.

Controle en toezicht

In het privacybeleid zijn meerdere vormen van intern toezicht beschreven. Hierin is vastgelegd dat het departement zelf eindverantwoordelijk is voor het toezicht op de naleving van de AVG. De CIO-afdeling opereert daarbij als *second line of defence*, ondersteund door de CPO die informeert en adviseert over toezicht op de naleving van privacykaders.

De interne toezichthouders van het departement en de ADR worden als *third line of defence* aangeduid. Ook de Algemene Rekenkamer kan onderzoeken uitvoeren die privacy-aspecten kennen, maar dit wordt niet expliciet benoemd in het *three lines of defence*-model.

Het interne toezicht wordt op meerdere manier ingevuld. De eerder beschreven tweejaarlijkse integrale uitvraag ziet (ook) op prestatie-indicatoren op het gebied van privacy, en naar aanleiding hiervan kan eventueel extra monitoring of onderzoek worden ingesteld. De ADR doet jaarlijks een audit van alle organisaties in het departement, en hierbij is privacy en gegevensbescherming een van de thema's.

Op verzoek van de FG kan de ADR worden ingeschakeld om specifieke onderwerpen op het gebied van privacy te onderzoeken en hierin te adviseren. Recent zijn bijvoorbeeld de processen omtrent het gegevensverwerkingsregister doorgelicht en zijn adviezen uitgebracht om hier meer lijn in aan te brengen. Ook is de afhandeling van datalekken bestudeerd. Deze onderzoeken worden over de hele breedte van het departement uitgevoerd. Het feit dat de ADR rapporteert op bestuurlijk niveau wordt door de FG als voordeel gezien, omdat zo indien nodig meer gewicht in de schaal kan worden gelegd. Hierbij kan ook nog om richtinggevend advies worden gevraagd.

De FG is geen onderdeel van de *three lines of defence* maar is intern toezichthouder conform de AVG. Daarmee houdt hij toezicht op de naleving van de AVG en van het vastgestelde privacybeleid. Ook houdt hij toezicht op de uitvoering van DPIA's. De FG kenmerkt zichzelf in de praktijk als toezichthoudend adviseur; de door het FG-team uitgevoerde onderzoeken dienen als input voor audits door andere toezichthouders. De focus van het werk van de FG is daarmee meer komen te liggen op het adviseren bij de totstandkoming van wet- en regelgeving. Als de uitvoering daarvan vervolgens bij het agentschap komt te liggen, dan kan de FG eventueel betrokken zijn bij advisering voor wat betreft gegevensbescherming.

Vanuit de organisatie van het agentschap is er weinig tot geen contact met de AP, afgezien van datalekmeldingen. De FG van het departement heeft wel contact met de AP, maar dat betreft dan vooral wet- en regelgevingsprocessen, niet de uitvoering door het agentschap. De AP heeft aangegeven dat het departement en daarmee het agentschap bovengemiddeld goed

presteren op het gebied van intern toezicht, met name door de structurele inzet van interne audits.

Uitdagingen

De eerste uitdaging van deze organisatie betreft de beleving van het belang van naleving van de AVG. Hierin worden tussen diensten en tussen afdelingen verschillen geconstateerd. Het belang van naleving lijkt samen te hangen met persoonlijke of binnen bepaalde teams gedragen ideeën, en is niet zozeer gebaseerd op een consistent uitgedragen en afgedwongen set van principes. Dit creëert kwetsbaarheid ten aanzien van de naleving van de AVG.

Ten tweede is geconstateerd dat het (tijdelijk) moeilijk is gebleken om de posities van decentrale privacy officers in te vullen en bezet te houden. Als gevolg hiervan zijn taken en verantwoordelijkheden soms tijdelijk elders belegd en soms niet opgepakt, en kan afstemming tussen privacy- en lijnorganisatie niet optimaal ingevuld zijn of worden.

Ten slotte is gebleken dat de kennis van privacycoördinatoren niet altijd is toegerust op de verantwoordelijkheden die zij hebben. Het is de vraag of de in het beleid vastgelegde verantwoordelijkheden reëel zijn, gezien de soms geringe omvang van deze rol binnen elke afdeling. Mogelijk is een herverdeling van verantwoordelijkheden, met meer erkenning van de mogelijkheid tot ondersteuning door privacy officers wenselijk.

Analyse

Dimensies van spontane naleving

Kennis van regels
Er wordt structureel ingezet op scholing van medewerkers over het belang van naleving van de AVG. Hiervoor worden zowel algemene als meer toegesneden cursussen aangeboden. Deze worden niet alleen gevolgd bij het begin van het dienstverband, maar vinden ook structureel en bij herhaling plaats met het oog op het in stand houden van bewustzijn.

Het agentschap valt onder een departement waar een centrale privacy-organisatie is opgezet. Daarmee bestaan uitgebreide mogelijkheden om in overleg te treden met collega's over vraagstukken, om kennis op te doen bij specialisten en – door de schaal van het departement – om expertise op te bouwen en te behouden. Doordat er diverse overlegstructuren bestaan, kan er ook sprake zijn van structurele kennisdeling.

Het feit dat er deels door uiteenlopende opvattingen een aantal privacy officer's zijn gestopt, is een mogelijke indicatie van onduidelijkheid bij het management over de invulling van die rol of over de interpretatie van de AVG in bredere zin. Dit is in de gesprekken verder niet duidelijk toegelicht, maar we kunnen wel constateren dat er in elk geval geen sprake is geweest van een breed gedragen, duidelijk geluid waarin alle betrokkenen zich konden vinden.

De privacy-organisatie is tot in de afdelingen ook gedecentraliseerd. Daar is te zien dat het kennisniveau dat vereist is om de verantwoordelijkheden in te vullen moeilijk in stand te houden is, doordat op het meest decentrale niveau de rol van privacyfunctionarissen klein is in vergelijking met hun gehele functie. Daar is het dus van belang dat de functionarissen de weg weten te vinden naar adviseurs en experts om de privacygerelateerde processen in goede banen te leiden.

Kosten en baten
Een interne toezichthouder constateert dat niet alle maatregelen ter verbetering van de privacy-organisatie in het gewenste tempo worden doorgevoerd, en constateert tegelijkertijd dat dit in belangrijke mate veroorzaakt wordt door tijdsgebrek in de organisatie. Dit duidt erop dat privacygerelateerde maatregelen geen even hoge prioriteit krijgen als de uitvoering van primaire processen.

Hierdoor is de borging van goede naleving van de AVG niet overal optimaal. Overigens leidt dit in de praktijk niet tot problemen; in veel gevallen is er sprake van onbewust bekwame uitvoering van gegevensverwerking en daarmee van AVG-conformiteit.

Voor het vormgeven van processen en het daarbij afwegen van kosten en baten van borging van privacy en gegevensbescherming kan het agentschap putten uit de expertise die op departementaal niveau aanwezig is. Het relatief grote aantal audits van interne toezichthouders zorgt er ook op dit vlak voor dat de inrichting van processen conform AVG geschiedt.

Mate van acceptatie
In het privacybeleid worden de principes van de AVG ten volle onderschreven. In het algemeen kan ook worden gesteld dat deze principes in het agentschap volledig van toepassing worden geacht; eventuele niet naleving van de AVG is niet te wijten aan met de wet strijdige wensen of weerstand tegen de privacywetgeving, maar eerder aan hoge werkdruk en prioriteitsstelling.

Maatschappelijke controle
Het agentschap is niet in publieke belangstelling gekomen naar aanleiding van AVG-gerelateerde kwesties. Dat kan komen doordat de gegevensverwerking voornamelijk een selecte groep direct betrokkenen (geïnspecteerden, ondertoezichtgestelden) betreft, en dat er geen omvangrijke registers zijn opgezet door deze organisatie.

Handhavingsdimensies
Toezicht en handhaving vindt vooral plaats door middel van intern toezicht, door het departement, door de ADR of door de Algemene Rekenkamer. Dit leidt regelmatig tot adviezen voor verbetering, maar doordat er structureel toezicht wordt gehouden is er in het recente verleden geen sprake geweest van extern toezicht of externe handhaving.

Andere relevante punten
Bij deze organisatie is nog niet alles optimaal ingericht. Er is een aantal verbetermogelijkheden geconstateerd door de eigen organisatie, waaraan nu invulling wordt gegeven. Bij het uitvoeren van de analyse van deze casestudy is het van belang om te realiseren dat door de veelvoorkomende interne onderzoeken en audits problemen relatief snel en regelmatig aan het

licht komen in vergelijking met andere organisaties. Daardoor lijkt de organisatie, volgens enkele geïnterviewden, soms wel slachtoffer van het eigen succes.

Bijlage 7: Uitvoeringsorganisatie 2

Inleiding

In dit hoofdstuk beschrijven we een zbo. Deze organisatie verwerkt persoonsgegevens voor de eigen organisatie, maar beheert ook onder andere persoonsgegevens in enkele openbare registers. Als zbo heeft de organisatie een eigen FG en is men zelf verantwoordelijk voor het vaststellen van privacybeleid en daaruit voortvloeiende regelgeving.

In het kader van deze casestudy is gesproken met een directeur, een beleidsadviseur die zich bezig houdt met dataverwerking, de CISO en de FG. De zbo heeft het privacybeleid, het jaarrapport van de FG voor het jaar 2021, een rapport over mogelijke verbeteringen op het gebied van gegevensverwerking, de privacyverklaring en procesbeschrijvingen voor het uitvoeren van DPIA's en het melden van datalekken verstrekt.

Gegevensverwerking door de organisatie

Door de organisatie worden gegevens verwerkt van de eigen werknemers, van personen en instanties die zijn opgenomen in de openbare registers en van de gebruikers van die registers.

Interne organisatie

Beleid

Voor het privacybeleid is enige tijd na de inwerkingtreding van de AVG een document vastgesteld, dat voor de hele organisatie van toepassing is. In dit document worden allereerst de visie op privacy, het juridisch kader en de principes met betrekking tot privacy geformuleerd. In de visie wordt uitgesproken dat men passende maatregelen neemt om persoonsgegevens te beschermen en alleen noodzakelijke gegevens te verwerken.

Een aantal principes met betrekking tot privacy zijn dat medewerkers zelf verantwoordelijk worden geacht voor naleving van de AVG binnen hun werk, en dat managers daarop toezien. Men streeft ernaar volledig transparant te zijn, zowel intern als naar buiten, over de wijze waarop gegevens verwerkt worden en de rechten die betrokkenen daarbij hebben. De persoonsgegevens worden zorgvuldig verwerkt en alleen wanneer dat gerechtvaardigd is.

Bij interviews is gebleken dat de cultuur in de organisatie niet altijd en overal overeenkomt met de ambities zoals geformuleerd in het beleid. Het komt wel eens voor dat opgetekende risico's, door de FG, door privacy-adviseurs of andere medewerkers, niet direct ten volle serieus worden genomen of dat maatregelen om de risico's te mitigeren geen prioriteit krijgen. Er wordt dus soms wat makkelijk gedacht over AVG-vraagstukken. Privacyfunctionarissen moeten issues vaak agenderen, waarna vaak eerst een fase volgt waarin men zich beraadt op maatregelen zonder echt in actie te komen. Pas wanneer er reële nadelen voor de eigen organisatie dreigen (in aanvulling op risico's voor betrokkenen) komt men definitief in beweging. Hierin bestaan overigens grote verschillen tussen afdelingen; er is geconstateerd dat afdelingen met meer ervaren medewerkers over het algemeen zich eerder bewust zijn van de noodzaak tot ingrijpen. Dit bewustzijn is dus gelinkt aan specifieke personen en is niet geborgd in de organisatie en processen.

Privacy-organisatie

De privacy-organisatie is ook beschreven in het privacybeleid, zij het op ietwat impliciete wijze. Het beleid bevat voor dertien privacygerelateerde taken een beschrijving van (mede)verantwoordelijke personen of afdelingen. Er is geen beschrijving gegeven van eventuele overlegstructuren, en de verantwoordelijkheden zijn op hoofdlijnen beschreven.

Het vaststellen van het beleid is belegd bij de bestuurlijk hoofdverantwoordelijke entiteit binnen de organisatie. Deze entiteit stelt tevens de Privacyverklaring vast. Voor beide documenten geldt dat revisies en kleinere wijzigingen onder verantwoordelijkheid vallen van de manager Juridische Zaken, waarbij voor de privacyverklaring input kan worden gegeven door de lijnmanagers.

De afdeling JZ vervult een rol die we bij andere organisaties veelal bij CPO's belegd zien. Deze afdeling geeft advies over de noodzaak van een DPIA bij nieuwe processen, en biedt ondersteuning bij de uitvoering van de DPIA's. Ook het beheer van het verwerkingsregister valt onder verantwoordelijkheid van de manager JZ, waarbij de afdeling ondersteuning biedt aan de lijnafdelingen bij het invullen ervan. Ook met tweedelijns privacyvragen kan de organisatie terecht bij de afdeling JZ, en de manager is verantwoordelijk voor de afhandeling van verzoeken van betrokkenen op grond van de AVG. Eventueel kan de afdeling op verzoek verwerkersovereenkomsten beoordelen.

Het lijnmanagement is primair verantwoordelijk voor correcte naleving van de AVG en als gevolg daarvan onder meer verantwoordelijk voor het doorgeven van proceswijzigingen ten behoeve van de actualisatie van de privacyverklaring. Ten aanzien van DPIA's is de lijnmanager verantwoordelijk voor het controleren van de noodzaak of wenselijkheid ervan, en indien dat

het geval is voor de uitvoering en het controleren van de DPIA. Eventueel te nemen maatregelen vallen ook onder verantwoordelijkheid van de managers. Ook bij het bijhouden van het verwerkingsregister, het op peil brengen van het privacybewustzijn van medewerkers, de opvolging van de documenteerplicht, het vaststellen en realiseren van bewaartermijnen, het zorgen voor verwerkersovereenkomsten en het bewerkstelligen van informatiebeveiliging valt steeds onder verantwoordelijkheid van de lijnmanager.

Bij verschillende taken zijn wel partijen benoemd die in de uitvoering kunnen ondersteunen. Zo is er een compliance-afdeling de opvolging van vanuit DPIA's voortvloeiende maatregelen controleert. Er zijn privacy-ambassadeurs die eerstelijns vragen met betrekking tot privacy verzamelen en doorgeleiden. Voor de registratie en afhandeling van beveiligingsincidenten is er apart team opgezet. De afdeling personeelszaken is verantwoordelijk voor de coördinatie van opleidingen voor het op peil brengen van kennis ten aanzien van privacyvraagstukken. Ten slotte is er een coördinator onder de compliance-afdeling die de informatiebeveiligingsactiviteiten organisatiebreed monitort en toeziet op de uitvoering ervan. In sommige gevallen is er ook een security officer binnen de afdeling aangesteld, die bij informatiebeveiliging kan ondersteunen.

De FG heeft volgens de bovenstaande beschrijving geen directe verantwoordelijkheid bij privacygerelateerde taken. De werkzaamheden van de FG zijn in het beleid apart beschreven. Hij dient onder meer eens per kwartaal aan de bestuursverantwoordelijke entiteit te rapporteren over de stand van zaken omtrent verwerking van persoonsgegevens in de organisatie. Hij signaleert risico's en treedt daarover in overleg met het management, en houdt intern toezicht op naleving van de AVG. Voor veel van de hierboven beschreven taken geldt dat de FG (ook) een rol heeft, met nadruk op advies en ondersteuning en beoordeling van privacyproducten zoals het procedures, registers en beleidsstukken. Ook is hij degene die als aanspreekpunt voor de AP fungeert.

Een aparte rol is weggelegd voor een bestuurder die op strategisch niveau verantwoordelijk is voor de integriteit en kwaliteit van de beheerde openbare registers en de verwerking van data daaruit. Deze functionaris zorgt ervoor dat de gegevens in de registers op een optimale manier benut kunnen worden, binnen de kaders van de AVG. Daarmee ligt in deze rol ook besloten dat grondige kennis van de AVG op strategisch niveau wordt meegenomen.

In de praktijk is gebleken dat de FG zelf een meer of minder betrokken rol kan kiezen al naar gelang de situatie. Het blijkt daarbij wel vaak dat de adviezen van de FG echt als zodanig worden meegenomen; er wordt niet altijd op geacteerd, het komt voor dat de adviezen terzijde worden geschoven of dat maatregelen niet direct worden opgepakt. Hierbij kan een rol spelen dat men de risico's of schade voor betrokkenen waarvan persoonsgegevens zijn verwerkt als beperkt inschat. In combinatie met soms hoge werkdruk kan dit zorgen voor een lagere prioritering van correctieve maatregelen. De capaciteitsproblemen spelen overigens zowel een remmende rol bij de uitvoering van taken, als bij het opzetten en ontwerpen van nieuwe processen. Het privacybewustzijn is wat dat betreft nog niet optimaal, al zien gesprekspartners wel een licht positieve trend hierin.

Inbedding privacy in de organisatie

In het privacybeleid is vastgelegd dat het lijnmanagement voor veel privacygerelateerde taken eindverantwoordelijk is. Daarmee is de inbedding op decentraal niveau geregeld; er is geen sprake van een aparte privacy-organisatie die parallel aan de lijnorganisatie activiteiten

uitvoert. De managers worden wel door diverse actoren ondersteund, geadviseerd en gemonitord.

Op strategisch niveau is er met de aanstelling van de Chief Data Officer (CDO) geregeld dat er iemand direct betrokken is bij de besluitvorming met voldoende kennis van en gevoel voor AVG-vraagstukken.

Praktijk

Opleiding en training

In het privacybeleid is vastgelegd dat naleving van de AVG primair een verantwoordelijkheid van de medewerkers zelf is. Om ervoor te zorgen dat dit goed gebeurt, is er in de organisatie een aantal taken belegd om het bewustzijn op dit vlak te creëren en in stand te houden. Zo worden nieuwe medewerkers ingelicht over het privacybeleid, en wordt dit beleid ook jaarlijks actief gecommuniceerd naar alle medewerkers, onder coördinatie van de afdeling JZ. Door middel van online cursussen worden medewerkers die in hun werk te maken hebben met de verwerking van persoonsgegevens uitgebreider op de hoogte gebracht van de risico's daarin. De manager van de afdeling personeelszaken draagt verantwoordelijkheid voor het opleidingsplan met betrekking tot privacykennis.

Processen

DPIA's

In het privacybeleid is opgenomen dat, als een voortvloeisel uit het *privacy by design*-principe, vooraan in het ontwerptraject van nieuwe activiteiten of processen (of aanpassingen hierin), een check wordt uitgevoerd of een DPIA nodig is. De proceseigenaar (manager) dient hiervoor een checklist te doorlopen en deze voor te leggen aan de adviseurs bij JZ. De checklist is een uitgebreid formulier, waarin wordt nagegaan welke gegevens verwerkt gaan worden, of het een type verwerking betreft waarbij een DPIA altijd verplicht is, of dat er mogelijk andere factoren een rol spelen die een DPIA noodzakelijk maken. Wanneer de JZ-adviseur tot de conclusie komt dat een DPIA inderdaad nodig is, dan volgt een gesprek waarin de vervolgstappen worden besproken. De uitvoering van DPIA en het documenteren ervan is de eindverantwoordelijkheid van de manager.

Minimaal eens per twee jaar moet worden gecontroleerd of de DPIA nog actueel is. Bij wijzigingen in de gegevensverwerking waarop de DPIA van toepassing is, moet weer advies worden ingewonnen bij JZ om te controleren of een wijziging van de DPIA ook nodig is. In het DPIA-rapport is standaard ook een advies van de FG over de betreffende gegevensverwerking opgenomen.

Mocht uit de check volgen dat een DPIA niet nodig is, dan wordt nog wel een document aan de manager gestuurd met daarin de standaardeisen aan gegevensverwerking conform de AVG. Hierin wordt onder meer gesproken over de bewaartermijnen, dataminimalisatie, beveiliging van gegevens en het belang van verwerkersovereenkomsten.

In de praktijk is de DPIA een goed instrument om het privacybewustzijn te vergroten. Lijnmanagers en -medewerkers worden gedwongen goed over privacy na te denken. Toch blijkt ook bij DPIA's vaak dat er verschillen in opvattingen zijn tussen de lijnafdelingen en de privacyspecialisten. Daarbij worden de adviezen van die laatste groep niet altijd als leidend gezien.

Datalekken
Het protocol voor datalekken en de daarbij geldende meldplicht is in een apart document uitgebreid beschreven. Hierin worden per stap in het proces steeds de benodigde acties en de verantwoordelijke partijen benoemd. Na de interne melding is de afdeling JZ verantwoordelijk voor de eerste interpretatie van aard en urgentie, en van de noodzaak tot melding bij de AP. Hiervoor is in een protocol een niet-uitputtende lijst van factoren opgenomen waarbij in elk geval melding bij de AP noodzakelijk wordt geacht. Ook het publiciteitsrisico wordt door hen ingeschat om eventuele maatregelen in gang te zetten. Vervolgens komt de eindverantwoordelijkheid bij de verantwoordelijk directeur te liggen. Deze dient maatregelen in gang te zetten en zorg te dragen voor correcte uitvoering, onderzoek te doen naar oorzaken en benodigde aanpassingen. De afdeling JZ is weer verantwoordelijk voor verdere afhandeling en documentatie, terwijl de FG kan adviseren over het datalek en de maatregelen, en in zijn vaste rapportage melding maakt van het lek. In het document is overigens ook een analyse van datalekgerelateerde risico's opgenomen, waarbij kans, impact en eventuele beheersmaatregelen in kaart zijn gebracht.

