213a-onderzoek naar de implementatie van de AVG

Gemeente Zoetermeer

Necker
van Naem

Colofon:

Datum:

13 oktober 2022

Opdrachtgever:

Björn Wijman, concerncontroller

Gemeente Zoetermeer

Onderzoekers:

Mr. C.A. (Carin) Schreuder
carin@necker.nl

Mr. E.J. (Evert Jan) Kruijswijk Jansen
evertjan@necker.nl

L.M. (Robert) Klaassen MSc
robert@necker.nl

C. (Christan) Schut MA LLM
christan@necker.nl

Bestuurlijke samenvatting

In 2016 is de gemeente Zoetermeer gestart met de implementatie van de Algemene Verordening Gegevensbescherming (AVG). Sindsdien heeft de gemeente veel stappen gezet om te voldoen aan de eisen van het gegevens(beschermings-)recht. Er zijn verschillende beleidsdocumenten vastgesteld en de nodige functionarissen hebben een positie gekregen binnen de gemeente. Met medewerkers is daarnaast door middel van scholing gewerkt aan de kennis en kunde die nodig is om te werken met de AVG, zoals bij het afhandelen van incidenten of het delen van informatie met derden. Het gemeentelijk beleidskader biedt voldoende waarborgen voor een zorgvuldige gegevensbescherming. In de uitvoering in de praktijk is er echter nog veel ruimte voor verbetering.

De gemeente kan veel meer doen om het toezicht op, evaluatie van en rapportage over de wijze waarop de gemeente invulling geeft aan de AVG-richtlijnen te versterken. Zo is er momenteel onvoldoende capaciteit om het onafhankelijke toezicht door de Functionaris Gegevensbescherming goed in te kunnen richten. Werkdruk, capaciteitsproblemen en verloop in de organisatie staan daarnaast in de weg van structurele kennisopbouw bij medewerkers en monitoring binnen de teams. Ondanks de gegeven trainingen en workshops zien veel medewerkers het werken met de AVG als lastig, en worden de bijbehorende extra processtappen door hen als belemmering ervaren. Doordat er door de aangewezen functionarissen veel tijd en inzet wordt gestoken in het ondersteunen bij acute vraagstukken, is er ten slotte beperkte ruimte voor prioritering en anticipatie op toekomstige ontwikkelingen.

Op basis van de conclusies van het onderzoek zijn er verbeterpunten geformuleerd door de onderzoekers. De belangrijkste verbeterpunten zijn:

- Stel een gezamenlijke visie op voor de omgang met privacy en de inrichting van de privacy-organisatie.
- Actualiseer het beleidskader en vervolledig de waarborgen voor een zorgvuldige gegevensverwerking.
- Zorg voor een versterking van de posities van de Functionaris Gegevensbescherming en Privacy Officer. Zorg voor een waarborging van de onafhankelijkheid van de Functionaris Gegevensbescherming.
- Ga aan de slag met het cyclisch monitoren en rapporteren over compliance en toezicht.
- Blijf regelmatige (verplichte) workshops en trainingen organiseren.
- Anticipeer op wettelijke ontwikkelingen en zet waar mogelijk alvast acties op.

Inhoudsopgave

Onderzoeksverantwoording

Inleiding en aanleiding

De Algemene verordening gegevensbescherming (hierna: AVG) is een Europese verordening met regels voor de verwerking van persoonsgegevens. De AVG is op 24 mei 2016 in werking getreden en sinds 25 mei 2018 zijn alle organisaties in Nederland aanspreekbaar op de naleving van de AVG.

Het voldoen aan de richtlijnen en regels uit de AVG bleek voor veel organisaties een forse uitdaging. Gemeenten vormden hier geen uitzondering op. Het zorgen voor een juiste vertaling van de AVG naar de organisatie, met de bijbehorende praktische uitwerking, is voor veel gemeenten geen vanzelfsprekendheid. Uit eerder door Necker van Naem uitgevoerde onderzoeken in diverse gemeenten, weten we bijvoorbeeld dat:

- het bewustzijn met betrekking tot privacy en informatiebeveiliging geen gemeengoed is onder medewerkers van gemeenten;
- medewerkers in de uitvoering vaak eigenstandig een afweging maken rondom het delen van gegevens;
- betrokkenen vaak slecht op de hoogte worden gesteld van de gemeentelijke omgang met persoonsgegevens.