In het verleden was de FG meer betrokken bij datalekken, nu is dit hoofdzakelijk bij de afdeling JZ komen te liggen. Hierdoor is de FG meer in de wettelijk bedoelde positie gezet. De FG constateert trouwens dat doordat brieven die door de organisatie worden gestuurd steeds minder onnodige persoonsgegevens bevatten, in de organisatie de impact van eventuele lekken via die weg steeds kleiner wordt ingeschat. Hierdoor lijkt soms ook de *sense of urgency* voor snelle maatregelen minder te zijn geworden.

Verwerkersovereenkomsten
Er is een standaard verwerkersovereenkomst in gebruik waar alleen van kan worden afgeweken als er overleg is geweest met de FG en een security officer. De manager is verantwoordelijk voor de documentatie omtrent eventuele afwijkingen, alsmede voor de overeenkomst zelf. In een bijlage in de overeenkomst worden technische en organisatorische maatregelen door de verwerker beschreven. Deze dienen ook voorgelegd te worden aan de security officer.

Bewaartermijnen
De organisatie voert redelijk standaard beleid ten aanzien van bewaartermijnen. Uitgangspunt is daarbij dat persoonsgegevens niet langer dan noodzakelijk voor de doeleinden waarvoor ze verzameld worden bewaard blijven. De lijnmanager is verantwoordelijk voor de van toepassing zijnde bewaartermijnen, waarbij het Basis Selectie Document als leidraad is gebruikt als basis voor een intern instructiedocument.[86] De bewaartermijnen worden, inclusief onderbouwing, vastgelegd in het verwerkingsregister.

Samenwerking met derden

In het privacybeleid is geen expliciete aandacht geschonken aan gegevensdeling of -verwerking met of door specifieke derde partijen, anders dan de secties die zien op de verwerkersovereenkomsten zoals hierboven beschreven. Ook uit de interviews is niet gebleken dat dit een thema is dat veel aandacht heeft.

[86] Het Basis Selectie Document (BSD) is het bij de Archiefwet 1995 voorgeschreven selectieinstrument voor overheidsarchieven.

Controle en toezicht

In het privacybeleid is vastgelegd dat de FG als intern toezichthouder toeziet op de verwerking van persoonsgegevens en de naleving van zowel privacywetgeving als intern beleid, alsmede op de uitvoering van DPIA's. Daarbij kan hij gebruik maken van het verwerkingsregister.

Als onderdeel van deze verantwoordelijkheid stelt de FG jaarlijks een rapportage op. Hierin komt onder meer aan bod:

- de stand van zaken met betrekking tot datalekken en trends daarin, inclusief meldingen aan de AP;
- de ontwikkelingen met betrekking tot externe en interne vragen die aan de FG zijn voorgelegd;
- de stand van zaken omtrent privacybewustzijn;
- de afhandeling van verzoeken op basis van rechten van betrokkenen, met daarbij ook trends over de jaren en de afhandeltermijnen van deze verzoeken;
- toelichting op de inzet van DPIA's en het gebruik van het verwerkingsregister;
- toelichting op overige belangrijke interne en externe ontwikkelingen omtrent privacy, zoals politieke ontwikkelingen en externe beeldvorming van de organisatie voor wat betreft privacy.

In de praktijk is duidelijk geworden dat de FG vooral vanuit een adviesrol opereert, en dus geen absolute doorzettingsmacht heeft. Zoals eerder beschreven onder de kopjes privacybeleid en -organisatie is naleving van de AVG in de regel één van de belangen die in overwegingen wordt meegenomen, en worden ook adviezen van de FG niet als direct op te volgen instructie geïnterpreteerd.

Extern toezicht vindt plaats vanuit de AP, waarbij de FG de contactpersoon is en indien gewenst samenwerking opzet bij het uitvoeren van toezichtstaken. De AP kan het verwerkingsregister opvragen, en ontvangt indien nodig meldingen van datalekken conform het daarvoor opgestelde interne beleid. De organisatie heeft in het verleden ook regelmatig overleg gehad over beleidsmatige keuzes.

Uitdagingen

Bij deze organisatie is gebleken dat een voorname kwetsbaarheid met betrekking tot naleving van de AVG zit in de cultuur van omgang met wetgeving en intern beleid. Bij de overwegingen tussen doelmatige uitvoering van taken, of het tijdig opstarten van nieuwe processen, is naleving van de AVG doorgaans een factor die in belangenafwegingen wordt meegenomen. Het is dan geen topprioriteit, en afhankelijk van specifieke personen in het lijnmanagement wordt aan adviezen en waarschuwingen van privacyfunctionarissen een prioriteit toegekend. Daarbij wordt er nogal eens voor gekozen om eerst primaire processen op orde te krijgen alvorens aandachtspunten op het gebied van privacy worden opgepakt. Dit proces is dus niet geborgd in processen en het uitgangspunt van eigen verantwoordelijkheid zorgt voor verschillen tussen afdelingen en eenheden in de daadkracht die hierbij wordt betracht.

Daarbij is geconstateerd dat beperkte capaciteit op de werkvloer een negatief effect kan hebben op de aanpak van privacygerelateerde aandachtspunten. Daar waar de menskracht

beperkt is, krijgen de uitvoering en het opzetten van primaire processen op een doelmatige manier prioriteit, en pas als dat voltooid is wordt gekeken naar aanvullende stappen ten behoeve van dit thema.

Analyse

Dimensies van spontane naleving

Kennis van regels
Zowel bij aanvang van het dienstverband als periodiek worden medewerkers geschoold om kennis van de regels op peil te brengen en te houden. Daarnaast wordt ook het DPIA-proces gezien als een middel om het bewustzijn met en denken over privacy-aspecten van de bedrijfsvoering te versterken. Op strategisch niveau is sinds kort een CDO aangesteld, waarmee het bewustzijn en de kennis over het thema privacy op dit niveau heeft gestimuleerd.

Kosten en baten
De cultuur binnen de organisatie werkt in de hand dat de naleving van de AVG en de daarvoor benodigde maatregelen geregeld uitgesteld worden, ten behoeve van het sneller en doelmatiger opzetten van processen en uitvoeren van primaire taken. Er wordt wat dit betreft regelmatig een trade-off ervaren, in plaats van dat de naleving van de AVG als integraal onderdeel van de taakuitvoering betreft. Hierbij speelt mee dat de capaciteit niet altijd beschikbaar is om direct maatregelen te nemen wanneer privacyfunctionarissen daartoe adviseren. Volgens de FG ontbreekt soms de *sense of urgency*, en pas wanneer er ook daadwerkelijk risico's dreigen voor de eigen organisatie (bijvoorbeeld in de vorm van reputatieschade) komt hier systematisch verandering in en wordt de noodzaak meer gevoeld.

Mate van acceptatie
Er is niet geconstateerd dat de normen vanuit de AVG niet geaccepteerd worden. Voor zover de naleving van de AVG (of daartoe benodigde maatregelen) niet direct wordt opgepakt, is het vooral een kwestie van prioriteit. Het beleid is dan ook volledig in lijn met de AVG, en de organisatie is hier ook goed op ingericht. Ook op strategisch niveau worden de normen geaccepteerd en doorgaans ook goed (en de laatste jaren steeds beter) uitgedragen naar de organisatie.

Handhavingsdimensies

Over de vermeende inbreuken op de AVG is uitvoerig overleg gepleegd met de wetgever en de AP. Hier is uiteindelijk uitgekomen dat er geen strafmaatregelen opgelegd hoefden te worden. De organisatie is zich wel voortdurend bewust van het spanningsveld tussen taakuitvoering en privacywetgeving.

Er is goed contact met de AP, er zijn vaste aanspreekpunten waartussen uitgebreid en zo nodig ad hoc contact is. Dit betreft vooral beleidsmatige vraagstukken op strategisch niveau. Voor reguliere contacten zoals het melden van datalekken worden de normale procedures gevolgd zoals die bij de AP van kracht zijn.

Bijlage 8: Caseverslag uitvoeringsorganisatie 3

Inleiding

In deze casebeschrijving staat de praktijk van de naleving door een zelfstandige uitvoeringsorganisatie op rijksniveau centraal. In het kader van deze casestudy is gesproken met de centrale privacy officer, twee decentrale privacy officers, de directeur bedrijfsvoering, een manager van een afdeling waarbinnen veel gegevens worden verwerkt en de FG. De uitvoeringsorganisatie heeft het beleid op het gebied van privacy en informatiebeveiliging toegezonden. Dit betreft onder andere een document met betrekking tot de privacygovernance, het gegevensbeschermingsbeleid, het leveranciersmanagementbeleid en het dataclassificatie- en sourcingsbeleid. Ook heeft de uitvoeringsorganisatie diverse werkinstructies, templates en een opleidingsplan verstrekt.

Gegevensverwerking door de organisatie

De gegevensverwerking door de organisatie bestaat uit het bijhouden van enkele registers. Deze registers bevatten onder andere NAW-gegevens en BSN-nummers. In sommige gevallen kunnen deze registers medische en strafrechtelijke gegevens bevatten. De gegevens uit de registers worden gedeeld met andere overheden; het merendeel van de gegevensdeling verloopt geautomatiseerd. De uitvoeringsorganisatie verwerkt daarnaast ook gegevens bij het contact met burgers en als werkgever.

Interne organisatie

Beleid

De uitvoeringsorganisatie beschikt over uitgebreid beleid en werkinstructies op het gebied van privacy. De functies, taken en verantwoordelijkheden zijn uiteengezet in een governancedocument. In dit document zijn ook de richtinggevende principes voor gegevensverwerking door de organisatie uiteengezet. Daarnaast beschikt de organisatie op gegevensbeschermingsbeleid, op grond waarvan nader beleid is geformuleerd voor specifieke onderwerpen, waaronder dataclassificatie, de uitvoering van DPIA's, datalekmeldingen en leveranciersmanagement.

In het kader van de ISO-certificering is een kader vastgesteld met een cyclus van activiteiten voor het beoordelen van privacyrisico's, de maatregelen om deze risico's te mitigeren en het monitoren van de effectiviteit van deze maatregelen.

Privacy-organisatie

De privacy-organisatie bestaat, naast de FG, uit een centrale privacy officer en op elk onderdeel een decentrale privacy officer. De centrale privacy officer heeft een coördinerende rol en houdt zich bezig met onderwerpen die onderdeel-overstijgend zijn. De decentrale privacy officers zijn op de verschillende onderdelen gepositioneerd en zijn daar de eerste adviseurs. Zij worden betrokken bij nieuwe projecten en aanbestedingen en bekijken deze vanuit privacy-oogpunt; ook geven zij antwoorden over privacyvragen vanuit de organisatie.

De privacy-organisatie is gebaseerd op het *three lines of defence*-model. Volgens de privacy-governance wordt de eerste lijn gevormd door de managers van de diverse onderdelen en de decentrale privacy officers. De verantwoordelijkheid voor het identificeren, classificeren, het nemen van beheersmaatregelen en het accepteren van restrisico ligt daarmee bij de verschillende onderdelen. De tweede lijn wordt gevormd door de centrale privacy officer. De tweede lijn is verantwoordelijk voor advisering, beleidsvorming en monitoring op het gebied van privacy. De derde lijn wordt gevormd door de FG.

Tijdens de gesprekken met de centrale privacy officer, decentrale privacy officers en de FG kwam naar voren dat de onderverdeling van drie lijnen ook anders kan. De decentrale privacy officers kunnen bijvoorbeeld ook in de tweede lijn worden gepositioneerd en ook kan worden gesteld dat de FG buiten het *three lines of defence*-model staat, omdat deze zich niet richt op de risico's voor de organisatie, maar op de risico's voor betrokken burgers. De FG geeft ook aan dat de precieze indeling minder relevant is.

Inbedding privacy in de organisatie

De privacy officers zijn ondergebracht bij de afzonderlijke organisatieonderdelen. Dit heeft als voordeel dat de privacy officers dichter bij de werkvloer staan, beter een netwerk kunnen opbouwen en benaderbaar zijn voor medewerkers.

Binnen de uitvoeringsorganisatie zijn daarnaast contactpersonen aangewezen. De contactpersonen zijn medewerkers in de uitvoering die affiniteit hebben met privacy; zij maken geen onderdeel uit van de privacy-organisatie. Het zijn van contactpersoon is geen formele functie, maar de contactpersonen zijn wel van belang voor de informatievoorziening van de decentrale privacy officers en het creëren van bewustzijn binnen hun onderdeel. Tussen de privacy officer en de contactpersonen van een organisatieonderdeel is één keer per maand een gesprek, waarin wordt gesproken over privacyvraagstukken en andere ontwikkelingen binnen het betreffende onderdeel.

Volgens het privacybeleid ontvangt de directie privacyrapportages van de centrale en decentrale privacy officers en van de FG. Deze rapportages worden besproken in een overleg waaraan de directeur bedrijfsvoering, de centrale security officer, centrale privacy officers, de FG, diverse managers en een externe auditor deelnemen.

Praktijk

Opleiding en training

Tijdens de gesprekken komt naar voren dat het van belang is dat medewerkers zich bewust zijn van de privacy-aspecten van hun werkzaamheden. Dit maakt dat zij weten wanneer zij een incident als datalek moeten melden en eerder met vragen naar een decentrale privacy officer

stappen. De FG, centrale privacy officer en decentrale privacy officers merken ook op dat het van belang is dat medewerkers, met name projectleiders, beseffen dat bij nieuwe projecten knelpunten op privacyvlak kunnen ontstaan en dat het om die reden van belang is de privacy-organisatie vroegtijdig bij het proces te betrekken.

Dit bewustzijn wordt binnen de uitvoeringsorganisatie op verschillende manieren ontwikkeld en bijgehouden. Nieuwe medewerkers krijgen een introductietraining die door een privacy officer en een security officer wordt gegeven. Voor alle medewerkers is een e-learning module beschikbaar; een uitgebreidere en verdiepende e-learning module is beschikbaar voor medewerkers die persoonsgegevens verwerken. De uitvoeringsorganisatie streeft naar een deelnemingspercentage aan de modules van boven de 90%; op dit moment zit de organisatie daar nog iets onder. De centrale privacy officer en FG constateren dat na invoering van de trainingen meer meldingen worden gedaan van mogelijke datalekken.

De decentrale privacy officers en contactpersonen vervullen een belangrijke rol bij het creëren van bewustzijn binnen hun organisatieonderdeel. Zij sluiten aan bij teamoverleggen. Dit gebeurt soms op verzoek van het betreffende team, soms moeten hier zelf om vragen.

Processen

DPIA's

In het beleid van de uitvoeringsorganisatie is vastgelegd dat, bij aanbestedingen of nieuwe projecten, de projectmanager een startgesprek plant. Bij dit gesprek is onder andere een privacy officer en een security officer aanwezig. De privacy officer en een uitvoerende medewerker voeren vervolgens samen een quick scan DPIA uit. Als de quick scan daartoe aanleiding geeft wordt een DPIA uitgevoerd. De DPIA is de verantwoordelijkheid van de betreffende proceseigenaar en wordt uitgevoerd door een multidisciplinair team, bestaande uit bijvoorbeeld medewerkers in de uitvoering, ICT-medewerkers, een security officer, privacy officer of een privacycontactpersoon. De privacy officer beoordeelt de DPIA, waarna de FG een finale toetsing doet. De proceseigenaar gaat vervolgens akkoord met de DPIA en wordt daarmee verantwoordelijk voor de restrisico's en het tijdig nemen van de in de DPIA genoemde maatregelen.

De in het beleid beschreven wijze voor uitvoering van DPIA's komt overeen met de praktijk, zo blijkt uit de gesprekken met de centrale en decentrale privacy officers. De centrale privacy officer geeft aan dat de processen en risico's binnen het multidisciplinaire team worden besproken, waarbij ook aandacht is voor dataethiek. Het uitvoeren van een DPIA wordt binnen de organisatie niet als een invuloefening beschouwd. De decentrale privacy officers geven aan dat op dit vlak nauw wordt samengewerkt met security. Ook vindt geregeld overleg plaats met de afdeling inkoop; zodat de decentrale privacy officers op de hoogte blijven van de inkoopactiviteiten van de organisatie.

Datalekmeldingen

Binnen de uitvoeringsorganisatie worden datalekken gemeld aan een datalekteam. Leden van dit team zijn verantwoordelijk voor het doorgeven van de meldingen aan de FG, centrale privacy officer en decentrale privacy officers.

In de gesprekken kwam aan de orde dat na het aanstellen van decentrale privacy officers en het aanbieden van trainingen meer meldingen worden gedaan van incidenten die een datalek zouden kunnen vormen.

Verwerkersovereenkomsten
Op basis van een DPIA worden aanbestedingseisen ten aanzien van security en privacy geformuleerd. Bij definitieve gunning maakt de contractmanager afspraken met een privacy officer en een security officer over het managen van het contract ten aanzien van aspecten rondom privacy en informatiebeveiliging. Gedurende de looptijd van het contract zijn er diverse contractbesprekingen waarin deze aspecten aan de orde komen. De contractbesprekingen wordt door de contractmanager gedaan; bij bepaalde contracten is het wenselijk dat de privacy officier of security officer bij dit gesprek aansluit. Contracten die betrekking hebben op verwerkingen met meer privacyrisico's of waarbij de leverancier de afgesproken maatregelen nog niet heeft geïmplementeerd, worden intensiever gemanaged. Dat houdt in dat door de uitvoeringsorganisatie of in opdracht van de uitvoeringsorganisatie audits kunnen worden uitgevoerd. Het recht om deze controles uit te voeren is in het template voor de verwerkersovereenkomst opgenomen.

Controle en toezicht

Positie FG
De uitvoeringsorganisatie beschikt over een FG die de functie fulltime uitvoert. In het beleid worden de taken en verantwoordelijkheden zoals die volgen uit de AVG uiteengezet en de onafhankelijkheid van de FG benadrukt. Daarnaast is in het beleid vastgelegd dat de FG regelmatig uitgenodigd dient te worden om aan managementvergadering deel te nemen. De FG neemt onder andere deel aan het overleg over privacy en informatiebeveiliging, waar onder andere ook de directeur bedrijfsvoering en de centrale privacy officer aan deelnemen, en een jaarlijks overleg met de Raad van Toezicht. De FG wordt in de praktijk ook betrokken bij privacy-incidenten.

Naast de FG is ervoor gekozen ook een centrale privacy officer aan te stellen. Met deze aanstelling is beoogd om te voorkomen dat de FG zich te intensief met uitvoeringswerkzaamheden moet gaan bezighouden. In de gesprekken met de centrale privacy officer en de FG komt naar voren dat de centrale privacy officer zich richt op beleidsvorming en het maken van strategische keuzes en dat de FG zich bezighoudt met het verrichten van analyses op organisatieniveau en het vertalen van ontwikkelingen naar de organisatie. De FG geeft aan dat deze zichzelf ook als adviseur ziet en graag meedenkt over strategische onderwerpen.

AP
De geïnterviewden constateren dat er een spanningsveld is tussen de toezichthoudende rol van de AP en het geven van advies aan organisaties. De geïnterviewden geven aan dat behoefte bestaat aan een meer informele contactmogelijkheid om onderwerpen die een grote privacy-impact kunnen hebben met de AP te bespreken. Ook het publiceren van best practices over het uitvoeren van DPIA's of het behandelen van datalekken kan volgens de geïnterviewden bijdragen aan bewustwording over en correcte implementatie van de AVG.

Uitdagingen

De belangrijkste uitdaging voor de organisatie bestaat volgens geïnterviewden uit het continu bevorderen van het privacybewustzijn. Dit bewustzijn wordt binnen de organisatie als belangrijkste factor voor naleving van de AVG beschouwd; het draagt eraan bij dat de privacy-

organisatie tijdig bij nieuwe projecten wordt betrokken en dat werkwijzen die vanuit privacy-oogpunt mogelijk problematisch zijn tijdig worden gesignaleerd. Om het privacybewustzijn blijvend op een hoog niveau te houden is het volgens de FG en centrale privacy officer van belang dat het management blijvend voorbeeldgedrag vertoont, dat het beleid steeds wordt geactualiseerd en dat het belang van privacy continu onder de aandacht wordt gebracht.

Een andere uitdaging zijn innovatieve projecten. De organisatie ziet zichzelf als innovatief en wil verder digitaliseren. Met deze digitaliseringsprojecten gaan privacyrisico's gepaard. De geïnterviewden geven aan dat aan de voorkant van het project rekening wordt gehouden met deze risico's en dat de privacy-organisatie hier tijdig bij wordt betrokken. Ook op dit vlak is het van belang dat medewerkers zich bewust zijn van de privacy-aspecten van hun werkzaamheden.

Uit de gesprekken komt naar voren dat (verouderde) wetgeving waarin privacy-aspecten onvoldoende zijn meegenomen een knelpunt kan zijn. De geïnterviewde manager noemt als voorbeeld een bepaling op grond waarvan de organisatie bepaalde gegevens schriftelijk moet delen. Het schriftelijk verstrekken brengt een verhoogd risico op datalekken met zich en zou beter geautomatiseerd kunnen worden.

Analyse

De uitvoeringsorganisatie vertoont op privacyvlak een hoog niveau van volwassenheid. De organisatie beschikt over gedetailleerd beleid en over voldoende capaciteit om dit beleid op de werkvloer te implementeren. Daarnaast vindt er een continue verbetering van het beleid en de processen rondom privacy plaats; de ISO-certificering en de audits spelen in dit verband een belangrijke rol.

De taakopvatting en cultuur van de organisatie lijken een belangrijke rol te spelen bij de naleving van de AVG. Volgens de FG ontleent de organisatie haar bestaansrecht aan het zorgvuldig beheren van de registers. Om die reden hield de organisatie zich al langer, voor invoering van de AVG, bezig met privacy. Dat heeft ertoe geleid dat de organisatie zich heeft kunnen doorontwikkelen en veel zaken nu op detailniveau heeft geregeld. Ook de directeur bedrijfsvoering geeft aan dat privacy als een van de hoekstenen van de organisatie wordt beschouwd en van belang is voor het behouden van vertrouwen als overheidsinstelling.