Gezien ook in de gemeente Zoetermeer de implementatie van de AVG nog niet geheel afgerond is – de vraag is of organisaties dat punt ooit bereiken, er is altijd sprake van doorontwikkeling –, heeft het gemeentebestuur gevraagd of Necker van Naem de implementatie van de AVG in de gemeente wil onderzoeken.

Doelstelling en focus

Voor het onderzoek naar de implementatie van de AVG in de gemeente Zoetermeer is de volgende doelstelling geformuleerd*:*

Inzicht geven in de mate waarin de AVG succesvol is geïmplementeerd richting medewerkers, zodanig dat de gegevensbescherming van burgers correct plaatsvindt.

De focus in het onderzoek zal daarbij zowel liggen op de technische/procesmatige kant als de organisatorische kant van de implementatie van de AVG. De geformuleerde aanbevelingen op basis van dit onderzoek kunnen daardoor op beide aspecten betrekking hebben.

In overleg met de opdrachtgever is gekozen om het onderzoek in het bijzonder te richten op drie domeinen binnen de gemeente: het sociaal domein, het publieksplein en het veiligheidsdomein.

Vraagstelling

Dit onderzoek is uitgevoerd aan de hand van hoofd- en deelvragen, welke zijn geformuleerd door de opdrachtgever. Door de onderzoekers zijn deze deelvragen onderverdeeld in drie categorieën: waarborgen, organisatie en lessen voor de toekomst.

Hoofdvraag

In hoeverre is de AVG succesvol geïmplementeerd binnen de gemeente Zoetermeer, zodat burgers volledige gegevensbescherming genieten en de medewerkers van de gemeente kunnen voldoen aan de eisen van de AVG?

Deelvragen

Waarborgen:

1. Zijn binnen de organisatie voldoende waarborgen aanwezig die voorzien in een betrouwbare bescherming van persoonsgegevens van betrokkenen, conform de AVG?

2. Is bij incidenten (datalekken) sprake van zorgvuldige afhandeling conform de AVG?

Organisatie:

3. Worden de medewerkers bij de uitvoering van hun taken voldoende gefaciliteerd in het efficiënt en effectief werken conform de AVG?

4. Hoe wordt ervoor gezorgd dat binnen de organisatie structureel voldoende kennis en kunde aanwezig is op het gebied van gegevensbescherming?

5. Hoe wordt ervoor gezorgd dat, als vervolg op de Leertuinen privacy voor het Sociaal Domein, medewerkers gegevensbescherming als onderdeel van hun werkzaamheden zien en niet als belemmering?

Lessen voor de toekomst:

6. Welke verbeterpunten zijn er ten aanzien van bovenstaande vragen?

7. Is de huidige organisatie voldoende toegerust om de toekomstige ontwikkelingen (zoals aankomende wet- en regelgeving, nieuwe technologieën etc.) aan te kunnen en zijn er eventuele verbeterpunten? Wat is daar eventueel nog voor benodigd (qua organisatie, middelen e.d.)?

Werkzaamheden en periode

De onderzoekswerkzaamheden zijn aangevangen met een startgesprek met de stuurgroep op 5 april 2022. Hierna startte de documentanalyse, die is afgerond in mei 2022. In de periode mei - augustus 2022 zijn de interviews gevoerd met de Functionaris gegevensbescherming (FG), Privacy Officer (PO) en Chief

Informatie Security Officer (CISO) en verschillende andere betrokkenen uit de organisatie. Een volledig overzicht van geïnterviewde personen is te vinden in de bijlage. In juni 2022 hebben drie groepsgesprekken plaatsgevonden met medewerkers van respectievelijk het sociaal domein, het veiligheidsdomein en het publieksplein. Daarnaast is een enquête uitgevoerd onder medewerkers van de gemeente. Een uitgebreide toelichting op deze enquête is opgenomen in hoofdstuk 3 van deze rapportage. In september 2022 heeft ten slotte een duidingsbijeenkomst plaatsgevonden met leden van de stuurgroep en medewerkers die eerder deelnamen aan de groepsgesprekken. De conceptrapportage is op 19 september 2022 voorgelegd aan de organisatie voor een feitelijke check en op 26 september 2022 in de stuurgroep besproken, waarna de rapportage voor ambtelijk wederhoor gereed gemaakt is. Op 27 september is de rapportage daartoe verstuurd. Daarna is de eindrapportage opgesteld.

Leeswijzer

Deze rapportage bestaat uit een vijftal hoofdstukken. Het eerste hoofdstuk richt zich op het uiteenzetten van het kader van de AVG en zet de belangrijkste richtlijnen en begrippen van het gegevensbeschermingsrecht uiteen die relevant zijn voor de gemeente Zoetermeer. Het tweede hoofdstuk gaat in op het beleid van Zoetermeer om invulling te geven aan de verplichtingen uit de AVG. In het derde hoofdstuk zoomt de rapportage in op de gemeentelijke organisatie, waarbij er gekeken wordt naar de drie genoemde domeinen: het sociaal domein, het publieksplein en het veiligheidsdomein. De focus ligt daarbij op de organisatie van gegevensbescherming en informatiebeveiliging. Daarbij wordt onder meer ingegaan op de verdeling van rollen en verantwoordelijkheden. In het vierde hoofdstuk wordt ingegaan op relevante toekomstige ontwikkelingen in wet- en regelgeving en bijbehorende risico's die relevant zijn voor de gemeente. Tot slot richt het vijfde hoofdstuk zich op de beantwoording van de onderzoeksvragen en het formuleren van lessen voor de toekomst. In dit laatste hoofdstuk zijn ook de aanbevelingen opgenomen.

1. De AVG als kader voor gegevensbescherming

1.1. Inleiding

Het belangrijkste wettelijke kader voor gegevensbescherming is de AVG. De AVG kent verschillende richtlijnen voor de inrichting van gegevensbescherming door organisaties die persoonsgegevens verwerken, waar gemeenten ook onder vallen. In dit hoofdstuk wordt ingegaan op de belangrijkste begrippen en richtlijnen die de AVG met zich meebrengt.

1.2. De AVG op hoofdlijnen

1.2.1. Een korte toelichting op de AVG

Op 25 mei 2018 werd de Algemene AVG van toepassing. Na een termijn van twee jaar waarin de AVG al in werking was getreden werden organisaties die persoonsgegevens verwerkten aanspreekbaar op de naleving van de AVG.[1]

In Nederland zijn de regels naast de AVG ook vastgelegd in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De AVG kent als Europese richtlijn een rechtstreekse werking in Nederland, welke is aangevuld met de UAVG door nationale werkgevers. De AVG en de UAVG vormen daarmee een vervanging van de richtlijn 95/46/EG en de Wet bescherming persoonsgegevens (Wbp).

Ook overheden moesten per 25 mei 2018 voldoen aan de eisen van de AVG. Binnen de overheid staan gemeenten het meest direct in contact met de burger, waardoor deze opgave veel impact heeft. Gemeentelijke organisaties hebben de afgelopen zes jaar gewerkt aan het implementeren van de AVG in de organisatie. De meeste gemeenten hebben daar flinke stappen in gezet de laatste jaren, desondanks is er nog een wereld te winnen voor veel gemeenten, getuige een recent onderzoek van *Bits of Freedom*.[2]

1.2.2. Begrippenkader van de AVG

De AVG is van toepassing op iedere verwerking van persoonsgegevens

[1] De verordening trad in mei 2016 in werking, maar organisaties kregen tot 25 mei 2018 de tijd om hun organisatie en/of bedrijfsvoering met de AVG in overeenstemming te brengen.
[2] Bits of Freedom (2022), De staat van privacy bij gemeenten, geraadpleegd via: Bits-of-Freedom-De-staat-van-privacy-bij-gemeenten.pdf (bitsoffreedom.nl).

Het gegevensbeschermingsrecht van de AVG kent een eigen systematiek en begrippenkader. Om helderheid te geven over dit kader zetten we hier de belangrijkste begrippen uiteen.

Belangrijk is allereerst om naar het toepassingsbereik van de AVG te kijken. De AVG is van toepassing op "*geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen*".[3] Dat maakt dat alle vormen van geautomatiseerde verwerking van persoonsgegevens onder de AVG vallen en dat alle verwerkingen van in een bestand opgenomen of voor bestanden bestemde persoonsgegevens onder de AVG vallen.[4]

Hoewel het toepassingsbereik van de AVG breed is, vallen niet alle gegevens onder de AVG. De AVG heeft betrekking op persoonsgegevens en definieert dit als alle informatie over natuurlijke personen. Dat wil zeggen: alle informatie die over iemand gaat of naar een persoon te herleiden is.[5] Gegevens als een identificatienummer of locatiegegevens vallen bijvoorbeeld onder deze noemer.