Dimensies van spontante naleving

Kennis van regels
Zoals eerder opgemerkt wordt privacybewustzijn binnen de organisatie als belangrijke factor voor naleving van de AVG gezien. Uit de gesprekken blijkt dat medewerkers zich in hoge mate bewust zijn van de rol die privacy en de AVG spelen bij de werkzaamheden van de uitvoeringsorganisatie. Dit bewustzijn is volgens de geïnterviewde manager met name tot stand gekomen door de decentrale privacy officers en de contactpersonen binnen de diverse onderdelen. Deze personen zorgen ervoor dat de rest van de organisatie wordt meegenomen op het gebied van privacy. Ook door de privacytrainingen en e-learning modules is het privactbewustzijn toegenomen. Dit blijkt uit de toename van het aantal mogelijke datalekken, waarbij ook vaker incidenten die minder evident een datalek zijn worden gemeld.

Kosten en baten

De belangrijkste taak van de uitvoeringsorganisatie is het beheren van de registers. Uit de casestudy blijkt niet dat de uitoefening van deze taak op gespannen voet staat met de naleving van de AVG of dat deze spanning wordt ervaren. Uit de gesprekken met de directeur bedrijfsvoering, centrale privacy officer en de FG blijkt dat privacybescherming als onderdeel van de taak, het zorgvuldig beheren van de registers, wordt beschouwd. Ook in het beleid wordt opgemerkt dat betrouwbaar informatiebeheer essentieel is voor de taakuitoefening en dat de bescherming van persoonsgegevens hier een onderdeel van is.

Op uitvoeringsniveau komt het soms voor dat privacy niet de hoogste prioriteit krijgt. De geïnterviewde decentrale privacy officers geven aan dat zij begrijpen dat managers ook rekening moeten houden met bijvoorbeeld financiële belangen, andere maatschappelijke belangen en het belang van de werknemers. Ook andere medewerkers hebben hun eigen takenpakket. De consequentie hiervan is dat de privacy officers in sommige gevallen later dan gewenst bij projecten worden betrokken. Bij de meeste medewerkers is het inmiddels bekend dat een project vertraging op kan lopen als de privacy officers niet tijdig worden aangehaakt: de medewerkers hebben dus ook een niet-privacygerelateerd belang om de privacy-organisatie bij projecten te betrekken.

Mate van acceptatie
Binnen de uitvoeringsorganisatie bestaat over het algemeen een hoge mate van acceptatie van de AVG, zowel bij de directie als bij het management en de medewerkers van de verschillende onderdelen. De FG en de CPO schrijven de goede prestaties van de organisatie op het gebied van privacy toe aan het belang dat het management hecht aan privacy, waardoor voor privacybescherming ook voldoende capaciteit beschikbaar wordt gesteld.

Uit de gesprekken blijkt dat ook op lager niveau voldoende draagvlak is voor naleving van de AVG: management en medewerkers nemen privacybescherming serieus en hechten daar belang aan. Net zoals bij het privacybewustzijn spelen de decentrale privacy officers en contactpersonen een belangrijke rol bij het creëren van dit draagvlak. Doordat ook op management- en uitvoeringsniveau het belang van privacybescherming wordt gezien, worden de privacy officers tijdig betrokken bij nieuwe projecten.

Maatschappelijke controle
Zoals gezegd hecht de uitvoeringsorganisatie belang aan het vertrouwen dat zij als overheidsinstelling geniet. Dat blijkt zowel uit het gesprek met de directeur bedrijfsvoering als uit het gesprek met de FG. Volgens de directeur is het voor een overheidsorganisatie van belang is dat deze het vertrouwen behoudt; de FG geeft aan dat de organisatie zijn bestaansrecht ontleent aan het zorgvuldig beheren van de registers. Vanuit dit oogpunt is het volgens beide van belang dat de organisatie conform de privacywetgeving handelt en dat zij dit ook naar buiten toe kan verantwoorden.

Bijlage 9: Caseverslag uitvoeringsorganisatie 4

Inleiding

Dit hoofdstuk beschrijft de praktijk van de naleving door een uitvoeringsorganisatie. Deze organisatie valt onder de verantwoordelijkheid van het ministerie van Justitie en Veiligheid. Het betreft een zelfstandig bestuursorgaan met ongeveer driehonderd medewerkers.

In het kader van deze casestudy is gesproken met de CIO, CISO en de FG. De CIO maakt deel uit van het managementteam van de uitvoeringsorganisatie. De CISO is ook de coördinator van het privacy- en informatiebeveiligingsteam. Ook is gesproken met een medewerker van de uitvoeringsorganisatie die, naast haar reguliere werkzaamheden, binnen een afdeling van de uitvoeringsorganisatie fungeert als centraal aanspreekpunt en privacyrisico's signaleert. Zij houdt zich ook bezig met het melden van datalekken en het bijhouden van het incidentenregister. In het vervolg wordt deze medewerker aangeduid als 'de contactpersoon'. De uitvoeringsorganisatie heeft de volgende documenten opgestuurd: een beleidsstuk waarin de governancestructuur is vastgelegd en een aanvulling daarop, het privacyhandboek, een zogenaamd awareness-plan om de bewustwording te bevorderen en een presentatie voor een training voor contactpersonen.

Gegevensverwerking door de organisatie

De uitvoering van haar taken brengt mee dat de uitvoeringsorganisatie contact heeft met burgers en professionele dienstverleners. De professionele dienstverleners verstrekken persoonsgegevens van cliënten aan de uitvoeringsorganisatie. Doorgaans zijn dit namen, BSN-nummers en financiële gegevens, maar het kan ook gaan om strafrechtelijke of medische gegevens. De uitvoeringsorganisatie bewaart deze gegevens, neemt beslissingen op basis van deze gegevens en wisselt deze in bepaalde gevallen uit met andere overheidsinstanties. Het contact tussen de uitvoeringsorganisatie en burgers vindt voornamelijk plaats via de post. De brieven bevatten in de regel NAW-gegevens, BSN-nummers en financiële gegevens en kunnen ook strafrechtelijke gegevens bevatten. Het verkeerd adresseren van brieven wordt door de geïnterviewden als voornaamste privacyrisico beschouwd. Een deel van de doelgroep van de uitvoeringsorganisatie wisselt namelijk regelmatig van adres, waardoor het risico op verkeerd geadresseerde post groot is.

Interne organisatie

Beleid

In 2019 heeft de uitvoeringsorganisatie de governancestructuur ten aanzien van privacy vastgelegd in een beleidsdocument (het governancedocument). In dit document zijn de rollen en verantwoordelijkheden op het gebied van privacy uitgewerkt, waarbij het *three lines of defence*-model is gevolgd. Ook is vastgelegd dat er een periodiek privacy-overleg plaatsvindt, wat hierin wordt besproken en wie hierbij aanwezig zijn en beschrijft het document in grote lijnen hoe de samenwerking met het informatiebeveiligingsteam is geregeld. De uitvoeringsorganisatie heeft dit document begin 2021 aangevuld met een nadere omschrijving van de taken en verantwoordelijkheden van de contactpersonen. Zowel leidinggevenden, de ondernemingsraad, het privacyteam als de contactpersonen zelf hadden behoefte aan een nadere uitwerking van de rol van contactpersonen.

Daarnaast beschikt de uitvoeringsorganisatie over een privacyhandboek. In dit handboek is in hoofdlijnen aangegeven hoe de organisatie omgaat met persoonsgegevens, bijvoorbeeld op het vlak van dataretentie, het afsluiten van verwerkersovereenkomsten en de vernietiging van persoonsgegevens. Het privacyhandboek vormt de basis voor andere beleidsdocumenten, zoals een richtlijn voor e-mailgebruik en de procesbeschrijvingen voor datalekken, inzageverzoeken en DPIA's. Het handboek besteedt ook aandacht aan trainingen en bewustwording op het gebied van privacy.

Privacy-organisatie

De privacy-organisatie is ingericht volgens het *three lines of defence*-model. De eerste lijn bestaat uit medewerkers die de primaire taken van de organisatie uitvoeren. In het beleid van de organisatie wordt opgemerkt dat elke medewerker zelf verantwoordelijk is voor de naleving van de AVG en het privacy beleid. Het betreffende afdelingshoofd kan worden aangesproken op de wijze van verwerking van persoonsgegevens op zijn op haar afdeling. Elke afdeling beschikt over een contactpersoon. Dit is een medewerker die – naast zijn of haar reguliere werkzaamheden – binnen de betreffende afdeling fungeert als aanspreekpunt, risico's signaleert en bewustzijn creëert.

De tweede lijn wordt gevormd door het privacyteam. Het privacyteam bestaat uit drie privacy officers, een security officer, de CISO (tevens coördinator van het IBP-office) en de CIO. De CIO geeft leiding aan het privacyteam en zit ook in het managementteam van de uitvoeringsorganisatie. De privacy officers zijn verantwoordelijk voor het formuleren en implementeren van beleid en het organiseren van activiteiten rondom privacycompliance. De privacy officers ondersteunen de eerste lijn bij de uitvoering van DPIA's, het afsluiten van verwerkersovereenkomsten en het geven van advies over het verwerken van persoonsgegevens. De privacy officers kunnen volgens het governancedocument ook rechtstreeks advies uitbrengen aan de directie.

De FG vormt de derde lijn. De FG heeft volgens de privacygovernance een onafhankelijke positie en een controlerende en toezichthoudende rol. De FG ziet toe op de naleving van de AVG en het opgestelde beleid. In de privacygovernance wordt opgemerkt dat de FG een adviserende rol kan innemen voor zover dit zijn onafhankelijke toezichthoudende rol niet aantast.

In het governancedocument is vastgelegd dat er een periodiek privacy-overleg is. Dit overleg vindt plaats tussen de privacy officers, security officer en contactpersonen. Tijdens het privacy-overleg komen veranderingen in wet- en regelgeving aan de orde, worden veranderingen binnen de organisatie die gevolgen hebben voor de verwerking van persoonsgegevens behandeld en worden actuele onderwerpen die de contactpersonen binnen hun afdelingen zijn tegengekomen. Van dit overleg wordt geen melding gemaakt in de interviews. De geïnterviewde contactpersoon geeft wel aan dat er een tweewekelijks overleg is tussen de contactpersonen, privacy officers en de FG.

Inbedding privacy in de organisatie

De FG heeft een aantal keren per jaar overleg met de directeur van de organisatie. Uit die gesprekken maakt hij op dat de directeur privacy uiterst serieus neemt. De CIO zit ook in het managementteam. Hij geeft aan dat in gevallen dat er serieus iets verkeerd gaat op het gebied van privacy het managementteam wordt geïnformeerd. De FG wordt in die gevallen in de gelegenheid gesteld om kritische vragen te stellen.

Op elke afdeling is een contactpersoon aanwezig. Deze contactpersonen brengen privacy-aspecten onder de aandacht en fungeren binnen de betreffende afdeling als eerste aanspreekpunt voor privacyvraagstukken. Ten aanzien van informatiebeveiliging hebben zij dezelfde rol.

Praktijk

Opleiding en training

Volgens de CIO hebben de medewerkers van de uitvoeringsorganisatie aandacht voor naleving van de AVG. De medewerkers van de uitvoeringsorganisatie werken namelijk in een juridische omgeving en hebben om die reden meer affiniteit met een juridisch thema als de AVG. Ook de contactpersoon geeft aan dat haar collega's, waar het datalekmeldingen betreft, goed op de hoogte zijn en begrijpen wanneer iets als datalek moet worden gemeld. De FG geeft daarentegen aan dat het bij de uitvoeringsorganisatie lastig is om bewustzijn op het gebied van privacy te ontwikkelen. Medewerkers van de organisatie hebben namelijk geen face-to-face contact met personen wiens privacy is geschonden en worden om die reden niet met de gevolgen van privacy-inbreuken geconfronteerd. Dat vraagt volgens de FG om extra stappen om privacybewustzijn te creëren.

Ter bevordering van het privacybewustzijn zijn medewerkers verplicht om e-learning modules te volgen. Deze modules zijn afkomstig van het ministerie van Justitie en Veiligheid en hebben verschillende niveaus. Zo is de module voor leidinggevenden uitgebreider dan de module voor medewerkers die net in dienst zijn getreden. Voor de contactpersonen zijn er uitgebreidere trainingen die worden verzorgd door het privacyteam en de FG. Naast deze trainingen maakt de organisatie gebruik van diverse 'awareness-prikkels' om het bewustzijn rondom privacy te bevorderen. Deze prikkels bestaan uit nep-phishingberichten -en telefoontjes en acties met mystery guests. Op het gebied van informatiebeveiliging worden penetratietesten uitgevoerd.

De contactpersonen spelen ook een rol in het bevorderen van privacybewustzijn. Op elke afdeling is een contactpersoon aanwezig. Deze contactpersonen brengen privacy-aspecten onder de aandacht en fungeren binnen de betreffende afdeling als eerste aanspreekpunt over privacyvraagstukken.

Processen

DPIA's
Voor het uitvoeren van DPIA's wordt gebruik gemaakt van de nieuwe model-DPIA van de Rijksoverheid. Een deel van dit model richt zich op de beschrijving van de voorgenomen gegevensverwerking. Op dit moment wordt dit gedaan door een privacy officer in samenwerking met een medewerker van Informatiebeveiliging een medewerker uit het primaire proces, doorgaans de contactpersoon. Op termijn is het de bedoeling dat dit deel door de contactpersoon wordt gedaan. Contactpersonen krijgen training op dit punt.

Datalekmeldingen
De uitvoeringsorganisatie verstuurt veel brieven. Dat leidt geregeld tot een datalek, bijvoorbeeld als een brief naar het verkeerde adres wordt gestuurd. De organisatie probeert het risico op deze datalekken te verkleinen door de professionele dienstverleners te informeren over het belang van het doorgeven van juiste adresgegevens en te informeren als zij een verkeerd adres hebben opgegeven. De geïnterviewde contactpersoon houdt zich bezig met het melden van datalekken. Zij geeft aan dat haar collega's op de afdeling begrijpen wanneer sprake is van een datalek. Desondanks komt het voor dat een datalek niet altijd wordt gesignaleerd. Gesignaleerde datalekken worden altijd gemeld, zij het niet in alle gevallen binnen de daarvoor geldende termijn van tweeënzeventig uur. Bij complexere datalekken wordt een privacy officer of de FG geïnformeerd. Tijdens het IBP-overleg wordt ook besproken of naar aanleiding van een datalek maatregelen genomen moeten worden.

Verwerkersovereenkomsten
De CIO geeft aan dat de langdurige relaties die de uitvoeringsorganisatie heeft met leveranciers een risico vormt. De verwerkersovereenkomsten zijn soms niet altijd goed in beeld en in sommige gevallen ook gedateerd. Ook volgens de CISO zijn de verwerkersovereenkomsten een punt van aandacht.

Samenwerking andere overheden

De uitvoeringsorganisatie wisselt gegevens uit met andere overheden. Afgelopen jaar heeft de uitvoeringsorganisatie gegevensuitwisselingsbeleid vastgesteld, zodat de samenwerking met andere overheden beter kan worden georganiseerd. Dit beleid bevat een checklist waarin wordt gevraagd naar de grondslag en de noodzaak van de gegevensuitwisseling. De uitvoeringsorganisatie verwerkt ook persoonsgegevens in opdracht van het ministerie van Justitie en Veiligheid. De verwerkingsverantwoordelijkheid ligt in dat geval bij het ministerie. De FG geeft aan dat hij heeft gemerkt dat het ministerie moeite heeft om deze verwerkingsverantwoordelijkheid in te vullen.

Daarnaast deelt de uitvoeringsorganisatie ook kennis met andere overheden. De privacy officers van de uitvoeringsorganisatie maken, tezamen met privacy officers van andere overheden die onder verantwoordelijkheid van het ministerie van Justitie en Veiligheid vallen, deel uit van een overlegorgaan. In dit overleg worden stukken uitgewisseld en handreikingen opgesteld, bijvoorbeeld voor het uitvoeren van DPIA´s. Ook maakt de uitvoeringsorganisatie deel uit van een samenwerkingsverband van kleinere uitvoeringsorganisaties, waarbinnen ook kennis wordt gedeeld op het gebied van privacy en informatiebeveiliging.

Controle en toezicht

Positie FG

De uitvoeringsorganisatie beschikt over een externe FG die voor een dag in de week werkzaam is bij de organisatie. Sinds de zomer van 2021 is de FG actief bij de uitvoeringsorganisatie. Hij geeft aan dat het van belang is om draagvlak te creëren, en dat het vanuit dat oogpunt niet handig is om gelijk de focus te leggen op controle-activiteiten. Op dit moment bestaan zijn werkzaamheden uit het meekijken bij verschillende processen zoals het uitvoeren van DPIA's, het melden van datalekken en het opstellen van verwerkersovereenkomsten en privacyverklaringen. De ervaring van de CIO met de FG is dat dit een persoon is die kritische vragen stelt en kennis van zaken heeft. Volgens de CIO beperkt de FG zich tot controleactiviteiten en staat hij op enige afstand van de organisatie.

AP

De CISO geeft aan dat het contact met de AP uiterst minimaal is. Sinds invoering van de AVG is drie keer contact geweest tussen de uitvoeringsorganisatie en de AP. Dit contact ging met name over de manier waarop de betrokkene bij een datalek is geïnformeerd. Volgens de CISO kan het nuttig zijn om vaker een terugkoppeling te krijgen op datalekmeldingen, omdat de uitvoeringsorganisatie vaak gelijksoortige datalekmeldingen doet.

Ook het contact tussen de FG en de AP is beperkt. De AP heeft een servicedesk voor FG's, maar de FG geeft aan dat hij meer behoefte heeft aan een gesprek waarin hij zijn zorgen kan bespreken en op die manier kan aangeven waar de knelpunten bij de organisatie zitten. De omstandigheid dat de organisatie weinig terugkoppeling ontvangt op datalekken is volgens de FG geen reden om deze niet meer te melden. In zijn optiek moeten organisaties op dit punt zo transparant mogelijk zijn. De FG heeft gemerkt dat alle datalekken worden besproken en gemeld bij de AP, zij het niet in alle gevallen binnen tweeënzeventig uur.

Uitdagingen

De geïnterviewden geven aan dat de uitvoeringsorganisatie steeds professioneler te werk gaat op het gebied van privacy. Zij wijzen desondanks op een aantal verbeterpunten en uitdagingen. Zoals eerder besproken wordt er gewerkt aan het verbeteren van het proces rondom het sluiten en bijwerken van verwerkersovereenkomsten. Een ander verbeterpunt dat wordt genoemd is het updaten van de privacyverklaring en het verwerkingsregister. De CISO geeft aan dat de komende periode (vanaf juni 2022) de focus ligt op het ontwikkelen van Governance, Risk and Compliance-tooling (GRC-tooling) voor privacyprocessen. Doel van de GRC-tooling is het inzetten van software om compliance-processen te stroomlijnen.

Een ander aandachtspunt is de capaciteit van contactpersonen. De contactpersonen komen soms tijd te kort om, naast hun reguliere werkzaamheden, hun werkzaamheden op privacygebied uit te voeren. Als een DPIA moet worden uitgevoerd hebben contactpersonen soms geen tijd. De CISO merkt dat primaire processen dan vaak voorrang krijgen. Ook de geïnterviewde contactpersoon geeft aan dat de in het governancedocument gestelde tijdsbesteding van twee uur per week voor de rol als contactpersoon doorgaans wel realistisch is, maar als de contactpersoon meer bij het uitvoeren van DPIA's wordt betrokken, zullen voor deze rol meer uren moeten worden uitgetrokken.

Volgens de CIO brengt de klantgerichtheid van de uitvoeringsorganisatie risico's met zich mee op het gebied van privacy. Hij noemt als voorbeeld het beveiligd sturen van e-mail. Als dat niet werkt, zijn medewerkers geneigd naar andere oplossingen te zoeken.

Daarnaast spelen er technische vraagstukken die zijn verbonden met informatiebeveiliging. Een van die vragen is hoe informatie binnen de systemen van de uitvoeringsorganisatie kan worden geïsoleerd. Ook het veilig werken vanuit de Cloud is een onderwerp dat binnen de uitvoeringsorganisatie aandacht krijgt. In meer algemene zin zijn volgens de CIO nog inspanningen nodig om volledig aan de Baseline Informatiebeveiliging Overheid (BIO) te voldoen. In de BIO zijn de basisvereisten op het gebied van informatiebeveiliging van de overheid vastgelegd.

Analyse

De uitvoeringsorganisatie beschikt over een redelijk goed ontwikkelde privacy-organisatie die in staat is tot zelfevaluatie. De wijze van gegevensverwerking is uitgewerkt in het beleid, de rollen op het gebied van privacy- en informatiebeveiliging zijn vastgelegd en duidelijk voor betrokken en de FG neemt een onafhankelijke positie in. Op een aantal punten is de privacybescherming nog niet op het gewenste niveau; de privacyfunctionarissen hebben aandacht voor de aspecten van privacybescherming die nog verder moeten worden ontwikkeld. Het bijwerken van verwerkersovereenkomsten, de privacyverklaring en het verwerkingsregister zijn hier voorbeelden van. In zijn algemeenheid is het proces rondom de evaluatie van deze documenten een punt van aandacht; de CISO heeft aangegeven dat hiervoor GRC-tooling in ontwikkeling is. Ook op het gebied van informatiebeveiliging moeten volgens de organisatie nog stappen worden gezet om aan de BIO te voldoen.

Dimensies van spontane naleving

Kennis van regels
Binnen de organisatie is veel aandacht voor het creëren van privacybewustzijn bij medewerkers. Dit hangt mogelijk samen met de aandacht die uitgaat naar datalekken door verkeerd geadresseerde post. Het voorkomen en herkennen van deze datalekken is afhankelijk van het gedrag van de betrokken medewerkers, waardoor veel aandacht wordt besteed aan het verbeteren van het gedrag.

Kosten en baten
De taakuitoefening van de organisatie wordt niet noemenswaardig gehinderd door de regels van de AVG en wordt dan ook niet als obstakel gezien. Dat laat onverlet dat medewerkers in hun dagelijkse werkzaamheden, wegens tijdsgebrek, niet altijd prioriteit geven aan de naleving van de AVG. Contactpersonen die soms niet toekomen aan hun taken op privacygebied of datalekken die niet tijdig worden gemeld zijn hier voorbeelden van.

Bijlage 10: Caseverslag waterschap

Inleiding

In dit hoofdstuk wordt de praktijk beschreven van de toepassing en naleving van de AVG door een waterschap. Het gaat om een waterschap met ongeveer 300 medewerkers. Waterschappen zijn verantwoordelijk voor voldoende en schoon water en zorgen voor bescherming tegen te veel water in Nederland. Ze zorgen voor het reguleren van de waterstand met bijvoorbeeld gemalen en sluizen, het zuiveren van afvalwater, het beheren van de dijken, het natuurbeheer in en aan het water en voor controle van de kwaliteit van het zwemwater.

In deze casestudy is gesproken met een lid van het dagelijks bestuur, een lid van de directie, een security officer en de teamleider van de afdeling Juridische Zaken. De functie van de FG was ten tijde van het uitvoeren van de casestudy vacant. Het waterschap heeft het handboek voor gegevensverwerking, het privacybeleid, het privacyreglement en een toetsings- en auditplan voor privacy-audits verstrekt.

Gegevensverwerking door de organisatie

Het waterschap verwerkt in heel beperkte mate gegevens van inwoners, veel minder dan bijvoorbeeld gemeenten doen. Dat komt doordat het waterschap de heffing van de waterschapsbelasting heeft uitbesteed aan een regionaal belastingkantoor. De gegevens die het waterschap verwerkt betreffen hoofdzakelijk informatie over eigen medewerkers. Deze informatie wordt verwerkt binnen de afdelingen financiën en personeelszaken. Er worden daarnaast persoonsgegevens verwerkt van ingelanden wanneer toezichthouders een schouw uitvoeren, maar dat betreffen basale persoonsgegevens zoals NAW-gegevens. Het gaat dan niet om bijzondere persoonsgegevens. Datzelfde geldt voor het verwerken van persoonsgegevens voor de behandeling van bezwaar- of klachtprocedures. In het actuele verwerkingsregister is voor alle processen vastgelegd welke gegevens worden verwerkt en wie die gegevens mogen inzien.

Interne organisatie

Beleid

Het waterschap heeft in 2016 een privacyreglement, en in 2019 privacybeleid voor de periode 2020 – 2022 vastgesteld. Het beleid wordt momenteel geactualiseerd. Het privacybeleid dient ervoor om op organisatie- en strategisch niveau duidelijkheid te geven over de

inrichtingskeuzes van privacy en te waarborgen dat de verwerking van persoonsgegevens op een rechtmatige wijze plaatsvindt. In het beleid worden de ambities en uitgangspunten uiteengezet. Ook deelt het beleid taken en verantwoordelijkheden toe binnen de organisatie op strategisch, tactisch en operationeel niveau. De PDCA-cyclus ten aanzien van privacy en gegevensverwerking is uitgewerkt in het beleid. Het waterschap heeft de ambitie om in 2023 volwassenheidsniveau 4 van het Capability Maturity Model voor privacy bereikt te hebben.

Naast het privacybeleid beschikt het waterschap over een toetsings- en auditplan privacy en AVG. In dit plan is uitgewerkt op welk niveau de toetsen moeten plaatsvinden (binnen processen, over processen heen of op organisatieniveau), wie verantwoordelijk is voor de uitvoering van de toetsen en met welke regelmaat (periodiciteit) de toetsen worden uitgevoerd.

Privacy-organisatie

Het waterschap heeft een privacy-organisatie die nog in ontwikkeling is, maar al een zekere mate van volwassenheid heeft bereikt. In een landelijke audit onder waterschappen scoorde de organisatie bovengemiddeld. De privacy-organisatie is ingericht op basis van het *three lines of defence*-model. De verantwoordelijkheden zijn belegd in de lijn. In de eerste lijn is per team iemand benoemd die als eerste aanspreekpunt en vraagbaak fungeert voor aan privacy gerelateerde vragen. Het aanspreekpunt voert deze taak uit naast zijn of haar reguliere taken en verantwoordelijkheden. Deze rol is medio 2020 in het leven geroepen. In de tweede lijn zijn de twee privacy officers gepositioneerd en de functionaris gegevensbescherming fungeert in de derde lijn als toezichthouder. Voor informatiebeveiliging is eveneens een aanspreekpunt binnen de teams aangewezen, met als tweede lijn een security officer en in de derde lijn de CISO. De CISO en de FG vallen hiërarchisch direct onder de secretaris-directeur.

Privacy en informatiebeveiliging zijn twee verschillende vakgebieden met elk hun *three lines of defence*, maar in de praktijk werken ze nauw samen. Binnen de organisatie werken de security officer en de privacy officer nauw samen en delen bovendien dezelfde werkkamer waardoor de lijnen kort zijn. Daar waar privacy en informatiebeveiliging samenkomen is samenwerking noodzakelijk. Daarvan is bijvoorbeeld sprake bij de inkoop van nieuwe software; daar spelen vraagstukken rondom informatieveiligheid, maar bij het verwerken van persoonsgegevens wordt daar ook rekening mee gehouden. Daar ontstaat de samenwerking tussen de twee kolommen.

De organisatie heeft twee overlegstructuren in het leven geroepen; een voor privacy en voor informatiebeveiliging. Ten aanzien van privacy is de privacydesk ontwikkeld waaraan vertegenwoordigers van personeelszaken, juridische zaken en de privacy officer deelnemen. Hier worden actiepunten uit het jaar- en uitvoeringsplan besproken, nieuws, actualiteiten, incidenten, datalekken en nieuwe wet- en regelgeving besproken. Voor informatiebeveiliging bestaat een soortgelijk gremium waaraan de teamleider I&A, de security officer en de CISO deelneemt.

Praktijk

Opleiding en training

Medewerkers kunnen zich opgeven om aanspreekpunt binnen het team te worden. De kandidaten zijn vervolgens met zorg geselecteerd. Dat kunnen medewerkers met verschillende achtergronden en expertises zijn, maar allen hebben affiniteit met privacy of informatiebeveiliging. De kandidaten hebben een interne opleiding gehad om de functie van aanspreekpunt te

kunnen vervullen en de scholing wordt periodiek herhaald. Hierin worden de onderwerpen van het handboek privacy onder de aandacht gebracht.

Het waterschap heeft een eigen e-learning ontwikkeld om medewerkers te scholen in de verschillende facetten van privacy en wat daarin hun eigen verantwoordelijkheden zijn. Daarin worden de basisprincipes over privacy en informatiebeveiliging bijgebracht, de belangrijkste do's en don'ts en het bewustzijn dat de grootste risico's in het menselijk handelen zitten. Ook het thema datalekken komt daarbij aan de orde en wat er van medewerkers verwacht wordt als daarvan sprake is. De e-learnings moeten verplicht worden gevolgd door alle medewerkers. Er wordt op toegezien dat dit ook gebeurt.

Ook worden op laagdrempelige en speelse wijzen nut en noodzaak van privacy en naleving van de AVG bij medewerkers onder de aandacht gebracht. Zo heeft het waterschap zelf een privacyquiz ontwikkeld die door de aanspreekpunten binnen de teams worden uitgevoerd. Via Mentimeter kunnen medewerkers deelnemen. Op deze manier wordt geprobeerd het onderwerp op een levendige manier onder de aandacht te houden. Blijvend bewustzijn wordt namelijk gezien als de belangrijkste randvoorwaarde. Ook worden er regelmatig berichten rondom privacy op het intranet en social intranet geplaatst die voor alle medewerkers te raadplegen zijn en waar alle relevante documentatie rondom privacy te vinden is.

De privacy officers en de security officer houden hun kennis op peil door het volgen van opleidingen en het participeren in verschillende landelijke werkgroepen waar kennis en informatie wordt uitgewisseld zoals CPW en CIB. De privacy officer en de security officer zijn gemiddeld een dag per maand bezig met hun eigen bijscholing.

Processen uitvoering

De privacy-organisatie op basis van het *three lines of defence*-model functioneert naar tevredenheid. Met name de aanspreekpunten op de werkvloer binnen de verschillende teams worden als zeer waardevol gezien. Zij zijn de ambassadeurs van het privacybeleid binnen de organisatie. De aanspreekpunten zorgen voor privacybewustzijn binnen de gehele organisatie. Hun nabije aanwezigheid op de werkvloer zorgt ervoor dat wanneer er bijvoorbeeld nieuwe projecten worden gestart, ook privacy-aspecten in ogenschouw genomen moeten worden. Dat leidt ertoe dat de privacy officer steeds in een vroeg stadium wordt betrokken in het proces. Dat geldt bijvoorbeeld ook bij de processen rondom inkoop. Daar wordt privacy nu aan de voorkant als voorwaarde gesteld waaraan een leverancier moet voldoen. De privacy officer en de security officer maken een jaar- en uitvoeringsplan waarin de verschillende acties op het terrein worden bepaald. De plannen worden door het MT goedgekeurd en vastgesteld.

Voor bepaalde processen worden DPIA's uitgevoerd. Dat gebeurt in de tweede lijn in samenwerking tussen privacy officer en een functioneel beheerder. Door middel van een Information Security Management System (ISMS), dat wordt voorgeschreven door de Baseline Informatiebeveiliging Overheid (BIO) wordt bepaald of voor een bepaald proces een DPIA moet worden uitgevoerd.

In geval van een datalek wordt er melding gedaan bij de privacy officer die een onderzoek instelt. Met de FG wordt een afweging gemaakt of er melding gedaan moet worden bij de AP. Alle datalekken worden in een datalekregister vastgelegd. Het management wordt hier middels een jaarrapportage over geïnformeerd. Het gros van de datalekken betreffen verkeerd geadresseerde e-mails. De organisatie probeert binnen de organisatie te benadrukken dat fouten maken menselijk is, dat datalekken kunnen voorkomen. Daarbij wordt eveneens

geprobeerd een veilig klimaat te scheppen waarin medewerkers niet bang hoeven te zijn om een melding te doen van een datalek. Dat verhoogt de meldingsbereidheid.

Het management en bestuur van het waterschap geeft nadrukkelijk prioriteit aan de naleving van de AVG. Dat komt bijvoorbeeld tot uitdrukking in de wens van het management en bestuur om op de hoogte gehouden te worden van ontwikkelingen of onderzoeken die gedaan worden. De privacy officer wordt regelmatig gevraagd om een toelichting te geven in het MT rondom aan privacy gerelateerde ontwikkelingen binnen het waterschap. De lijnen tussen de privacy officer en de security officer met het MT zijn kort, zowel op formele als informele basis. De betrokkenheid is groot en dat wordt gevoeld in de organisatie. Uit de casestudy komen geen signalen naar voren over onduidelijkheden of onwerkbaarheden die voortvloeien uit de AVG.

Uitdagingen

De belangrijkste uitdagingen waarvoor de organisatie gesteld staat is om voldoende bewustzijn en support te ontwikkelen en te behouden, maar ook om er voldoende capaciteit voor te hebben. Dat lukt tot dusver voldoende, maar de kunst is dit ook te behouden. Privacy wordt immers soms nog steeds gezien als ‘iets dat men erbij moet doen’, terwijl het een integraal onderdeel van de processen moet zijn. De verantwoordelijkheden met betrekking tot privacy liggen in de lijn, maar medewerkers moeten ook in staat gesteld worden om er voldoende aandacht aan te kunnen besteden.

Een belangrijk verbeterpunt voor deze organisatie dat in de audit onder waterschappen naar voren kwam is dat het Toetsings- en auditplan privacy en AVG dat is opgesteld nu ook in de praktijk gebracht moet worden. In het toetsingsplan is vastgelegd welke toetsen op welke processen, wanneer en door wie moeten worden uitgevoerd. Daar zit een belangrijke uitdaging waaraan de organisatie momenteel werkt.

Analyse

De casestudyorganisatie verwerkt relatief weinig persoonsgegevens. De gegevens die verwerkt worden hebben in hoofdzaak betrekking op de eigen medewerkers. Desalniettemin geeft de organisatie blijk van een volwassen privacy-organisatie. Uit een landelijke audit onder waterschappen scoort deze organisatie bovengemiddeld. De belangrijkste factoren die daaraan ten grondslag liggen is dat de organisatie in een vroeg stadium, klaarblijkelijk eerder dan andere waterschappen, de privacy-organisatie heeft opgebouwd. Het management en bestuur hebben daaraan een belangrijke bijdrage geleverd door hiervoor capaciteit en middelen beschikbaar te stellen en uit te dragen dat privacy en naleving van de AVG belangrijk is.

Dimensies van spontante naleving

Kennis van de regels
Het waterschap hecht zichtbaar belang aan het ontwikkelen van het kennisniveau en het bewustzijn rondom privacyvraagstukken. Dat komt onder meer tot uitdrukking in de scholing van medewerkers via e-learnings waarin medewerkers de basisprincipes van de AVG en privacy worden bijgebracht en wat hun eigen verantwoordelijkheden hierin zijn. Datzelfde geldt voor de laagdrempelige privacyquiz. De aanspreekpunten op de werkvloer vormen enerzijds een

vraagbaak voor werknemers, maar zijn daarnaast ook de ambassadeurs van het privacybeleid. Hun nabijheid in de organisatie zorgt ervoor dat het bewustzijn in de organisatie van privacy ontwikkeld wordt. Dat leidt ertoe de privacy steeds meer een integraal en vanzelfsprekend onderwerp wordt binnen alle processen.

Mate van acceptatie
Deze verklarende factor vloeit voort uit de kennis van regels. Op het moment dat medewerkers binnen de organisatie voldoende kennis hebben van de privacyregelgeving, deze verinnerlijkt hebben en doorzien welk belang de AVG dient, zal men de regels ook sneller gaan accepteren en naleven. Wanneer naleving van de AVG slechts wordt gezien als een lastige bijzaak waarvan men nut en noodzaak niet inziet, zal de naleving tekortschieten.

Sanctie-ernst
De grootste risico's op datalekken zitten in het menselijk handelen. De organisatie probeert een veilig klimaat te scheppen waarin medewerkers zich veilig voelen een melding te doen zonder daar direct op te worden afgerekend.

Bijlage 11: Caseverslag gemeente 1

Inleiding

In deze paragraaf wordt de praktijk beschreven van de toepassing en naleving van de AVG door een grotere gemeente. Deze gemeente loopt in Nederland voorop bij het gebruik van algoritmes, maar is daarnaast ook nog druk bezig om het inzicht in de AVG binnen de organisatie te vergroten en de AVG tijdig onderdeel te laten zijn bij beleidsvorming en de implementatie van dat beleid.

In het kader van deze casestudy is gesproken met de concerndirecteur, de concern-privacy officer en de FG. Ook is een groepsgesprek gevoerd met een privacy officer, een beleidsadviseur, een teamleider en projectleider van een afdeling waarbinnen complexe gegevensverwerkingen plaatsvinden. De gemeente heeft een beschrijving van de governancestructuur, het privacybeleid, een overzicht van de bestaande privacy-overleggen en een richtlijn voor het melden van datalekken. Tevens is het register van verwerkingsactiviteiten online geraadpleegd.

Gegevensverwerking door de organisatie

De gemeente verwerkt een grote hoeveelheid (bijzondere) persoonsgegevens en ziet zich onder meer geconfronteerd met grote uitdagingen met betrekking tot de taakuitvoering en de samenwerking in verschillende samenwerkingsverbanden met andere (overheids)partijen. Daarnaast verwerkt deze gemeente persoonsgegevens voor de eigen organisatie.

Interne organisatie

Beleid

Met het van toepassing worden van de AVG heeft het college van burgemeester en wethouders het privacybeleid vastgesteld. Dit document geeft inzicht in de governancestructuur en beoogt richting te geven aan hoe de organisatie om moet gaan met privacy en laat zien dat de organisatie de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente waarin (bijzondere) persoonsgegevens worden verwerkt. Het privacybeleid is vooraf concernbreed afgestemd voordat het ter besluitvorming werd aangeboden.

In dit document wordt aan de hand van de door deze gemeente gehanteerde kernwaarden een visie geformuleerd over de omgang met de bescherming van persoonsgegevens. Daarnaast worden de interne actoren en hun rol geïdentificeerd, de verplichtingen van de verwerkingsverantwoordelijke nader uitgewerkt, waaronder informatiebeveiliging en de meldplicht datalekken, de rechten van betrokkene besproken en de inzet van het AVG-instrumentarium, zoals het verwerkingsregister en de DPIA om tot risicobeheersing en controle daarop te komen.

Ten tijde van het onderzoek werd gewerkt aan een aanscherping van de governancestructuur. Daarin wordt gekeken hoe de rolverdeling strakker kan worden vormgegeven en hoe taken, verantwoordelijkheden en bevoegdheden beter kunnen worden geformuleerd. De huidige governance structuur is op deze punten te algemeen beschreven.

Organisatie-inrichting

De privacy-organisatie van deze gemeente is in grote lijnen vastgelegd in het Privacybeleid. Hieronder worden alle relevante stakeholders en hun plaats binnen het privacybeleid en de organisatie besproken. De gemeente hanteert het *three lines of defence*-model.

De *eerste lijn* is de lijnorganisatie. Zij is verantwoordelijk voor het realiseren van de doelen van de gemeentelijke organisatie, waarvan privacy een vast onderdeel behoort te zijn. Risicomanagement lijkt daarbij het uitgangspunt. De lijnorganisatie werkt volgens het privacybeleid met relevante privacykaders en vastgestelde processen: Met de lijnorganisatie worden de hierna genoemde actoren bedoeld.

Het college van burgemeester en wethouders en de burgemeester

Zij zijn de verantwoordelijke bestuursorganen die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheid die krachtens de AVG zijn toebedeeld aan de verwerkingsverantwoordelijke. Formeel is het college van B&W respectievelijk de burgemeester dan ook verantwoordelijk voor de verwerkingen die onder de reikwijdte van de AVG vallen. Zij zijn verantwoordelijk voor:

a. De naleving van de beginselen voor de verwerking van persoonsgegevens.
b. De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd.

De gemeentesecretaris/ algemeen directeur

De algemeen directeur draagt de verantwoordelijkheid op ambtelijk niveau. Deze functionaris vormt de schakel tussen het bestuur en de ambtelijke organisatie en is in dit kader ambtelijk verantwoordelijk. Als portefeuillehouder in de concerndirectie is een van de concerndirecteuren aangewezen om namens de algemeen directeur verantwoordelijk te zijn voor de inhoudelijke voorbereiding van besluitvorming op het gebied van privacy. Naast privacy is deze concerndirecteur ook verantwoordelijk voor ICT/informatiebeveiliging en integriteit.

Deze concerndirecteur is voorzitter van de stuurgroep privacy, die het privacybeleid handen en voeten geeft voor het hele concern. Daarin zitten ook de concern-privacy officer, de FG en vertegenwoordigingen van alle clusters. Het gaat daarbij om zowel het interne privacybeleid voor de organisatie zelf, als beleid met betrekking tot uitvoering van de publieke taken.

Clusterdirecteuren

Deze directeuren dragen de verantwoordelijkheid op operationeel niveau. De verantwoordelijkheid voor het voldoen aan de privacywetgeving en beleid voor privacy binnen de clusters ligt bij de clusterdirecteuren. Een clusterdirecteur kan de verantwoordelijkheid voor taken die hierop betrekking hebben op operationeel niveau bij één van de MT-leden beleggen. Uitvoeringsgerichte bevoegdheden in dit kader – zoals de beslissing op verzoeken betreffende de uitoefening van rechten en ondertekening van de verwerkersovereenkomsten – worden de clusterdirecteur in mandaat verleend, met de bevoegdheid deze verder in de lijn onder te mandateren tot het niveau van afdelingsmanagers.

Proceseigenaar (lijnmanagement)
Binnen de afdelingen zijn de proceseigenaren verantwoordelijk voor de naleving van de privacywetgeving en het privacybeleid. De proceseigenaar legt verantwoording af aan de clusterdirectie. Binnen de afdelingen zijn privacy-ambassadeurs aangewezen. Dit zijn medewerkers die naast hun primaire taak de AVG als aandachtsgebied hebben en oog hebben voor gegevensbescherming bij beleidsvorming en implementatie van beleid.

De *tweede lijn*, waarin disciplines van privacy, informatievoorziening en integrale beveiliging zitten, helpt de eerste lijn door het opstellen van kaders, advies te geven over het toepassen van de kaders, coördinatie van activiteiten waar nodig. Het gaat hierbij over de hiernavolgende functionarissen.

Concern-privacy officer en privacy officers
De rol van de privacy officers is met name die van adviseur van het management van elk cluster/directie. Daarnaast ondersteunt de privacy officer bij het verrichten van DPIA's en overlegt waar nodig met de CPO over nieuwe ontwikkelingen. Per cluster zijn er een of meerdere privacy officers. Deze zijn verantwoordelijk voor specifiek aan de cluster/directie gerelateerde kennis en implementatie van privacyvraagstukken.

De CPO is de linking-pin naar directies en clusters en verantwoordelijk voor de behandeling van organisatiebrede privacyvraagstukken en is verantwoordelijk voor het privacyproces. Verder heeft de CPO volgens het privacybeleid een rol in de algemene kennisoverdracht met betrekking tot privacy en het signaleren en implementeren van organisatiebrede privacyvraagstukken.