Er moet een grondslag zijn voor verwerking van persoonsgegevens

De AVG geeft zes grondslagen voor de verwerking van persoonsgegevens. Voorbeelden van grondslagen zijn toestemming of een wettelijke verplichting.

De AVG heeft een aantal persoonsgegevens apart gezet onder de categorie bijzondere persoonsgegevens. Bijzondere persoonsgegevens krijgen extra bescherming doordat hun verwerking in beginsel verboden is.[6] De verwerking van bijzondere persoonsgegevens is alleen mogelijk als er een grondslag voor verwerking is én een van de uitzonderingsgronden uit art. 9 lid 2 AVG van toepassing is. Verschillende van deze uitzonderingsgronden zijn verder uitgewerkt in hoofdstuk 3 van de UAVG. Daarbij kan bijvoorbeeld gedacht worden aan de uitzonderingsgronden voor verwerking van genetische persoonsgegevens zoals onder meer een zwaarwegend geneeskundig belang.[7]

Een andere belangrijke bepaling om te zien of de AVG van toepassing is, is de vraag of er sprake is van verwerking. Artikel 4 lid 2 AVG beschrijft het begrip verwerking als volgt: "*elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens*".[8] In de praktijk zijn de meest voorkomende manieren van verwerking het opslaan, verzamelen, raadplegen en versturen van persoonsgegevens. Het begrip verwerken moet echter ruim gelezen worden. Ook het structureren of ordenen vallen bijvoorbeeld onder verwerking.

De verwerking van persoonsgegevens moet volgens zes beginselen plaatsvinden

Op het moment van verwerking van persoonsgegevens is er altijd een verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke is degene die "*het doel van en de middelen voor de verwerking van*

[3] Artikel 2 Algemene Verordening Gegevensbescherming.
[4] Voor de reikwijdte van geautomatiseerde verwerking zie: HvJ EU 6 november 2003, C-101/01, NJ 2004/248 (Lindqvist), r.o. 26-28.
[5] Artikel 4 lid 1 Algemene Verordening Gegevensbescherming.
[6] Artikel 9 Algemene Verordening Gegevensbescherming.
[7] Artikel 28 lid 2 sub a Uitvoeringswet Algemene Verordening Gegevensbescherming.
[8] Artikel 4 lid 2 Algemene Verordening Gegevensbescherming.

persoonsgegevens vaststelt".[9] Naast een verwerkingsverantwoordelijke is er in sommige gevallen ook sprake van een verwerker. De verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Voor verwerking dienen beide partijen een verwerkersovereenkomst te sluiten.[10]

Naast dat er voor de verwerking van persoonsgegevens altijd een grondslag nodig is, moeten bij de verwerking van persoonsgegevens ook altijd de zes beginselen uit artikel 5 van de AVG nageleefd worden. De verwerking van persoonsgegeven moet daardoor rechtmatig, behoorlijk en transparant gebeuren door binnen de wettelijke kaders te blijven en te vermelden welk type gegevens worden verwerkt. Daarnaast is het beginsel van doelbinding van belang. Dit beginsel maakt dat de verwerkingsverantwoordelijke gegevens niet verder mag verwerken dan het aangegeven doel. Verder mogen organisaties niet meer data verzamelen dan noodzakelijk, is de juistheid van gegevens belangrijk en moet er verwijdering van gegevens plaatsvinden als de gegevens niet langer relevant zijn voor het doel. De verwerkingsverantwoordelijke moet ook de vertrouwelijkheid en integriteit van de documenten garanderen voor een gepaste beveiliging.

De AVG verplicht tot het melden van datalekken

Tot slot verplicht de AVG ook het melden van datalekken in de organisatie. Volgens Artikel 33 dient er in geval van "*een inbreuk in verband met persoonsgegevens*" binnen 72 uur na ontdekking van deze inbreuk, melding gemaakt te worden bij de Autoriteit Persoonsgegevens (AP), tenzij het onwaarschijnlijk is dat het datalek grote risico's met zich brengt voor de betrokkenen.[11] Met 'betrokkenen' bedoelt de AVG personen van wie de persoonsgegevens worden verwerkt.[12]