Concern informatiesecurityofficer en decentrale informatie security officer
De concern informatie security officer is verantwoordelijk voor het informatiebeveiligingsproces binnen het concern. De concern informatie security officer stelt kaders op voor informatiebeveiliging en adviseert het bestuur hierover op strategisch niveau. De decentrale informatie security officer is gepositioneerd binnen een cluster en legt verantwoording af aan de concern informatie security officer en de clusterdirectie. Samen houden de concern informatie – security officer en decentrale informatie security officer toezicht op de informatiebeveiligingsmaatregelen die een cluster neemt om gegevens, waaronder persoonsgegevens, te beveiligen. De concern informatie security officer en decentrale informatie security officer werken hierbij nauw samen met de FG, CPO en de privacy officers.

De *derde lijn* is het *interne toezicht* dat op grond van de AVG is belegd bij *de FG*. De AVG verbindt eisen aan de positionering van een FG. Zo ziet de FG onafhankelijk toe op de naleving van de AVG in de betreffende organisatie en heeft de FG toegang tot het bestuur van de organisatie.

De FG heeft in deze gemeente toegang tot de gemeentesecretaris en de wethouder op het moment dat er 'iets geks' gebeurt en het niet wordt opgepakt. Bovendien, als de FG vindt dat iets 'niet door de beugel kan' – bijvoorbeeld het niet informeren van betrokkenen na een datalek of een onbehoorlijke gegevensverwerking of het bewust niet doorvoeren van te treffen maatregelen –, dan benadrukt hij bij de desbetreffende persoon dat diegene de wethouder op de hoogte moet stellen. Als dat niet gebeurt, dan wijst de FG erop dat het dan op de weg van de FG ligt om dit alsnog te doen. De toegang tot de gemeentesecretaris en de wethouder en het druk uitoefenen om de wethouder te informeren zijn de enige mogelijkheden die de FG heeft om naleving af te dwingen. Hij heeft geen zogenoemde *stopping power* om te eisen dat bijvoorbeeld acuut een verwerking wordt beëindigd. Het is namelijk aan de verantwoordelijke om te beslissen wat er uiteindelijk wordt gedaan; de FG kan enkel wijzen op de risico's en een advies geven. De FG zorgt er bovendien voor dat het bestuur goed geïnformeerd wordt. Dit om te voorkomen dat een project van start gaat met enkel enthousiaste verhalen, maar waarbij de kanttekeningen onvoldoende voor het voetlicht worden gebracht. De FG heeft dus geen *stopping power*, maar wel een adviesmogelijkheid. De FG ziet zichzelf uiteindelijk niet als politieagent, maar vindt het wel zijn taak om de lijnorganisatie en uiteindelijk het bestuur erop te wijzen en te benadrukken dat deze dient te komen tot een expliciete, afgewogen beslissing. Daarnaast doet de FG regelmatig zelf onderzoek. Zo voert de FG steekproeven bij datalekken uit en gaat hij na of maatregelen zijn getroffen om de onderliggende oorzaak weg te nemen. Bij uitgevoerde DPIA's gaat de FG na of de daarin benoemde mitigerende maatregelen zijn geïmplementeerd. Hij doet ook onderzoek naar de actualiteit van het register van verwerkingen. Deze onderzoeken hebben als achterliggend doel om bij de organisaties bewustzijn te creëren om deze aspecten ook zelf te controleren en, waar nodig, managementsystemen daarop aan te passen.

Binnen de tweede lijn en tussen de tweede en derde lijn vindt periodiek overleg plaats, zo komt naar voren uit de interviews. Om ervoor te zorgen dat alle privacy officers op hetzelfde informatieniveau zitten, is er elke twee weken een privacy officers overleg. Ook hebben de CPO , de FG en de CISO een keer in de drie weken overleg. Daarnaast vindt binnen deze organisatie een veelvoud aan overleggen plaats, waarbij thematisch tussen deze disciplines, maar ook met de integriteitsofficer en jurdische zaken in overleg wordt gegaan.

Uit de interviews is gebleken dat de cultuur in de organisatie niet altijd en overal overeenkomt met de ambities zoals geformuleerd in het beleid. Binnen de *three lines of defence* vormen de lijnorganisatie, de privacy officers en de FG een driehoek die gezamenlijk, maar vanuit hun eigen rol komen tot een juiste uitvoering van de AVG. In de praktijk blijkt volgens de geïnterviewden dat de eerste lijn vaak wel wil, maar niet weet wanneer of hoe ze moeten acteren. Dit is een struikelblok om tot AVG-compliance te komen. De tweede lijn ervaart onduidelijkheid over wat tweedelijns advisering precies inhoudt: is dat alleen advies geven aan de eerste lijn of ook hen meehelpen en verder op weg helpen zodat ze hun taken goed kunnen voldoen? In de praktijk zitten hier nog veel onduidelijkheden, waardoor de afstand tussen de eerste en tweede lijn groot is en niet als het ware naar elkaar worden toegezogen.

Inbedding van privacy in de organisatie

De FG valt rechtstreeks onder de algemeen directeur. De FG heeft toegang tot de algemeen directeur, de verantwoordelijk concerndirecteur en wanneer nodig tot de betrokken wethouder. Bij het aantreden van de FG heeft deze de algemeen directeur en de verantwoordelijk concerndirecteur om steun gevraagd en ook gevraagd deze steun te uiten tijden

personeelsbijeenkomsten. Dit heeft ertoe geleid dat de FG op toereikende toegang heeft tot de organisatie en vragen en verzoeken snel worden ingewilligd.

De functie van privacy officers is een fulltime functie binnen deze gemeente. In de praktijk heeft ieder cluster één of meerdere privacy officers. Afhankelijk van de grootte van de clusters en de taken van de clusters verschilt ook het aantal privacy officers; sommige clusters hebben er één, andere clusters vier. De clusters nemen daarbij zelf de verantwoordelijkheid voor het werven van privacy officers.

De privacy officers worden telkens gedwongen om tot een goede prioritering te komen. Naast advisering van de eerste lijn vechten de afhandeling van datalekken en de behandeling van verzoeken, waarbij de rechten van betrokkenen worden uitgeoefend om voorrang. Daarnaast kan een privacy officer ook nog betrokken zijn bij meerdere grote en soms ook complexe projecten of is deze betrokken bij clusteroverstijgende kwesties, waar een juiste samenhang bewaard moet worden. Wanneer een cluster maar één privacy officer heeft, komt dit allemaal op het bordje van die ene privacy officer. In de praktijk blijkt volgens de geïnterviewden dat de privacy officers geneigd zijn om niet te prioriteren en om alles tegelijkertijd op te pakken. Bovendien worden de vraagstukken steeds complexer en meer divers. Privacy officers hebben niet altijd de kennis om deze nieuwe vraagstukken goed op te pakken. Extra kennis en vaardigheden en tijd zijn nodig om die kennis en vaardigheden te kunnen ontwikkelen.

Wil tot AVG-compliance gekomen worden dient de eerste lijn tijdig de tweede lijn te betrekken bij beleidsvorming of de interpretatie daarvan en dient de tweede lijn haar rol te pakken. Uit de interviews komt het beeld naar voren dat dit nog geen automatisme is en nog onvoldoende is ingebed in de organisatie. Deels komt dit doordat mensen niet de vaardigheden hebben vraagstukken te herkennen of om die samenwerking te zoeken, maar ook omdat proceseigenaren onvoldoende tijd vrijmaken voor AVG-vraagstukken en dit al snel zien als iets van de ‘privacykolom’. Wanneer dit te vaak gebeurt, loopt de de ‘privacykolom’ over, waardoor meer afstand wordt genomen van de eerste lijn en zij hun rol anders invullen.

Factoren uit de interviews die kunnen bijdragen tot het verbeteren van de verbinding tussen de eerste en tweede lijn zijn het bij projecten aanwijzen van één verantwoordelijke uit de lijn voor AVG-vraagstukken. Als voorbeeld wordt genoemd een kwestie waarin de gemeenteraad wilde dat een bepaalde technische applicatie werd geregeld. Vervolgens is er één projectleider aangesteld voor het hele proces: de aanbesteding, technische implementatie, training van de betrokkenen, etc. Deze aanpak is ook daarna zeer succesvol gebleken.

Ook het aanwijzen van ambassadeurs kan als een succes worden aangemerkt. De ambassadeurs signaleren tijdig AVG-vraagstukken en brengen in de eerste lijn de juiste mensen bij elkaar, waaronder de privacy officers en/of de CPO. Die tijdige betrokkenheid is van belang om al voorafgaande aan een DPIA een ‘nulgesprek’ te kunnen laten plaatsvinden, bijvoorbeeld over de vraag of inzet van bijvoorbeeld algoritmen wel ethisch verantwoord is of dat het risico’s met zich meebrengt op het vlak van de bescherming van persoonsgegevens. Een dergelijk gesprek dient plaats te vinden ook wanneer bijvoorbeeld de gemeenteraad over een bepaalde verwerking van persoonsgegevens al besloten heeft. Binnen deze gemeente probeert de CPO bijvoorbeeld ‘aan de voorkant’ te gaan zitten van het proces door bijvoorbeeld in verkennende gesprekken te bespreken wat de wensen en ideeën zijn en wat wel en niet kan. Die gesprekken zijn van groot belang om draagvlak te creëren en tot elkaar te komen. Door met elkaar de privacyvraagstukken te formuleren en die vragen af te pellen, wordt het voor de eerste lijn behapbaar.

Praktijk

Opleiding en training

Bij het van toepassing worden van de AVG is een 'blijf alert' campagne gestart, gericht op het vergroten van bewustwording. Inmiddels is er een e-learning voor privacy en informatiebeveiliging opgezet. Dit is een basis e-learning voor de gehele organisatie. Daarnaast is er ook een verdiepingsmodule voor onder andere de ambassadeurs. Ook bestaan er plannen om een aantal mini-modules te maken ten aanzien van specifieke onderwerpen. Er bestaat al een dergelijke module voor de meldplicht datalekken, maar er wordt nu ook gekeken naar een minimodule voor inkoop. Ook wordt aan de hand van checklists en procesbeschrijvingen vastgelegd wanneer wie waarom moet aanhaken. Verder wordt bekeken of intranet meer kan worden ingezet om medewerkers te informeren. In het verleden, voor corona, werden ook sessies bij MT's belegd.

De invloed van de rapporten en handhavingsacties van de AP moeten niet worden onderschat. Dit biedt bijvoorbeeld de FG een podium om op specifieke onderwerpen het bewustzijn te vergroten. Ook geeft de FG duidelijk aan welke aspecten hij belangrijk vindt en goed dienen te worden uitgewerkt in de DPIA. Dit vergroot de alertheid in de eerste lijn, zo blijkt uit de interviews.

Processen

DPIA's

Een DPIA wordt doorgaans uitgevoerd door de privacy Officer, voorafgaand aan de verwerking en bij bestaande verwerkingen met een hoog risico. Bij het uitvoeren van een DPIA is het de wens dat iedereen bij elkaar komt om met elkaar de beste resultaten te bereiken. Zeker bij complexe verwerkingen, waaronder de inzet van algoritmes is het van belang dat de verschillende disciplines, waaronder security, privacy, informatiebeheer, data en ethiek) aan tafel zitten. Het proces om te komen tot een DPIA verloopt dan naar behoren. In een enkel geval loopt dit goed en is er geleerd van eerdere ervaringen en is er het besef dat de totstandkoming van een DPIA en de beoordeling daarvan tijd vergt. Hiervoor moeten vaardigheden worden ontwikkeld die nog niet in alle onderdelen van de organisatie aanwezig zijn.

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende verwerkersovereenkomst en het model Gegevensbeschermingseffectbeoordeling. Daarnaast houdt hij toezicht op het DPIA proces. De FG heeft een sturende rol. De eerste en tweede lijn weten waar hij op let en zorgen er ook voor dat in de DPIA's die aspecten goed worden uitgewerkt. Afhankelijk van het onderwerp wordt een handover-moment opgezet om met onder meer de proceseigenaar, afdelingsleiding, de FG, de privacy officers een aantal aspecten te bespreken: toelichting op het proces, belangrijkste risico's en wat nodig is om naleving AVG te borgen. Wanneer de FG een risico niet voldoende gemitigeerd acht voor een positief advies, dan kan de afdeling weer aan het werk gezet worden om daarvoor extra maatregelen te nemen, of om het risico beargumenteerd te nemen.

Datalekken

De gemeente heeft een Protocol Meldplicht en afhandeling van datalekken en een register om datalekken bij te houden. Hiertoe is de gemeente ook verplicht. De individuele medewerker is verantwoordelijk voor het doen van de eerste melding. De decentrale security officer van het

betreffende cluster is samen met de privacy officer verantwoordelijk voor het onderzoek naar een beveiligingsincident. De decentrale informatie security officer is verantwoordelijk voor regie op het dichten van het lek en de privacy officer voor het oppakken ervan. Het college is eindverantwoordelijk. Een datalek heeft altijd prioriteit bij een privacy officer en de FG.

De gedane meldingen en het datalek zelf worden in lijn met het protocol geëvalueerd. Zo wordt nagegaan wat precies is misgegaan en wordt gekeken naar de getroffen maatregelen. Een volgende stap zou kunnen zijn dat de eerste lijn zelf nagaat of die maatregelen ook daadwerkelijk zijn uitgevoerd en of die maatregelen ook werken. De FG monitort of het datalek in het register is opgenomen en of de maatregelen die getroffen moeten worden ook daadwerkelijk getroffen zijn.

Weging belangen, waaronder privacy

Dat de AVG een verwerking niet toelaat en dus strijdig is met de AVG, hoeft niet te betekenen dat een beslissing niet wordt genomen. De tweede en de derde lijn zijn zich ervan bewust dat het niet aan hen is om daarover te beslissen. Dat is uiteindelijk een bestuurlijke aangelegenheid, wel zorgen zij ervoor dat privacy als wegingsfactor in de uiteindelijke besluitvorming en de daaraan ten grondslag liggende belangenafweging wordt meegenomen. Soms kan het zijn dat een maatschappelijk belang zwaarder weegt. Dit betekent niet dat de AVG niet serieus genomen wordt. Ook in die gevallen worden waarborgen geformuleerd om zoveel mogelijk de AVG na te leven.

Indien blijkt dat aan bepaalde voorwaarden van de AVG niet kan worden voldaan, dan wordt een escalatieproces gehanteerd. De FG brengt in dat geval een advies uit, als dat niet wordt of kan worden opgevolgd, dan kan het geëscaleerd worden tot op het niveau van de concerndirectie. Er kan uiteindelijk besloten worden om toch door te zetten in afwachting van aanvullende maatregelen. Die ruimte is er, maar men doet dat niet zomaar. Uit de interviews blijkt een worsteling, omdat ook bij burgers verschillende belangen kunnen spelen (privacy versus goede handhaving bijvoorbeeld).

Samenwerking met derden

Wanneer de verwerkingsverantwoordelijke samen met anderen doel en middelen bepaalt, bijvoorbeeld in een samenwerkingsverband, dan kan sprake zijn van gezamenlijke verantwoordelijkheid. Bij elk samenwerkingsverband dient op basis van de eigen doelen, de samenstelling van de partners en de taken op basis waarvan zij samenwerken te worden gekeken naar de wettelijke grondslag en het doel van het verstrekken van informatie.

Voor individuele casussen (dus geen beleidsmatige taak) kan alleen een bestuursorgaan deelnemen vanuit een specifieke wettelijke taak. De persoonsgegevens die zij in een verband met een dergelijke taak verkrijgt, mogen niet zomaar voor andere doeleneinden worden gebruikt, tenzij de wet dat uitdrukkelijk toestaat. Voor gegevensuitwisseling op persoonsgerichte aanpak bij complexe problematiek is vanuit de VNG een handvat uitgebracht.

In het geval van ketensamenwerking moeten de partijen onderling duidelijke afspraken maken over wie invulling geeft aan de diverse rechten en plichten uit de AVG. Het is in het bijzonder van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen. Samenwerking en met name samenwerking door middel van een samenwerkingsverband wordt

als lastig en complex ervaren om de gezamenlijke verwerkingsverantwoordelijkheid op een overzichtelijke wijze in te vullen.

Controle en toezicht

Zie toelichting derde lijn van de *three lines of defence*.

Uitdagingen

Uit de interviews volgt dat de privacy officers beter in staat moeten worden gesteld om hun rol te pakken. Ook moet worden onderzocht hoe specifieke kennis kan worden verkregen en ingezet in de organisatie. De privacyvolwassenheid van de eerste lijn wisselvallig. Een concernbrede inzet om AVG automatisch als onderdeel van de taak te zien, is gewenst. Een verdere inbedding van het juist doorlopen van het DPIA-proces dient vanuit de eerste lijn prioriteit te krijgen. Dit begint met het onderkennen van het belang van het 'nulgesprek'. Een dergelijk gesprek wordt gehouden nog voordat de verwerkingsactiviteit ontwikkeld wordt, waarbij de verschillende belangen, waaronder het voldoen aan de AVG, besproken worden. Dit vergt wel dat de juiste mensen op het juiste moment met elkaar dat gesprek aangaan. Een dergelijk nulgesprek is zeker van belang waar het gaat om de inzet van algoritmes. Lessons learned uit geslaagde projecten of projecten die anderszins leerzaam zijn geweest, kunnen helpen bij het verkrijgen van de relevante inzichten die behulpzaam zijn bij de ontwikkeling van een verwerkingsactiviteit.

Analyse

Het volwassenheidsniveau op het gebied van privacy van deze organisatie omschrijft zich als een organisatie, waarop op het concernniveau heldere regels zijn gesteld en de privacyorganisatie positie heeft ingenomen. De bewustwording in de eerste lijn lijkt in ontwikkeling te zijn. Echter privacyvraagstukken worden nog niet altijd (tijdig) onderkent en de privacy officers zijn nog niet voldoende in staat concernbreed op te pakken.

Dimensies van spontane naleving

Kennis van regels
De wijze waarop de FG, de CPO en de concerndirecteur hun taak opvatten en daaraan invulling geven, vormen binnen deze gemeente een goede basis om op het vlak van privacyvolwassenheid tot een verdere groei te komen. Ook de aanwezigheid van ambassadeurs in organisatieonderdelen helpt daarbij, omdat zij – indien zij over voldoende kennis beschikken – tijdig AVG-vraagstukken kunnen herkennen en bij het ontplooien van activiteiten kunnen betrekken.

Ook wordt structureel ingezet op scholing van medewerkers over het belang van naleving van de AVG. Hiervoor worden zowel algemene als meer toegesneden cursussen aangeboden. De inzet op dit vlak is een voortdurend punt van aandacht.

Wel valt op dat de privacy officers, al dan niet vanwege gebrek aan capaciteit of onduidelijkheid in de taakopvatting, in onvoldoende mate in staat zijn op hun adviesrol concernbreed op

toereikende wijze vorm te geven. Dit kan de verdere groei van de privacyvolwassenheid van de eerste lijn in de weg staan.

Wat in positieve zin opvalt, is dat de privacy-organisatie rapporten en boetebesluiten van de AP goed weet aan te wenden om aandacht te vragen voor specifieke vraagstukken en om veranderingen in de processen door te laten voeren.

Kosten en baten
Binnen de gemeente wordt bij grotere of complexe verwerkingen, waaronder de inzet van algoritmes, de privacycomponent – mede door de aanwezigheid van ambassadeurs – als een van de aspecten gezien waar vroegtijdig aandacht aan moet worden besteed. Ook leeft het besef dat dit tijd kost, waarmee rekening moet worden gehouden in de planning. Daarbij is het behulpzaam dat het in de organisatie zeer helder is wat de FG belangrijk vindt en daarmee wat in de beoordeling van de verwerking moet worden meegenomen en wat wel of niet geaccepteerd wordt.

Aan de andere kant komt uit de interviews naar voren dat in overige gevallen de AVG nog onvoldoende op het netvlies van de eerste lijn staat en dat de vaardigheden ontbreken om deze te herkennen en tijdig onder de aandacht van de tweede en uiteindelijk derde lijn te brengen. Ook komt het voor dat verwerkingen of AVG-relateerde aspecten die niet door de beugel kunnen door de eerste lijn niet onder de aandacht van de bestuurder worden gebracht of dat bij projecten de privacyrisico's onvoldoende worden uitgelicht.

Mate van acceptatie
Binnen deze gemeente is er een groeiend besef dat de AVG integraal onderdeel is van de uitvoering van de wettelijke taken en bevoegdheden en wordt het voldoen aan de AVG ook belangrijk gevonden. Wanneer echter andere maatschappelijk belangen zwaarder wegen, kan het AVG-belang het onderspit delven. Ook in die gevallen wordt vervolgens getracht om voldoende waarborgen te treffen die in lijn zijn met de AVG.

Maatschappelijke controle
Vanuit de gemeenteraad worden met regelmaat AVG-kwesties geagendeerd en dat vormt vaak een trigger om over bepaalde privacy-aspecten na te denken. Het helpt vervolgens de tweede lijn om de organisatie in beweging te krijgen. De maatschappelijke ontwikkelingen die aldus worden geagendeerd kunnen gesprekspartners helpen om binnen de organisatie het verhaal meer te laten landen. De concern-privacy officer gebruikt dit als kapstok om privacy op de kaart te krijgen.

Omgekeerd geldt dat als een bepaald thema voor de raadsvergadering wordt geagendeerd en aan bepaalde vraagstukken privacy-aspecten kleven de concern-privacy officer hier doorgaans van op de hoogte wordt gesteld. Indien deze functionaris AVG-technische complicaties ziet, geeft deze geen akkoord. Deze escalatie kan ertoe leiden dat onder druk AVG-technische complicaties alsnog worden weggenomen om een thema tijdig op de agenda te krijgen.

Handhavingsdimensies
Toezicht en handhaving vindt vooral plaats door middel van intern toezicht. Dit betekent niet dat de AP op de achtergrond geen rol speelt. Er wordt, indien noodzakelijk, met de toezichthouder contact gezocht.