1.3. Relevante richtlijnen voor gemeenten

1.3.1. Richtlijnen vanuit de AVG

De AVG benoemt verschillende verplichtingen

Bij het verwerken van persoonsgegevens is (de bestuursorganen van) de gemeente in de meeste gevallen de verwerkingsverantwoordelijke.[13] Op basis van artikel 5 AVG heeft de verwerkingsverantwoordelijke een verantwoordingsplicht en moet daardoor kunnen aantonen dat de verwerking voldoet aan de eisen van de AVG. Daarnaast geeft de AVG verschillende andere verplichtingen:

- het instellen van een register van verwerkingsactiviteiten;
- het instellen van de functionaris gegevensbescherming;
- het voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren;

[9] Artikel 4 lid 7 Algemene Verordening Gegevensbescherming.
[10] Artikel 28 lid 3 Algemene Verordening Gegevensbescherming.
[11] Artikel 33 Algemene verordening gegevensbescherming.
[12] Autoriteit Persoonsgegevens (2022). Rechten van betrokkenen: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen.
[13] Dit zijn bijvoorbeeld de burgemeester, het college van B&W, de gemeenteraad en de rekenkamer.

- het raadplegen van de Autoriteit Persoonsgegevens voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit;
- de toepassing van de principes van privacy door ontwerp en standaardinstellingen (‘privacy by design & default’);
- het nemen van passende beveiligingsmaatregelen met het oog op de bescherming van persoonsgegevens;
- het onder bepaalde omstandigheden melden van een datalek bij de Autoriteit Persoonsgegevens en het informeren van betrokkenen;
- het maken van afspraken tussen verwerkingsverantwoordelijke en verwerker;
- het opstellen van privacybeleid.

De AVG verplicht tot het instellen van een functionaris gegevensbescherming

Om aan de AVG te voldoen moeten gemeenten een functionaris gegevensbescherming (hierna: FG) aanstellen. De FG moet erop toezien dat de gemeente de AVG correct toepast en naleeft. De FG treedt hierbij intern op als strategisch adviseur van de organisatie als het gaat om de verwerking van persoonsgegevens.

Volgens artikel 38 en overweging 97 van de AVG dient de FG zijn of haar taken binnen een organisatie onafhankelijk te kunnen uitvoeren.[14] De Autoriteit Persoonsgegevens licht toe dat dit betekent dat de FG ''in staat moet worden gesteld met voldoende middelen zijn taak uit te voeren, dat hij geen instructies mag krijgen met betrekking tot zijn FG-taken en dat de FG geen andere taken mag uitvoeren die mogelijk tot aantasting van zijn onafhankelijke positie leiden.''[15] De Autoriteit Persoonsgegevens geeft daarnaast aan welke uitgangspunten organisaties dienen te hanteren om de positie van de FG te borgen:

- De organisatie moet de FG in een vroeg stadium als adviseur betrekken bij de (door)ontwikkeling van producten en diensten, en samen vastleggen wat er met de adviezen van de FG gebeurt.
- De FG moet goed zichtbaar zijn binnen de organisatie. En direct, zonder tussenkomst van anderen, benaderbaar en aanspreekbaar zijn. Ook voor personen van buiten de organisatie.
- De FG is de onafhankelijke interne toezichthouder: hij grijpt in als het (mogelijk) fout gaat en hij signaleert risico’s bij (voorgenomen) verwerkingen. De FG spreekt de organisatie hierop aan en moet op het hoogste bestuurlijke niveau zijn zorgen kunnen uiten. De organisatie moet dat faciliteren.
- De organisatie moet de onafhankelijke positie van de FG waarborgen door deze op de juiste manier organisatorisch in te bedden, hem adequate toegang te geven tot het hoogste bestuurlijke niveau en door hem tijd en middelen te verstrekken om zijn taak uit te voeren.
- De FG neemt een centrale positie in bij contacten tussen de AP en de organisatie. In die positie moet de FG op de hoogte zijn van de communicatie van de AP met de organisatie. Maar: de FG heeft een onafhankelijke positie en kan dus niet namens de organisatie spreken.[16]

Het opstellen van een privacybeleid is onderdeel van de verantwoordingsplicht

[14] Artikel 38 lid 3 en overweging 97 Algemene Verordening Gegevensbescherming; Autoriteit Persoonsgegevens: richtlijnen FG.
[15] Autoriteit Persoonsgegevens (2021). Positionering van de FG, p. 1.
[16] Autoriteit Persoonsgegevens (2021). Positionering van de FG, pp. 2-5.

De AVG geeft de verwerkingsverantwoordelijke een verantwoordingsplicht om aan te tonen dat de verwerkingsverantwoordelijke voldoet aan de privacyregels.[17] Onderdeel van deze verantwoordingsplicht is het opstellen van een privacybeleid (ook wel gegevensbeschermingsbeleid genoemd). In een privacybeleid staat de visie op de wijze van gegevensverwerking beschreven, waardoor zij hierover op een transparante wijze kan communiceren richting de AP en personen wiens persoonsgegevens worden verwerkt.

Het is niet voor iedere organisatie verplicht om een privacybeleid vast te stellen. Deze verplichting moet in verhouding staan tot de verwerkingsactiviteiten van de organisatie. Hierbij moet gekeken worden naar de aard, de omvang, de context en het doel van de gegevensverwerking. In deze afweging zullen volgens de AP gemeenten vaak verplicht zijn om een privacybeleid op te stellen. Gezien de omvang van de gemeente Zoetermeer vormt het opstellen van een privacybeleid een verplichting.

De AVG stelt geen harde eisen aan de precieze inhoud van het privacybeleid. De Autoriteit Persoonsgegevens heeft wel geformuleerd wat er onder meer in het privacybeleid zou moeten staan, uitgaande van de principes van de AVG. Een privacybeleid moet volgens de Autoriteit Persoonsgegevens een beschrijving van de volgende zaken bevatten:[18]

- de categorieën te verwerken persoonsgegevens;
- de doeleinden en grondslag voor verwerking;
- de wijze waarop de voldaan is aan de beginselen uit artikel 5 AVG;
- de privacyrechten van betrokken en de wijze van uitoefening van de rechten;
- maatregelen voor de beveiliging van persoonsgegevens;
- bewaartermijn van persoonsgegevens.

1.3.2. Richtlijnen vanuit de Baseline Informatiebeveiliging Overheid

De BIO biedt een normenkader en richtlijnen voor de inrichting van informatiebeveiliging

Naast de bepalingen uit de AVG en de UAVG is de Baseline Informatiebeveiliging Overheid (BIO) van belang als het gaat om gegevensbescherming. De BIO vormt als baseline voor overheden een belangrijk kader voor informatiebeveiliging. De BIO is sinds 1 januari 2020 van kracht en zorgt voor één normenkader voor informatiebeveiliging voor gemeenten, waterschappen, provincies en het Rijk. De BIO kan gezien worden als een update van de Baseline Informatiebeveiliging Gemeenten (BIG), met in vergelijking minder maatregelen, het toewijzen van maatregelen aan eindverantwoordelijken en meer nadruk op risicomanagement.[19]

De BIO vormt voor gemeenten zowel een richtlijn als een hulpmiddel om informatiebeveiliging goed te organiseren. Binnen de BIO wordt onderscheid gemaakt tussen verschillende basisbeveiligingsniveaus (BBN's) waarbij wordt beschreven aan welke controlemaatregelen dient te worden voldaan en hoe

[17] Artikel 5 lid 2 Algemene Verordening Gegevensbescherming.
[18] Autoriteit Persoonsgegevens (2022). Verantwoordingsplicht AVG: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht?qa=privacybeleid&scrollto=1.
[19] Informatiebeveiligingsdienst (2022). Baseline Informatiebeveiliging Overheid: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/.

verantwoording dient te worden afgelegd. De BIO biedt handvatten voor de afwegingen die betrokken medewerkers hierbij maken. De verdeling van verantwoordelijkheid en de mate van verantwoording zijn afhankelijk van het basisbeveiligingsniveau (BBN). In geval van niveau BBN1 is de proceseigenaar volledig verantwoordelijk voor beslissingen en informeert de proceseigenaar de Chief Information Security Officer (CISO) alleen op verzoek over zijn BBN1-informatiesysteem.[20] In het geval van niveau BBN2 is er een grotere rol neergelegd voor de CISO doordat de proceseigenaar het informatiesysteem voor ingebruikname ter consultatie moet voorleggen aan de CISO.[21] Voor overheden, en dus ook voor de gemeente Zoetermeer, geldt BBN2 als uitgangspunt voor de beveiliging van informatiesystemen.[22] In het geval van het hoogste basisbeveiligingsniveau (BBN3) is er toestemming nodig van de secretaris of algemeen directeur van de gemeente. Deze taak kan echter ook aan de CISO worden gemandateerd.[23]