Andere relevante punten

De organisatie heeft een grote slag gemaakt met het register van verwerkingen, waarin ook aandacht is voor de uitgevoerde DPIA's. Daarnaast is van belang te noemen dat een ontwikkeling gaande lijkt te zijn dat de eerste lijn steeds meer de privacy-organisatie weten te vinden.

De concern-privacy officer en de FG overleggen met regelmaat met de andere grotere gemeenten. Tijdens deze overleggen worden gezamenlijke standpunten geformuleerd op bepaalde privacy-aspecten die ook richtinggevend kunnen zijn voor andere, kleinere gemeenten. Daarnaast wordt collegiaal advies gegeven. Ook wordt gezamenlijk contact gezocht met de AP om specifieke onderwerpen te bespreken.

Bijlage 12: Caseverslag gemeente 2

Inleiding

Deze casestudybeschrijving doet verslag van het onderzoek naar de naleving van de AVG in een middelgrote gemeente met iets minder dan 100.000 inwoners en een ambtelijke organisatie met ruim 600 werknemers. Deze zijn verdeeld zijn over zes afdelingen: Openbare Ruimte, Publiekszaken, Sociaal Plein, Interne Dienstverlening, Interne Advisering en Beleid en Ontwikkeling. Het is een gemeente die zichzelf ziet als een voorloper in gemeenteland op het gebied van AVG-naleving, maar waar nog voldoende uitdagingen en opgaven liggen voor de toekomst. Met name in het sociaal domein wordt geworsteld met soms conflicterende belangen bij de naleving van de AVG. Van grootschalige datalekken of calamiteiten is de afgelopen jaren geen sprake geweest.

In het kader van deze casestudy is gesproken met de privacy officer, de FG, de manager bedrijfsvoering en een teamleider Sociaal Domein. Het privacybeleid van de gemeente is bestudeerd.

Gegevensverwerking door de gemeente

Zoals alle gemeenten verwerkt de casestudygemeente veel persoonsgegevens van haar inwoners. Dat gebeurt bijvoorbeeld door het raadplegen van de Basisregistratie Personen (BRP) bij de uitgifte van paspoorten en rijbewijzen, bij het verlenen van omgevingsvergunningen, Alcoholvergunningen evenementenvergunningen etc. Ook worden dagelijks veel persoonsgegevens verwerkt bij de uitvoering van Participatiewet, de Jeugdwet en de Wet maatschappelijke ondersteuning, de Wet gemeentelijke schuldhulpverlening en de Wet passend onderwijs. Binnen het sociaal domein ligt dan ook het zwaartepunt van gegevensverwerking. De persoonsgegevens die er worden verwerkt zijn bovendien vaak ook van gevoelige aard. Hier liggen dan ook de grootste risico's, maar ook de meeste uitdagingen. Daarnaast is de gemeente als werkgever verantwoordelijk voor de verwerking van persoonsgegevens van de eigen medewerkers voor bijvoorbeeld de salarisadministratie.

Interne organisatie

Beleid

De privacy-organisatie van de casestudygemeente is in grote lijnen vastgelegd in het Privacybeleid 2020-2024. Dit beleid is vastgesteld door het college van burgemeester en wethouders.

Het beleid is van toepassing op de gehele organisatie en is primair gericht aan alle medewerkers die in het kader van hun taak persoonsgegevens verwerken. In werkplannen, procedures en werkinstructies wordt een verdere uitwerking gegeven aan de wijze waarop de bescherming van persoonsgegevens is geborgd. Het huidige herijkte privacybeleid was nodig om onder andere meer aandacht te vestigen op risicogestuurd werken, de visie van het gemeentebestuur in het digitale tijdperk en verbinding te maken met de planning & control-cyclus. Op basis van het jaarverslag van de functionaris voor gegevensbescherming (FG) is in een meerjarenplan van vier jaar uitgewerkt om de AVG binnen de gemeentelijke organisatie te borgen. Met de uitvoering van deze jaarplannen wordt beoogd het volwassenheidsniveau te bereiken waar de wetgever vanuit gaat.

Privacy-organisatie

Hieronder worden alle relevante stakeholders besproken en hun plaats binnen de -organisatie. De gemeente werkt via het *three lines of defence*-model, maar voor de volledigheid worden hier alle relevante spelers benoemd.

De raad

Het privacybeleid van de gemeentelijke organisatie wordt opgesteld door het college van burgemeester en wethouders en wordt gecontroleerd door de raad. De raad ziet erop toe dat het college overkoepelend beleid vaststelt ten aanzien van de wijze waarop de organisatie met persoonsgegevens omgaat. De raad stelt hiervoor middelen ter beschikking. De raad controleert het college bij de uitvoering van de gestelde kaders. De raad wordt hiertoe in staat gesteld door verantwoordingsinformatie die door de FG wordt aangeleverd zoals het jaarlijkse verslag van de FG.

Het college

Het college is integraal verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking binnen de organisatie. Hij is verantwoordelijk voor een duidelijk te volgen privacybeleid, doet aan de gemeenteraad voorstellen voor het beschikbaar stellen van middelen en stelt specifieke regelingen vast. Ook controleert hij het management van de verschillende organisatieonderdelen op de maatregelen die verband houden met de bescherming van persoonsgegevens. Het college heeft een portefeuillehouder aangewezen die namens het college de beleidsvoering waarborgt. De portefeuillehouder legt politieke verantwoording af aan de raad over het beleid en de uitvoering.

Gemeentesecretaris

De ambtelijke uitvoeringsverantwoordelijkheid voor gegevensbescherming ligt bij de gemeentesecretaris. De gemeentesecretaris is samen met de directie verantwoordelijk voor de uitvoering van het meerjarenplan, een juiste uitvoering van privacybeleid en sturing op (concern) risico's. Daarnaast zorgt de directie voor een passend niveau van informatieveiligheid en gegevensbescherming binnen de organisatie.

Lijnmanagers

De lijnmanagers vormen een centrale schakel binnen de privacy-organisatie. De verantwoordelijkheid voor zorgvuldige omgang met persoonsgegevens en de verwerkingen daarvan vallen onder de lijnmanagers van de verschillende vakafdelingen. Zij zijn procesverantwoordelijke. Dat houdt in dat zij verantwoordelijk zijn voor de nakoming van het naleven van de privacyregelgeving en het desbetreffende vakinhoudelijke privacybeleid binnen hun

organisatieonderdeel. Ook zijn de lijnmanagers verantwoordelijk voor het ontwikkelen en behouden van het bewustzijn van medewerkers omtrent privacy en gegevensbescherming.

De lijnmanagers zijn verantwoordelijk voor de volgende onderwerpen:

- Risicogestuurd werken. Hiervoor wordt gebruik gemaakt van de vastgestelde modellen van de DPIA-light en /of de 'schaal van erg' en/of Data Protection Impact Assessments (DPIA's).
- Naleving van principes van *privacy by design* & *default*
- Het hanteren van daartoe vastgestelde procesplannen en formats, zoals de DPIA en de (door de VNG vastgestelde) verwerkersovereenkomst.
- Dat datalekken volgens de daartoe te volgen procedure zo snel mogelijk bij de privacy officer of bij het Privacy & Informatieveiligheid Team (PIT) worden gemeld.
- Het opnemen van nieuwe verwerkingen en gewijzigde verwerkingen in het register van verwerkingsactiviteiten.
- Het informeren en het afhandelen van de rechten van de betrokkene
- Het maken van schriftelijke afspraken bij risicovolle verwerkingen en verwerkingen bij ketensamenwerking
- Het bijstaan van de uitvoering door professionals op het gebied van privacy en informatieveiligheid waar nodig
- Het bekend maken van het privacybeleid bij de medewerkers
- Ten slotte rapporteren de lijnmanagers via de gebruikelijke P&C-cyclus over de naleving van het beleid.

De lijnmanagers vormen samen met de medewerkers op de vloer de *first line of defence*.

Medewerkers op de vloer

Alle medewerkers (inclusief inhuurkrachten) zijn verantwoordelijk voor een zorgvuldige omgang met en verwerking van persoonsgegevens. Dat wil zeggen dat elke medewerker, binnen de kaders van zijn of haar taak en verantwoordelijkheid, zorgt voor een zorgvuldige, rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Wanneer er twijfels rijzen over hoe in een bepaalde situatie te handelen, dan zijn de lijnmanager of het Privacy-informatieteam de aangewezenen om hulp en advies in te winnen.

Specifieke ondersteuningsfuncties

Naast het beleggen van verschillende verantwoordelijkheden bij de bovengenoemde bestuurders, lijnmanagers en medewerkers zijn ook de rollen van een aantal specifieke privacyfunctionarissen beschreven.

- De FG bekleedt een zelfstandige positie binnen de organisatie en is met een aantal taken belast. Zo informeert en adviseert hij over de werking van de AVG, overige wetgeving en het gemeentelijke privacybeleid, houdt hij toezicht op naleving van het privacybeleid, vervult hij een ombudsfunctie bij privacygerelateerde klachten, adviseert hij bij privacy-incidenten binnen de organisatie, ziet hij toe op het beheer het register van verwerkingen (artikel 30 AVG), helpt hij het privacybeleid uit te dragen en bewustzijn te creëren en is hij het contactpunt voor de landelijke toezichthouders, waaronder de AP. Het uitgangspunt is dat de FG tijdig wordt betrokken bij aangelegenheden waarbij de verwerking van persoonsgegevens in het geding zijn. Ook dient hij volledig te

worden geïnformeerd over bedrijfsvoeringsprocessen waarbij persoonsgegevens worden verwerkt of wanneer daartoe het voornemen bestaat. De FG is onafhankelijk. Dat wil zeggen dat hij niet geïnstrueerd wordt over de wijze waarop hij zijn taak uitvoert. De FG fungeert als *third line of defence*. De gemeente heeft bewust gekozen voor een externe FG om zo de onafhankelijkheid te benadrukken.

- De privacy officer is de verbindende schakel tussen de organisatie en de FG. Hij/zij ondersteunt vanuit de tweede lijn bij vraagstukken omtrent de bescherming van persoonsgegevens. De privacy officer stelt het meerjarenplan op en rapporteert jaarlijks aan de directie en de portefeuillehouder op basis van deze plannen. Daarnaast coördineert de privacy officer de uitvoering van het meerjarenplan, waar nodig in samenwerking met de FG. Tevens stelt de privacy officer beleidsnotities en werkinstructies op en laat deze vaststellen door directie en /of de portefeuillehouder. Gevraagd en ongevraagd adviseert de privacy officer over activiteiten ter bescherming van persoonsgegevens.
- De CISO ondersteunt en adviseert op het gebied van privacy. Op het gebied van informatiebeveiliging heeft hij een controlerende en toezichthoudende taak. Omdat informatiebeveiliging nauw verwant is aan naleving van privacywetgeving adviseert hij (vooraf) bij projecten en het beheersen van risico's.
- De security officer is verantwoordelijk voor het vormgeven en bewaken van het informatieveiligheidsbeleid. Daarnaast heeft hij of zij een ondersteunende functie bij het in kaart brengen van risico's omtrent informatiebeveiliging en adviseert bij het treffen van maatregelen voor informatiebeveiliging.
- De Adviseur Informatie is de expert op het gebied van de gemeentelijke producten, informatiestromen, processen en informatiesystemen. Hij is een centrale schakel binnen de privacy-organisatie en hij adviseert op vraagstukken die betrekking hebben op verwerking en bescherming van persoonsgegevens.
- De juristen van het team Juridische Zaken ondersteunen indien juridische expertise wenselijk is bij bijvoorbeeld complexe inzageverzoeken.

Privacy Informatieveiligheidsteam (PIT)

Naast de hierboven beschreven specifieke ondersteunende functies op het gebied van privacy en gegevensbescherming wordt de organisatie ondersteund door het Privacy en Informatieveiligheidsteam (PIT). Het PIT vormt binnen de privacygovernance van de gemeente de tweede lijn.

Dit team bestaat uit een vast kernteam van professionals, waaronder de hierboven beschreven functionarissen, eventueel en zo nodig aangevuld met de FG. Dit team overlegt op periodieke basis, maar kan ook op afroepbasis samenkomen als daar aanleiding toe is. Zo nodig wordt het team aangevuld met medewerkers vanuit de vakafdelingen. Dat zijn medewerkers die affiniteit dienen te hebben met privacyregelgeving en de wijze waarop deze doorwerken binnen de processen op de afdeling. Door hun coördinerende functie kan dit team bewaken dat binnen de organisatie aandacht is voor privacy en bijsturen als de teamleden van mening zijn dat dit onvoldoende is. Uit gesprekken blijkt dat het PIT nog meer zou kunnen inzetten op preventie en bewustzijn. Nu bestaan de werkzaamheden in grote mate uit het uitvoeren van audits binnen de organisatie. Het PIT een grotere rol geven in het vergroten van het bewustzijn bij medewerkers vraagt tegelijkertijd ook iets in de persoonlijke kenmerken van de PIT-leden. Proactief het 'AVG-verhaal' uitdragen vraagt namelijk om bepaalde vaardigheden om de boodschap op de juiste manier onder de aandacht te brengen.

Inbedding in de organisatie

De privacy officer en de CISO zijn ondergebracht in het team Informatiemanagement dat valt onder de afdeling Interne Dienstverlening. De functies vallen normaliter onder de concerndirecteur en dus niet in de lijn, maar over de verschillende afdelingen heen. Omdat de functie van concerndirecteur vacant is, vallen de CISO en de privacy officer hiërarchisch onder het afdelingshoofd Interne Dienstverlening. Dat is dus niet ideaal, maar in de praktijk goed werkbaar. Het levert vooralsnog geen problemen op, is de ervaring. Het wordt vooral van belang geacht dat de privacy officer en de CISO het goede gesprek voeren binnen de organisatie over gezamenlijke opgaven en dat zij zich door hun manier van werken en profileren positioneren in de organisatie. Ze moeten niet als last worden gezien, maar als toegevoegde waarde. Dat zit niet in hiërarchische positionering, maar in houding en gedrag.

Praktijk

Opleiding en training

De gemeente besteedt op verschillende manieren aandacht aan het bewustzijn van medewerkers op het gebied van informatiebeveiliging en de veilige omgang met (persoons)gegevens. In 2020 is gestart met een driejarig bewustwordingsprogramma. Dat houdt in dat iedere medewerker e-learning modules moet volgen. De eerste module die wordt aangeboden gaat over informatiebeveiliging. De tweede module gaat over privacy, datalekken en het rechtmatig verwerken van persoonsgegevens. Alle medewerkers dienen deze modules te doorlopen en met goed gevolg af te sluiten.

Het programma start met een nulmeting om inzicht te hebben in de startsituatie. Bij de daaropvolgende metingen kunnen de verbeteringen – na maatregelen die zijn genomen om het bewustzijn van medewerkers te versterken – inzichtelijk worden gemaakt. Of dergelijke trainingen echt beklijven wordt door een van de gesprekspartners betwijfeld. Ze kunnen een bijdrage leveren aan het privacybewustzijn, maar voor het daadwerkelijk verinnerlijken daarvan is meer nodig dan dat.

Ter vergroting van het informatieveiligheidsbewustzijn worden naast dit programma nog andere activiteiten uitgevoerd. Zo krijgen alle medewerkers de 'Gouden regels Informatiebeveiliging en Privacy' uitgereikt (bij het begin van dit traject en wanneer ze nieuw in dienst komen). Daarin is vastgelegd welke eisen aan medewerkers worden gesteld en wat hun verantwoordelijkheden zijn.

Naast het bewustwordingsprogramma vervult de privacy officer een belangrijke functie in het scholen en trainen van medewerkers. De privacy officer schuift regelmatig aan tijdens werkoverleggen van de vakafdelingen om daar de betekenis van privacy onder de aandacht te brengen en hoe dit doorwerkt in de primaire processen. In de praktijk blijkt dat een uitdaging te zijn; het is soms lastig om de vertaalslag te maken tussen een juridische werkelijkheid van de AVG en de dagelijkse praktijk van de vakafdelingen. Ook wordt er vanuit het MT niet op toegezien dat privacy en informatiebeveiliging voldoende geagendeerd worden tijdens teamoverleggen.

Daarnaast geeft de privacy officer gevraagd en ongevraagd advies. Dat gebeurt bijvoorbeeld door aan de voorkant te adviseren bij bijvoorbeeld nieuwe projecten of inkoop. Het risico dat wordt ervaren bij het nadrukkelijk onder de aandacht brengen van het belang van privacy, is

dat het in de organisatie als 'drammerig' wordt ervaren. Wanneer aandacht vragen voor het belang van privacy op de verkeerde wijze en op de verkeerde toon plaatsvindt, kan dit een contraproductief effect hebben. Medewerkers kunnen het ervaren als een extra last die 'erbij gedaan' moet worden. De privacy officer ziet het daarom als zijn/haar rol om de boodschap op de juiste manier over te brengen zodat men ontvankelijk wordt voor het belang van privacy. De privacy officer stuurt er bij de verschillende vakafdelingen op aan hem/haar aan de voorkant te betrekken en hem/haar daarop te attenderen. Ook dat bewustzijn moet groeien. Deze rol en verantwoordelijkheid wordt momenteel vooral door de privacy officer opgepakt, maar omdat hij een éénpitter is zijn de mogelijkheden daartoe beperkt. Een van de gesprekspartners geeft aan dat ook het PIT hier een actievere rol in zou moeten nemen. Een gemiste kans die daarnaast gesignaleerd wordt, is dat er nog onvoldoende geleerd wordt van gemaakte fouten. Incidenten rond datalekken zouden als leerstof/casuïstiek kunnen dienen, dat gebeurt nu niet of nauwelijks.

De privacy officer neemt eens per zes weken deel aan een regionaal overleg met andere privacy officer's. Verder is er weinig tijd voor de privacy officer om aan eigen bijscholing te doen. De volle agenda laat dat niet toe. In de ideale situatie zouden er meerdere decentrale privacy officer's zijn, maar daarvoor worden geen middelen vrijgemaakt. Dat is een kosten-baten afweging die door de organisatie gemaakt wordt. Er zijn bovendien nog geen grootschalige of ernstige incidenten geweest, wat de noodzaak tot decentrale privacy officer's verkleint.

Een belangrijk begrip in de wijze waarop naleving van de AVG gestalte moet krijgen is door begrip eigenaarschap een centrale plek te geven. De FG geeft aan dat naleving van de AVG niet primair gaat om waarborgen van privacy, maar om het centraal stellen van de betrokkene om wie het gaat. In het geval van de gemeente, de inwoner. Gegevensverwerking moet zo georganiseerd zijn dat het ten dienste staat van de burger.

Processen

Risicogericht toezicht

De gemeente heeft in het huidige privacybeleid de bewuste keuze gemaakt om meer in te zetten op risicogestuurd toezicht. De gedachte die daarachter schuilgaat is dat voor het vaststellen van risico's een objectieve beoordeling nodig. Er dient gekeken te worden naar de waarschijnlijkheid dat zich iets ernstigs voordoet. Voorbeeld: de webcare afdeling van de gemeente maakt gebruik van Whatsapp om te communiceren met inwoners. Hoeveel schade levert het op dat deze gegevens opgeslagen worden op de server van een Amerikaans bedrijf? Dat hoeft niet per definitie een probleem te zijn. Dergelijke angst wordt elkaar veelal ingepraat waardoor ervan afgezien wordt gebruik te maken van een dergelijke bruikbare en klantvriendelijke toepassing. Zie je ervan af, dan maak je dus een punt van een formaliteit. Het is belangrijker dat er gekeken wordt naar eventuele impact en risico's van het gebruik van zo'n toepassing. Het opslaan of verwerken van gegevens is namelijk niet direct slecht of een schending van de privacy. Hiervoor is eerst die objectieve beoordeling nodig. De gemeente hanteert hiervoor een matrix om risico's in kaart te brengen.

Het risico wordt bepaald door zowel de kans en de impact van bepaalde negatieve gevolgen van fouten te beoordelen. Een grote kans op een kleine impact kan dus resulteren in een risico met score 'midden'. Tegelijk kan een zeer kleine kans op een hoog risico ook resulteren in score 'midden'.

De risico-inschatting wordt gemaakt met medewerkers die nauw bij het nieuwe project, de beleidsontwikkeling of het proces betrokken zijn.

Inventarisatie van werkprocessen
Verschillende aspecten van het privacybeleid van de gemeente zijn uitgewerkt in regels, procedures en werkprocessen. Een belangrijk aspect van het beleid is dat alle werkprocessen binnen de organisatie worden geïnventariseerd en aangepast op vereisten met betrekking tot privacy en informatiebeveiliging. De coördinatie van deze opdracht wordt ingevuld door het PIT. De verantwoordelijkheid voor het inventariseren van de werkprocessen en het aandacht besteden aan het waarborgen van de privacy ligt bij de betrokken lijnmanagers.

Vooralsnog zijn er door de FG meer dan zo'n dertien werkprocessen geïdentificeerd. De FG heeft in 2018 de organisatie geadviseerd om voor deze processen op basis van een zogeheten DPIA een procesplan op te stellen en te implementeren om zo in die werkprocessen vaste afspraken te maken voor een correcte omgang met privacygevoelige gegevens. Momenteel zijn nog niet alle genoemde werkprocessen doorgelicht op privacyrisico's.

De privacy officer zou graag meer tijd willen hebben voor de ontwikkeling van werkprocessen en -instructies en eenduidig organisatiebreed beleid. Vanwege de vele ad hoc verzoeken die de privacy officer krijgt is hier echter weinig tijd en ruimte voor. De privacy officer wordt momenteel pas vaak op het eind van een proces gevraagd of mogelijke privacy-aspecten een rol spelen waarmee rekening moet worden gehouden al wordt de privacy officer steeds vaker aan de voorkant betrokken. Dat komt door toenemend bewustzijn binnen de organisatie.

DPIA's
De AVG draagt op tot het nemen van passende maatregelen. De gemeente maakt gebruikt van een DPIA als risico-inventarisatie. Een DPIA moet altijd worden gedaan voorafgaand aan de start van een geautomatiseerde verwerking, bijvoorbeeld bij cameratoezicht. Bij een grootschalige verwerking of wanneer er een grootschalige monitoring van openbare ruimten wordt beoogd, geldt ook een DPIA, bijvoorbeeld bij Smart City toepassingen. Ook bij bestaande verwerkingen kan een DPIA worden uitgevoerd. Het gaat dan om verwerkingen waarbij:

- een hoog risico geldt, bijvoorbeeld bij processen in het sociaal domein of openbare orde en veiligheid;
- nieuwe technologieën worden toegepast;
- de context van de verwerking verandert door maatschappelijke ontwikkelingen;
- organisatorische veranderingen spelen die van invloed zijn op de verwerking.

De intentie is om op alle bestaande verwerkingen een DPIA-light uit te voeren om in beeld te krijgen welke risicovolle verwerkingen er binnen de gemeente plaatsvinden. De DPIA's met een hoge risicoscore worden aan de FG voorgelegd.

Een compleet overzicht van processen waar een DPIA moet worden uitgevoerd is er niet. Idealiter beslist de proceseigenaar of een DPIA nodig is, maar in de praktijk is het momenteel vooral de privacy officer die daartoe adviseert of het initiatief neemt. Als de lijnmanager al niet onbewust nalaat aan te geven dat een DPIA moet worden uitgevoerd, blijft dit buiten beeld. Het uitvoeren van een DPIA is op zichzelf niet altijd een complexe procedure, maar soms is de organisatie zelf complex waardoor DPIA's niet altijd worden afgerond. Dat komt bijvoorbeeld doordat mensen die betrokken zijn bij de totstandkoming van een DPIA gedurende het

proces de organisatie verlaten en er geen directe vervanging is. In de praktijk blijft zo'n DPIA dan nogal eens liggen. Ook komt het nog voor dat er geen DPIA is uitgevoerd, terwijl achteraf blijkt dat dit wel had gemoeten. De praktijk is daarmee dus nog niet helemaal in overeenstemming met het beleid. Het uitvoeren van DPIA's wordt volgens gesprekspartners nog te vaak als een 'moeten' ervaren.

Grote risico's met gegevensverwerking doen zich voor in het sociaal domein. Om die reden is een kwaliteitsmedewerker aangesteld die het thema privacy als taakaccent heeft meegekregen. Diegene fungeert als vooruitgeschoven post van de privacy officer. De kwaliteitsmedewerkers privacy moet iemand zijn die affiniteit heeft met het onderwerp, anders heeft het weinig zin. De kwaliteitsmedewerkers controleren in algemene zin of bijvoorbeeld de besluiten en de besluitvorming zorgvuldig zijn. De accenthouder privacy let specifiek op de privacyaspecten binnen de afdeling en kijkt gevraagd en ongevraagd mee met de medewerkers op de vloer. De kwaliteitsmedewerker privacy probeert hierin zo benaderbaar mogelijk te zijn. Ook binnen de afdeling Publiekszaken is er zo'n vooruitgeschoven post aangesteld die zich specifiek met privacy bezighoudt.

De kwaliteitsmedewerkers krijgen AVG-training specifiek voor hun domein. De wens is om bij alle afdelingen van de organisatie dit soort kwaliteitsmedewerkers aan te stellen, maar dit stuit nog op weerstand in de organisatie. Privacy wordt dikwijls ervaren als iets extra's dat erbij moet, als een lastige verplichting die afleidt van de hoofdtaak.

Binnen het team Jeugd wordt het binnen het kader van de persoonsgerichte aanpak zaken aangemeld door verschillende instanties, zoals politie en Veilig Thuis en vindt er veelvuldig contact plaats met zorgaanbieders. Voorheen verliep alle communicatie per mail. Dat voelde niet goed, vertelt een direct betrokkene van de gemeente. Het mailverkeer bevatte persoonsgegevens van vaak gevoelige aard. Het was ondoenlijk om het mailverkeer van persoonsgegevens te ontdoen. Daardoor is ervoor gekozen om via een beveiligde applicatie berichten uit te wisselen met zorgaanbieders. Voorafgaand aan het gebruik van dit geautomatiseerde systeem is een DPIA uitgevoerd. Daaruit blijkt dat hiermee aan de privacy-eisen wordt voldaan. De zorgaanbieders waren geen voorstander van dit systeem omdat zij met meerdere gemeenten moeten communiceren. De gemeente heeft in het privacyconvenant met de zorgaanbieders vastgelegd dat uitsluitend informatie uitgewisseld mag worden met behulp van de specifieke beveiligde applicatie.

Datalekken

Als er sprake is van een datalek en dat grote gevolgen kan hebben voor de betrokkene, bijvoorbeeld identiteitsfraude, informeert de verwerkingsverantwoordelijke de betrokkene in eenvoudige en heldere taal. Alle meldingen, en de wijze van afhandeling, worden in een register bijgehouden. De procedure die moet worden gevolgd is voor medewerkers te vinden op het intranet. Er is een meldformulier die medewerkers hiervoor kunnen gebruiken. De privacy officer ontvangt het meldformulier van de medewerker die het datalek ontdekt. De privacy officer neemt vervolgens contact op met de melder en beoordeelt of het datalek dermate ernstig is dat hiervan melding moet worden gedaan bij de AP. De beoordeling vindt dus niet plaats in het PIT. De handelswijze wordt achteraf wel altijd besproken in het PIT.

De meldingsbereidheid van medewerkers fluctueert, zo is de ervaring. Over het algemeen durven medewerkers een datalek dat zijzelf veroorzaakt hebben wel te melden bij de privacy officer. Er wordt bewust aan gewerkt om de drempel te verlagen om een datalek te melden. Dat wordt gedaan door actief duidelijk te maken binnen de organisatie dat er in principe niet bestraffend opgetreden zal worden bij een datalek. Waar gewerkt wordt, worden fouten gemaakt, is de gedachte. De privacy officer stuurt er bij de teammanagers op aan die boodschap uit te dragen onder de medewerkers. Tussen 2018 en 2020 steeg het aantal gerapporteerde datalekken van 15 naar 24. Dit wijst niet zozeer op een toenemende onzorgvuldigheid in de omgang met privacygevoelige informatie, maar eerder op een grotere alertheid in de organisatie op mogelijke incidenten.

Steun vanuit de top

Vanuit management komt steeds meer steun en aandacht voor het belang van naleving van de AVG. De nieuwe gemeentesecretaris heeft daar ook een belangrijke impuls aan gegeven. Toch voelt het voor de privacy officer nog steeds als een strijd die gevoerd moet worden binnen de organisatie om medewerkers te doordringen van het belang van naleving van de AVG. Dat kost veel energie. De steun vanuit het management is er, maar zou nog sterker benadrukt kunnen worden.

Elk kwartaal stelt het PIT een rapportage op met resultaten. Deze worden altijd serieus besproken in het MT en met de portefeuillehouder. Het belang van naleving wordt door het gehele MT onderschreven, maar het lukt nog niet altijd om op juiste wijze de vertaalslag naar de werkvloer te maken. Dat is een proces dat nog volop in ontwikkeling is, maar waar nog geen pasklare methoden voor zijn. Hierin is de organisatie nog zoekende.

Controle en toezicht

De gemeente heeft een externe FG benoemd. Dat is een bewuste keuze geweest om de onafhankelijkheid van de toezichthouder te benadrukken. In de visie van de FG is zijn werk maar heel beperkt, mits de 1e en 2e lijn goed hun werk doen. De taken die voor de FG overblijven gaan met name om het bieden van ondersteuning, het afhandelen van klachten en een vinger aan de pols houden. Met inhoudelijke zaken waarvoor de 1e en 2e lijn verantwoordelijk zijn dient de FG zich niet bezig te houden.

In de samenwerking tussen de privacy officer en de FG wil het wel eens schuren, al wordt dat niet direct als negatief ervaren. Verschillende visies leiden soms tot discussies waarbij uiteindelijk de FG een doorslaggevende stem heeft. Binnen de organisatie is nog niet altijd voldoende helder wat de precieze taak van de FG en van de privacy officer is.

Samenwerking met derden

Wanneer de verwerkingsverantwoordelijke samen met anderen doel en middelen bepaalt, bijvoorbeeld in een samenwerkingsverband, dan kan sprake zijn van gezamenlijke verantwoordelijkheid. Bij elk samenwerkingsverband dient op basis van de eigen doelen, de samenstelling van de partners en de taken op basis waarvan zij samenwerken te worden gekeken naar de wettelijke grondslag en het doel van het verstrekken van informatie.

Voor individuele casussen (dus geen beleidsmatige taak) kan alleen een bestuursorgaan deelnemen vanuit een specifieke wettelijke taak. De persoonsgegevens die zij in een verband met een dergelijke taak verkrijgt, mogen niet zomaar voor andere doeleneinden worden gebruikt, tenzij de wet dat uitdrukkelijk toestaat. Voor gegevensuitwisseling op persoonsgerichte aanpak bij complexe problematiek is vanuit de VNG een handreiking uitgebracht.

In het geval van ketensamenwerking moeten de partijen onderling duidelijke afspraken maken over wie invulling geeft aan de diverse rechten en plichten uit de AVG. Het is in het bijzonder van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen. Bij onduidelijkheden of complexe verhoudingen tussen de verwerkingsverantwoordelijke en de derde partij onder de AVG wordt altijd contact gezocht worden met de privacy officer, zodat bekeken kan worden welke afspraken eventueel gemaakt moeten worden.

Uitdagingen

Een eerste belangrijk knelpunt – en tevens verbeterpunt – is om beleidsprocessen regelmatig en op zorgvuldige wijze te toetsen op de wijze waarop met gegevens van inwoners wordt omgegaan. Daaraan ontbreekt het nog te vaak. Ook zou er beter zicht moeten komen op de vraag in welke gevallen een DPIA moet worden uitgevoerd en dient ervoor zorg gedragen te worden dat de juiste kennis en expertise daarbij aan tafel zit. Het lijnmanagement moet daar meer verantwoordelijk voor gaan dragen.

Bewustwording en bewustzijn over het belang van naleving van de AVG moet worden versterkt. Wanneer medewerkers daarvan beter doordrongen zijn vergemakkelijkt dit ook het werk voor de privacyofficer. Die hoeft dan minder te ‘sleuren’ om het belang onder de aandacht te brengen. Hoe groter het draagvlak voor naleving binnen de organisatie is, des meer kan de privacyofficer zich focussen op de inhoud en de wijze waarop die naleving gestalte kan krijgen.

De positie van de FG en de privacyofficer is nog onvoldoende duidelijk. Wie is waarvoor verantwoordelijk en wie kan op welk moment ergens bij betrokken worden of worden bevraagd. Daarover is op dit momenteel nog onvoldoende duidelijkheid. Wanneer daarin meer duidelijk wordt gecreëerd sluit de rolinvulling beter aan bij het *three lines of defence*-model.

Analyse

Op basis van de theorie van de Tafel van 11 zijn er elf factoren die kunnen verklaren waarom regels wel of niet worden nageleefd. De belangrijkste factoren die op grond van de bevindingen op deze gemeente van toepassing zijn worden hieronder toegelicht.

Dimensies van spontane naleving

Kennis van regels
De gemeente is in 2020 gestart met verplichte bewustwordingsprogramma’s rondom privacy. Medewerkers zijn verplicht om aan e-learnings deel te nemen waarin de kennis over privacy wordt getoetst. Het programma startte met een nulmeting waarna gerichte maatregelen worden genomen om het bewustzijn te versterken. Ook krijgen medewerkers sinds 2020 een handreiking met de belangrijkste principes rondom privacy en gegevensverwerking. Daarmee

stuurt de gemeente actief op het verinnerlijken van het belang van privacy binnen de verschillende processen. De rol van de privacy officer draagt ook bij aan het vergroten van het bewustzijn door gevraagd en ongevraagd te adviseren over privacy en gegevensverwerking. Het periodiek aanschuiven bij werkoverleggen binnen de verschillende afdelingen draagt bij aan het vergroten van het bewustzijn onder medewerkers. Het is echter de vraag of dit momenteel voldoende is, daar de privacy officer nog steeds signalen krijgt dat sommigen privacy lastig vinden en een extra last bovenop de primaire taken.

Kosten en baten
Uit de gesprekken blijkt dat het belang van de AVG nog niet overal verinnerlijkt is binnen de organisatie. Dat leidt ertoe dat medewerker het naleven van de AVG vaak nog als iets lastigs zien 'wat men erbij moet doen'. Wanneer de tijdsdruk hoog is kan men in een kosten-baten-afweging terecht komen om al dan niet de AVG na te leven als het proces hierdoor langer duurt. DPIA's kunnen dan mogelijk terzijde worden geschoven omdat de kosten niet opwegen tegen de baten. In dit verband hangt deze factor nauw samen met 'kennis van regels'. De baten van naleving kunnen immers alleen op de juiste manier gewogen worden op het moment dat men kennis van de regels heeft en snapt welke meerwaarde naleving heeft.

Mate van acceptatie
Binnen het sociaal domein kunnen de belangen van de inwoner/cliënt botsen met het belang van naleving van de AVG. Dat kan in de praktijk tot gevolg hebben dat er 'losjes' met de bepalingen uit de AVG wordt omgegaan omdat men vindt dat in bepaalde situaties het belang van de inwoner/cliënt prevaleert door bijvoorbeeld onrechtmatig gegevens toch te delen.

Maatschappelijke controle
Uit de gesprekken is niet gebleken of en in welke mate deze factor van invloed is op het nalevingsgedrag. Uit gesprekken is niet gebleken dat de invloed en mogelijke sanctionering (en het ontbreken daaraan) van AP een drijfveer vormt vorm normnaleving.

Handhavingsdimensies
Handhaving is van invloed op de vraag of medewerkers geneigd zijn zich te houden aan het protocol voor het melden van datalekken. Vanuit het management en de privacy officer wordt erop aangedrongen bij medewerkers om datalekken altijd te melden. Er wordt nadrukkelijk gewezen op het feit dat er (in beginsel) geen consequenties zitten aan het melden van een datalek. Waar gewerkt wordt worden immers fouten gemaakt, is gedachte die wordt uitgedragen. De stijging van het aantal datalekmeldingen hebben volgens deze verklaring daarom niet te maken met toenemende onzorgvuldigheid, maar met een grotere bereidheid om een datalek te melden.

Bijlage 13: Caseverslag gemeente 3

Inleiding

In dit hoofdstuk wordt de praktijk beschreven van de toepassing en naleving van de AVG door een kleine gemeente. De gemeente heeft te maken gehad met een incident op het gebied van informatiebeveiliging, waarbij potentieel gegevens van medewerkers en inwoners zijn gelekt. Door de beperkte omvang van de organisatie is de privacy-organisatie ook relatief beperkt en kent deze daarmee ook haar kwetsbaarheden. De gemeente is een belangrijke verwerker van persoonsgegevens en ziet zich geconfronteerd met grote uitdagingen met betrekking tot de taakuitvoering, met name ook in het sociaal domein.

In de casestudy is gesproken met de directeur, een concern-controller, de FG en een juridisch medewerker. De juridisch medewerker was lid van de kerngroep AVG. Deze kerngroep is, kort gezegd, belast met de monitoring van de kwaliteit van de privacybescherming binnen de gemeente. De gemeente heeft een document over de privacy-governance, het privacybeleid en een viertal rapportages met betrekking tot het beveiligingsincident verstrekt.

Gegevensverwerking door de organisatie

De gemeente is bij uitstek een overheidsorganisatie waarmee inwoners veel contact hebben. Zo verzorgt zij onder meer het beheer van de Basisregistratie Personen (BRP) voor wat betreft de inwoners van de gemeente, waarin voor alle inwoners van Nederland persoonsgegevens zijn geregistreerd zoals namen, geboortedatum, geslacht, nationaliteit en gezinsrelaties. Deze gegevens worden ook gebruikt door andere (semi-)overheden.

Voor de uitvoering van gemeentelijke taken verwerkt de gemeente ook in grote mate persoonsgegevens. Zo worden in het fysieke domein bijvoorbeeld gegevens verwerkt met betrekking tot vergunningen, en worden regelmatig gegevens verwerkt ten behoeve van beleidsuitvoering op het gebied van mobiliteit, energie, veiligheid en huisvesting. Het zwaartepunt van de gemeentelijke gegevensverwerking ligt in het sociaal domein: gemeenten zijn onder meer verantwoordelijk voor uitvoering van taken op het gebied van de Jeugdwet, de Wet maatschappelijke ondersteuning, de Participatiewet, de Wet gemeentelijke schuldhulpverlening en de Wet passend onderwijs. Daarbij worden veel persoonsgegevens verwerkt die bovendien vaak gevoelige informatie bevatten.

De gemeente is tenslotte ook een grote werkgever. Bij de bestudeerde gemeente gaat het om meer dan 200 werknemers, waarvan ook gegevens worden verwerkt ten behoeve van personeelszaken en dergelijke.

Interne organisatie

Beleid

In 2019 heeft de gemeente het privacybeleid vastgesteld. In dit document is beschreven hoe werkprocessen worden georganiseerd conform de AVG, wordt in grote lijnen de privacy-organisatie beschreven, wordt het juridisch kader voor verwerking van persoonsgegevens beschreven, worden rechten van betrokkenen en de omgang met de uitoefening daarvan beschreven. Ook wordt er ingegaan op algemeen te verwachten zaken zoals het verwerkingsregister, informatiebeveiliging, bewaartermijnen en de omgang met datalekken. Daarnaast worden er voor de gemeente meer specifieke onderwerpen beschreven zoals de geautomatiseerde gegevensverwerkingen, informatiewisseling met derden en de Baseline informatiebeveiliging overheid (BIO) die als beleidskader geldt.

In een apart document, vastgesteld in 2021, wordt de privacygovernance besproken, waarin de rollen, taken en verantwoordelijkheden met betrekking tot dit onderwerp aan bod komen.

Privacy-organisatie

In het governancedocument is vastgelegd dat de bestuurlijke en ambtelijke verantwoordelijkheid respectievelijk bij het college van B&W en bij de gemeentesecretaris liggen. Ook is vastgelegd dat de afdelingsmanagers als eigenaren van de persoonsgegevens verantwoordelijk zijn voor integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens. De verantwoordelijkheid bij de dagelijkse gang van zaken omtrent gegevensverwerking is volledig gedecentraliseerd neergelegd bij teamcoördinatoren en bij alle medewerkers die betrokken zijn bij processen waarbij persoonsgegevens worden verwerkt. Op dit niveau is dus de verantwoordelijkheid belegd voor onder meer bijhouden van het verwerkingsregister, initiëren en uitvoeren van DPIA's, beheer van verwerkersovereenkomsten, acteren bij veiligheidsincidenten (onder meer melden bij de AP) en creëren van bewustzijn omtrent naleving van de AVG. In het beleid is de optie opgenomen om binnen het team een decentrale contactpersoon informatieveiligheid en privacy aan te wijzen.

Naast het beleggen van verschillende verantwoordelijkheden bij de bovengenoemde bestuurders, managers en lijnmedewerkers, is er ook een aantal specifieke privacyfunctionarissen beschreven.

- De FG heeft een rol op de achtergrond: hij adviseert en informeert omtrent gegevensverwerking, ziet toe op naleving van de AVG, andere privacywetgeving en van lokaal privacybeleid, op het toewijzen van verantwoordelijkheden conform het privacybeleid en op de opleiding van medewerkers; hij adviseert over onder meer over privacyvraagstukken, de afhandeling van incidenten en het uitvoeren van DPIA's, en bij het opstellen van privacygerelateerd beleid. Ook treedt hij op als contactpersoon met de AP.
- De CISO is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages. Hij speelt daarvoor onder meer een rol bij het opstellen van verwerkersovereenkomsten, het beoordelen van datalekken en het uitvoeren van DPIA's. Hij zorgt tevens voor de informatieveiligheidsanalyse en voor de prioritering van informatieveiligheidsmaatregelen die hierbij naar voren komen. Hij fungeert daarnaast als informatiebron met betrekking tot informatieveiligheid voor zowel management als medewerkers in de organisatie. Ook hij heeft een rol bij het creëren van bewustzijn op het gebied van

informatieveiligheid. Hij registreert incidenten en rapporteert over informatieveiligheid in managementrapportages.
— De rol van privacy officer is gericht op de uitvoering en de naleving van de privacywetgeving, waarbij hij adviseert over privacybescherming, vaak vanuit een juridische invalshoek. Hij moet onder meer privacywet- en regelgeving uitleggen binnen de organisatie, standaard (model)documenten zoals verwerkersovereenkomsten, convenanten en reglementen opstellen en adviseren bij het inzetten daarvan, en ondersteunen bij de uitvoering van DPIA's. Net als de FG ziet hij toe op de toewijzing van verantwoordelijkheden met betrekking tot privacybeleid.

Binnen de gemeente is een kerngroep AVG in het leven geroepen, die belast is met de monitoring van de kwaliteit van de privacybescherming binnen de gemeentelijke organisatie. In dit team zitten: de FG, de CISO, de privacy officer, een beleidsmedewerker informatievoorziening en een juridisch medewerker sociaal domein. Daarnaast kunnen bij bepaalde onderwerpen nog andere medewerkers aanschuiven. De kerngroep is een overleg- en afstemmingsorgaan dat onder meer overlegt over privacybeleid en privacybewustzijn, maar ook op andere manieren betrokken kan zijn bij activiteiten die organisatiebreed of op bepaalde afdelingen worden ondernomen met betrekking tot privacy, zoals het doorlopen van DPIA's.

In het governancedocument is verder vastgelegd hoe verantwoordelijkheden met betrekking tot privacy zijn belegd. Zo is voor verschillende taken steeds aangegeven wie verantwoordelijk is voor de deeltaken die daaronder vallen. Hierbij worden de volgende taken onderscheiden:

— het beheer van het verwerkingsregister;
— registratie, beheer en actualisatie van verwerkersovereenkomsten of gegevensuitwisselingsovereenkomsten;
— de afhandeling van veiligheidsincidenten;
— advies en voorlichting aan medewerkers;
— het uitvoeren van DPIA's;
— de afhandeling van klachten en verzoeken op basis van rechten van betrokkenen;
— het ontwikkelen en beheren van formats, procedures en beleid.

In het governancedocument valt op dat het nogal eens voorkomt dat (deel)taken bij verschillende partijen belegd zijn, zonder dat verder gespecificeerd wordt welke functionaris in welke situatie verantwoordelijk is. Voor een aantal (deel)taken geldt dat in de praktijk nog moet zijn uitgewerkt hoe de verdeling van verantwoordelijkheden is belegd.

In het beleid is qua taakverdeling gekozen voor een privacy-organisatie waarbij de *three lines of defence* in positie zijn gebracht. Uit interviews is gebleken dat de flexibiliteit die de documentatie biedt in de privacy-organisatie in de praktijk ook kan leiden tot vervaging van rollen. Zo heeft de FG ook wel meegeschreven aan beleidsstukken op het gebied van privacy, waarmee de verantwoordelijkheid van 'adviseren en ondersteunen' bij het opstellen van privacybeleid wel is opgerekt. Ook in bredere zin is aangegeven dat de FG en de CPO veel samenwerken en daarbij soms pragmatisch taken verdelen. De kerngroep AVG is door natuurlijk verloop na verloop van tijd leeggelopen. Leden werden niet automatisch vervangen door hun opvolger in de organisatie; het lidmaatschap was niet gekoppeld aan de functie, maar ook aan affiniteit met het onderwerp. Bovendien verminderde het aantal vraagstukken dat door de kerngroep besproken kon worden enige tijd na de inwerkingtreding van de AVG zodanig dat de

vergaderfrequentie werd verminderd (van wekelijks in het begin tot zeer onregelmatig aan het eind). Momenteel is er alleen nog sprake van overleg tussen de FG en de CPO, en eventueel ad hoc overleg met andere mensen in de organisatie.

De rol van CISO is in de afgelopen jaren ingevuld door verschillende (interim) medewerkers. Na het omvangrijke beveiligingsincident is er sprake geweest van een crisissituatie, waardoor het vooral prioriteit was om de functie van CISO steeds direct bezet te krijgen en niet de tijd genomen kon worden om iemand te vinden die ook voor lange termijn deze functie kon vervullen. Daarbij merkt de gemeente dat er op dit vlak al enige tijd krapte op de arbeidsmarkt is. Voor de CISO is, mede naar aanleiding van het beveiligingsincident, gekozen om mensen met een technisch georiënteerd profiel aan te stellen. Daarmee kent het werkterrein van de CISO slechts in beperkte mate overlap of raakvlakken met dat van de FG en de privacy officer.

Inbedding privacy in de organisatie

Voor de onafhankelijke plaatsing van de FG en de CISO is ervoor gekozen dat deze onder de concernstaf vallen. De FG heeft (samen met de privacy officer) de mogelijkheid om het managementteam (MT) te adviseren, bijvoorbeeld door memo's op te stellen waarin privacymaatregelen worden voorgesteld. Het is vervolgens aan het MT om te besluiten die adviezen ook op te volgen. De FG is niet betrokken bij de overwegingen daarbij, en krijgt na afloop van het beraad van het MT een reactie waar geen verder overleg op volgt. Het is geen uitzondering dat een advies van de FG niet volledig of niet direct wordt opgevolgd. Dat heeft er wel eens toe geleid dat er een hernieuwd advies vanuit de FG aan het MT is gericht. Ook bestaan er bij de FG zorgen over diens integrale betrokkenheid bij privacykwesties. Idealiter zou hij als FG vooraan in processen betrokken moeten worden wanneer gegevensbescherming van belang is, maar dat is nog niet structureel het geval. De rol van adviseur en sparringpartner komt daardoor niet altijd goed uit de verf.

De inbedding is verder geregeld doordat in de beleidsdocumenten expliciet de primaire verantwoordelijkheid voor de dagelijkse gang van zaken omtrent gegevensverwerking is neergelegd bij de teamcoördinator en de bij het proces betrokken medewerkers. Daarmee is de lijnorganisatie eerst aangewezen om ervoor te zorgen dat de AVG bij de eigen processen wordt nageleefd.

Praktijk

Opleiding en training

Zowel de FG als de privacy officer hebben vanuit het privacybeleid als verantwoordelijkheid om toezicht te houden op onder meer de opleiding en training van de medewerkers. De uitvoering van de trainingen is de verantwoordelijkheid van teamcoördinatoren en afdelingsmanagers, maar ook (weer) van de FG, de privacy officer en de CISO.

Uit de interviews blijkt dat met name vlak na de inwerkingtreding van de AVG in de hele gemeente veel aandacht is besteed aan de AVG. Dit is in de jaren daarna iets afgenomen. Er is een training ontwikkeld, die nieuwe medewerkers verplicht moeten volgen. Hierin komen onder meer onderwerpen zoals verwerkersovereenkomsten, bijzondere persoonsgegevens en verantwoordingsmechanismen voor gegevensverzameling aan bod. Ook in herhaalcursussen wordt aandacht geschonken aan de AVG, zodat men zich periodiek moet blijven verdiepen in de materie. Daarnaast wordt erop aangestuurd dat het een gespreksonderwerp is in het

teamoverleg, zodat men elkaar scherp kan houden en het bewustzijn in stand blijft. Op het intranet staat informatie die men kan raadplegen, maar dit wordt niet meer actief onder de aandacht gebracht en het is dus de vraag in hoeverre dit effectief bijdraagt aan het privacybewustzijn.

Over de inhoud van opleidingen beslist het management, waarbij de FG, privacy officer en de CISO adviseren over de vereisten, dilemma's en verantwoordelijkheden. Voor het opzetten van trainingen wordt gebruik gemaakt van externe trainingsinstituten, aangevuld met interne expertise. Er wordt bewust gebruik gemaakt van het aanbod dat professionele partijen hebben ontwikkeld, omdat de gemeente zich ervan bewust is dat ze te klein is om alle expertise zelf in huis te hebben.

Direct na het beveiligingsincident is het bewustzijn in de organisatie met name ten aanzien van de technische aspecten van gegevensbeveiliging aanzienlijk toegenomen. Medewerkers werden zich veel bewuster van wat hun verantwoordelijkheden waren en wat de risico's waren van onvoorzichtige gedragingen. Toch is dit niveau van bewustzijn na verloop tijd ook iets gedaald. Daarnaast is geconstateerd dat de naleving van de AVG in brede zin door een groot deel van de organisatie los wordt gezien van de noodzaak van beveiliging van gegevens en systemen. Dat kan ook als verklaring worden gezien voor het feit dat ook na het incident de FG nog niet altijd optimaal wordt ingezet als adviseur bij AVG-gerelateerde vraagstukken. Bij een nieuw op te zetten integraal frontoffice voor het sociaal domein is hij vooraf in het proces betrokken, maar de mate waarin de FG wordt betrokken kan verschillen per afdeling.

Processen

DPIA's

Zoals eerder gezegd wordt in het privacybeleid verwezen naar de BIO als beleidskader voor informatiebeveiliging. Hierbij wordt ook expliciet vastgesteld dat "het tijdig, juist en volledig uitvoeren van DPIA's, het opvolgen van de maatregelen die voortvloeien uit deze DPIA's (comply) of het uitleggen waarom dit niet het geval is (explain) een integraal onderdeel vormen van de BIO". In het governancedocument is uitgewerkt hoe de verantwoordelijkheden met betrekking tot het uitvoeren van DPIA's zijn verdeeld.

Zo is vastgelegd dat het afdelings- en teammanagement dient te beoordelen wanneer een DPIA noodzakelijk is en ervoor te zorgen dat deze wordt uitgevoerd. Jaarlijks vindt overleg met FG, privacy officer en CISO plaats om deze DPIA's in kaart te krijgen. De uitvoering vindt plaats onder verantwoordelijkheid van de teamcoördinator, die ondersteund kan worden door de kerngroep AVG (wat in de huidige situatie neerkomt op de FG en de privacy officer). Ook de uitvoering van maatregelen naar aanleiding van de DPIA is de verantwoordelijkheid van de teamcoördinator. Het DPIA-rapport wordt beoordeeld door de FG en (indien een IT-voorziening onderdeel is van het nieuwe proces) de CISO, en hun adviezen worden verwerkt in het rapport. De opvolging van aanbevelingen in het DPIA-rapport dient door de afdeling en/of het team te worden opgepakt.

Uit interviews blijkt dat het beleid in de praktijk niet altijd navolging vindt. De agenderende rol voor DPIA's in de hele organisatie die aan de kerngroep AVG was toebedacht, is met het inactief worden van die groep niet steeds goed ingevuld. Omdat ook de managers op afdelings- en teamniveau hun verantwoordelijkheid voor gegevensbescherming onvoldoende invullen, is er in het recente verleden onvoldoende prioriteit gegeven aan het uitvoeren van DPIA's, en aan het grondig opstellen van de rapportages hierover. Uit een gesprek met een

medewerker blijkt dat ook wordt getwijfeld aan het nut van DPIA's; als instrument om bewustzijn te creëren onder medewerkers wordt het als een te intensief proces gezien (waarmee de andere functies van de DPIA niet gewaardeerd lijken).

Datalekken
Voor de afhandeling van veiligheidsincidenten zijn verantwoordelijkheden verdeeld in het governancedocument. Hierbij is de teamcoördinator primair verantwoordelijk voor de afhandeling. Deze dient het incident intern en eventueel extern te melden en dient een overleg op te zetten. Hierbij zijn de FG, privacy officer en CISO ook betrokken in ondersteunende en adviserende rollen. Indien nodig wordt de afhandeling opgeschaald naar het niveau van MT, of naar de ambtelijk of bestuurlijk eindverantwoordelijke partijen. Er is een protocol opgenomen in het document waarin stap voor stap is vastgelegd wat moet worden gedaan, in welke volgorde en wie verantwoordelijk is. Daarbij valt op dat het beoordelingskader (dat wordt gebruikt bij het afwegen of bij een incident melding moet worden gedaan bij de AP en of betrokkenen geïnformeerd moeten worden) niet is uitgewerkt en dus nog deels open kan staan voor interpretatie door de verantwoordelijke medewerker.

Bij de bestudeerde gemeente heeft zich een tweetal voorname beveiligingsincidenten voorgedaan. Bij het eerste was potentieel sprake van het grootschalig lekken van persoonsgegevens, naast het feit dat er een groot aantal systemen onbruikbaar is geweest. Bij het tweede ging het om een relatief kleinschalig lek van persoonsgegevens. Beide incidenten hebben de (lokale) pers gehaald en veroorzaakten dus een groot risico, niet alleen voor de betrokkenen van wie gegevens gelekt waren, maar ook voor de bedrijfsvoering en de reputatie van de gemeente. Naar aanleiding hiervan is een reactie gekomen waarbij de focus is gelegd op beveiligingsaspecten van gegevensbescherming, zowel technisch als met betrekking tot bewustzijn en verantwoordelijk gedrag van medewerkers. Ten aanzien van het nadenken over gegevensverwerving en -verwerking zijn minder grote stappen gemaakt en is, door de grote aandacht voor het beveiligingsaspecten, mogelijk zelfs sprake geweest van het teruglopen van de aandacht voor gegevensbescherming.

Verwerkersovereenkomsten
Ook voor het opstellen en afsluiten van overeenkomsten zijn de verantwoordelijkheden in het beleid nauwkeurig toebedeeld. De hoofdverantwoordelijkheid ligt bij het afdelingsmanagement, het opstellen is een taak van de teamcoördinator. De privacy officer stelt standaardovereenkomsten op en adviseert bij het gebruik hiervan. De CISO adviseert ten aanzien van veiligheidsaspecten indien nodig. De FG heeft hierbij een toezichthoudende rol met betrekking tot naleving van privacywetgeving en registratie van de verwerkersovereenkomsten.

In de praktijk blijkt er onduidelijkheid te zijn (geweest) over de noodzaak van verwerkersovereenkomsten in specifieke gevallen waarbij IT-systemen in gebruik zijn, en over wie de verantwoordelijkheid draagt voor het opstellen hiervan. Dit heeft ertoe geleid dat er mogelijk overeenkomsten nog niet zijn opgesteld zijn waar dat wel nodig is. Een nieuw proces, waarbij voor elke nieuwe IT-applicatie ook een medewerker verantwoordelijk wordt gesteld die moet onderzoeken of een verwerkersovereenkomst nodig is, moet hierin verbetering aanbrengen.

Samenwerking met derden

In het privacybeleid wordt ook aandacht geschonken aan informatie-uitwisseling met derden. Dit is mogelijk wanneer dat noodzakelijk is voor de uitvoering van de gemeentelijke taken of

wanneer er een wettelijke verplichting is en gebeurt altijd na een afweging van belangen van de gemeente en de ontvanger en van de betrokkenen. Er wordt belang gehecht aan het feit dat belangenafwegingen worden gemaakt door medewerkers waarbij elke situatie nauwkeurig beoordeeld wordt.

De gemeente neemt deel in veel samenwerkingsverbanden. Voor de grootste verbanden geldt dat er doorgaans sprake is van een Gemeenschappelijke Regeling (GR), waarbij een eigen FG is aangewezen. Deze organisaties hebben ook een eigen dagelijks en algemeen bestuur. Voor de overige samenwerkingsverbanden geldt dat vraagstukken over gegevensdeling niet als complex worden gezien of voor veel vragen zorgen.

Controle en toezicht

In het beleid is het interne toezicht conform de AVG vastgelegd in de functie van de FG. Hij ziet toe op in elk geval:

- naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- naleving van het gemeentelijke beleid met betrekking tot de bescherming van persoonsgegevens;
- toewijzing van verantwoordelijkheden, op de bewustmaking en op de opleiding/training van de medewerkers;
- uitvoeren van DPIA's.

Dat wordt verder uitgewerkt in zijn rol bij diverse taken. Zo heeft hij een rol bij de toetsing van de integriteit en volledigheid van het verwerkingsregister, ziet hij toe op het afsluiten van verwerkersovereenkomsten, controleert hij of adviezen uit rapportages naar aanleiding van veiligheidsincidenten geïmplementeerd worden, houdt hij toezicht op de kwaliteit van het doorlopen van procedures bij verzoeken in het kader van rechten van betrokkenen en houdt hij toezicht op de kwaliteit, archivering, communicatie en toepassing van procedures, formats en beleid.

Naar eigen oordeel krijgt de FG binnen de organisatie in de praktijk voldoende ruimte om deze toezichtrol in te vullen. Toch is er ook geconstateerd dat er soms doorzettingsmacht ontbreekt, bijvoorbeeld waar het gaat om verwerkersovereenkomsten. Daar zien we dat het feit dat de FG via het MT moet proberen te sturen op de organisatie, er soms voor zorgt dat maatregelen die hij nodig acht worden uitgesteld en dat adviezen mogelijk geen (volledige) opvolging krijgen.

Voor deze grootschalige lekken is gebleken dat het contact met de AP niet naar tevredenheid is verlopen. Het meldingsproces bleek niet goed ingericht op de grootschaligheid van het (mogelijke) lek en de initiële reactie wordt als 'beperkt' omschreven. Wel volgt de AP de gemeente nu voor een langere periode om te controleren dat de gemeente goede maatregelen heeft genomen en dat de systemen zodanig ingericht zijn dat een dergelijk incident zich niet meer kan voordoen. Daarover is nu halfjaarlijks contact.

Voor kleinschalige lekken (bijvoorbeeld verkeerd geadresseerde brieven) blijken de intern opgezette processen relatief eenvoudig gevolgd te kunnen worden. Wel is er ontevredenheid

over de manier waarop de AP deze meldingen verwerkt. De feedback over meldingen is onvoldoende, terwijl er wel veel tijd is gemoeid met deze meldingen. Hierdoor komt de motivatie om altijd meldingen te doen, zeker bij kleine incidenten, in het gedrang.

Uitdagingen

Tijdens de casestudy is een aantal uitdagingen boven tafel gekomen. Ten eerste is geconstateerd dat het AVG-bewustzijn nog niet optimaal is, niet alleen qua persoonlijke beveiliging en techniek, maar vooral qua belangenafweging bij keuzes omtrent gegevensverwerking.

De privacy-organisatie is op een aantal punten nog niet optimaal ingericht of ingebed. Zo wordt de FG nog te weinig als adviseur en sparring partner ingezet, maar meer als toezichthouder achteraf. Er liggen dus kansen om meer uit de expertise van de FG te halen bij het inrichten van processen. Er is een kerngroep AVG ingesteld, maar inmiddels is deze om praktische redenen niet meer actief, terwijl er wel officieel verantwoordelijkheden zijn belegd. Hierdoor vallen extra taken op de schouders van de FG en de privacy officer, wat een smalle basis is. Deze twee werken veel op pragmatische basis samen, waardoor rollen mogelijk wat door elkaar kunnen lopen. Een laatste punt in deze categorie betreft de afhankelijkheid van de FG van het MT. De adviezen worden door het MT niet altijd overgenomen, maar er worden meer subjectieve afwegingen gemaakt waardoor privacy-aspecten minder hoge prioriteit kunnen krijgen onder druk van werkprocessen of de roep om doelmatigheid.

Ten slotte is aangegeven dat het beheer van verwerkersovereenkomsten strakker geregeld kan worden, en dat de concrete planning van de uitvoering van DPIA's beter geborgd zou kunnen worden.

Analyse

Dimensies van spontane naleving

Kennis van regels
Het beveiligingsincident heeft een behoorlijke indruk gemaakt op de organisatie. Door middel van cursussen wordt bij aanvang van het dienstverband en daarna periodiek getracht het bewustzijn over privacy-aspecten en de kennis van het belang van naleving van de AVG bevorderd. Daarnaast wordt er door het management op gestuurd dat bij teamoverleggen regelmatig privacy-onderwerpen worden besproken. Daarmee is het bewustzijn groot ten aanzien van de technische beveiliging van toegang tot gegevens en het bestrijden van risico's op lekken. Doordat de gemeente een relatief kleine organisatie is, kunnen signalen van de werkvloer het management makkelijk bereiken. Privacyfunctionarissen hebben toegang tot het MT. De gemeente is zich ervan bewust dat ze door de geringe omvang er goed aan doet om expertise van buiten te betrekken en doet dat ook geregeld.

Kosten en baten
De gemeente staat, net als veel gemeenten, onder grote druk om met beperkte middelen een groot takenpakket uit te voeren. Daarmee bestaat een prikkel om doelmatig te werken en te focussen op het doelmatig opzetten en uitvoeren van werkprocessen. Het grondig uitvoeren van DPIA's, opzetten van verwerkersovereenkomsten en bijhouden van registers draagt niet direct bij aan de 'productie' van de gemeente, en er ontstaat daardoor een prikkel om AVG-

aspecten in elk geval geen voorrang te geven. Afhankelijk van de afdeling is er soms voor gekozen om AVG-gerelateerde zaken even uit te stellen, met het oog op correcte en tijdige invoering van nieuwe processen of systemen. Ook adviezen vanuit de FG aan het MT worden niet altijd direct opgevolgd.

Mate van acceptatie
Het bovenstaande wil niet zeggen dat men niet doordrongen is van het belang van naleving van de AVG. Die wordt zonder meer onderschreven. Door tijdsdruk kan de prioritering van werkzaamheden echter wel richting primaire processen verschuiven. Privacy-aspecten worden daardoor niet altijd als integraal onderdeel van het opzetten van processen gezien.

Maatschappelijke controle
De gemeente weet, zeker ook naar aanleiding van twee beveiligingsincidenten, dat als er zich datalekken van voldoende omvang voordoen daaraan veel aandacht in de lokale samenleving, lokale pers maar ook landelijke pers wordt geschonken. Daardoor is er zeker sprake van een ervaren maatschappelijke controle. Men is er goed van doordrongen dat een soortgelijk incident niet nogmaals mag gebeuren. Dit werkt ook door in het bewustzijn in de gehele organisatie. Toch is dit effect na verloop van tijd wel iets afgenomen.

Handhavingsdimensies
De gemeente staat momenteel naar aanleiding van het beveiligingsincident onder verscherpt toezicht van de AP. Dit houdt in dat er gedurende halfjaarlijks rechtstreeks contact is om de AP te informeren over de stappen die gezet worden om de informatiebeveiliging volledig te laten voldoen aan de eisen zoals vastgelegd in de BIO en in de AVG. Dit proces verloopt naar tevredenheid van de gemeente.

Andere relevante punten
Het beveiligingsincident heeft in eerste instantie grote impact gehad op de organisatie, zowel in de primaire werkprocessen als in het privacybewustzijn. Wat opvalt is dat er in het onderwerp wel een sterk onderscheid wordt gevoeld tussen de ‘technische’ dimensie, waarbij het vooral gaat om beveiliging van de ICT-infrastructuur en om zorgvuldige omgang met inloggegevens en apparatuur, en anderzijds de dimensie van zorgvuldige gegevensverzameling en -verwerking. Die tweede dimensie betreft meer het nadenken over de noodzaak van verwerking van gegevens, registratie van verwerkingen, opstellen van overeenkomsten en beleggen van verantwoordelijkheden, en juist daarin bestaat spanning tussen voldoende aandacht voor naleving van AVG en doelmatige opzetten en uitvoeren van primaire processen.


pro facto