De BIO verplicht tot het opstellen van informatiebeveiligingsbeleid

De BIO geeft aan dat er een informatiebeveiligingsbeleid nodig is en zet uiteen waar dit beleid aan moet voldoen. Zo dienen bijvoorbeeld de strategische uitgangspunten en randvoorwaarden te worden vastgelegd, dient het beleid inzicht te geven in de verantwoordelijkheidsverdeling op het gebied van informatiebeveiliging en moeten de gemeenschappelijke betrouwbaarheidseisen en normen van de organisatie worden geformuleerd. Daarnaast schrijft de BIO voor dat het informatiebeveiligingsbeleid periodiek moet worden geëvalueerd.

De CISO is verantwoordelijk voor het in goede banen leiden van de uitvoering van het informatiebeveiligingsbeleid en de beheersmaatregelen (zoals het opstellen van voortgangsrapportages), zoals benoemd in de BIO.[24] Gemeenten kunnen middels verschillende jaarlijkse toetsen en risicoanalyses (waaronder zogeheten GAP-analyses) nagaan in hoeverre zij voldoen aan de BIO.[25]

[20] Baseline Informatiebeveiliging Gemeenten (2020).
[21] Baseline Informatiebeveiliging Gemeenten (2020).
[22] Baseline Informatiebeveiliging Gemeenten (2020).
[23] Baseline Informatiebeveiliging Gemeenten (2020).
[24] Baseline Informatiebeveiliging Gemeenten (2020), pp.25-29.
[25] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p.9.

2. Invulling van de kaders binnen de gemeente Zoetermeer

2.1. Inleiding

De gemeente Zoetermeer heeft verschillende (beleids-)kaders vastgesteld waarin wordt uitgelegd hoe de gemeente invulling geeft aan de richtlijnen uit de AVG. In dit hoofdstuk wordt ingegaan op deze gemeentelijke kaders, te weten: het privacybeleid en het informatiebeveiligingsbeleid. Hierbij wordt gekeken naar de gemeentelijke normen en richtlijnen, niet naar de invulling hiervan in de praktijk. De praktijkinvulling wordt behandeld in hoofdstuk 3.

2.2. Privacybeleid

2.2.1. Toelichting op het privacybeleid

Het privacybeleid van de gemeente voldoet op grote lijnen aan de richtlijnen van de AVG

Uit het privacybeleid van de gemeente moet volgens de AP blijken op welke manier de gemeente voldoet aan de verplichtingen uit de AVG. Zoals in paragraaf 1.2.1. beschreven geeft de Autoriteit Persoonsgegevens een aantal handvatten waar een privacybeleid aan moet voldoen om te zorgen dat de gemeente voldoet aan de verantwoordingsplicht.

Op 7 mei 2019 heeft het college van de gemeente Zoetermeer het privacybeleid vastgesteld. Met het privacybeleid van de gemeente, wat hieronder verder wordt uitgelegd, voldoet de gemeente op hoofdlijnen aan de relevante richtlijnen voor het opstellen van privacybeleid.[26] Op twee punten wijkt het privacybeleid van de gemeente af van wat de Autoriteit Persoonsgegevens van een privacybeleid vraagt. Allereerst kent het privacybeleid geen omschrijving van de categorieën van persoonsgegevens die door de gemeente worden verwerkt. Daarnaast koppelt het gemeentelijke privacybeleid de verwerking van de verschillende categorieën van persoonsgegevens niet aan doeleinden en grondslagen voor verwerking. Dat de gemeente op deze punten afwijkt van wat de AP voorschrijft is te begrijpen gezien de omvang en veranderlijkheid van deze opsommingen.

Het privacybeleid is vastgesteld voor de duur van drie jaar en zou daarna worden geëvalueerd. Gezien de datum van vaststelling (7 mei 2019) zou de evaluatie al plaatsgevonden moeten hebben. De organisatie ziet dit rapport ook mede als evaluatie van het privacybeleid.

Het privacybeleid werkt vanuit drie uitgangspunten

[26] Autoriteit Persoonsgegevens (2019). Zes aanbevelingen voor privacybeleid: https://autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid.

Het gemeentelijk privacybeleid gaat uit van drie uitgangspunten voor het waarborgen van een juiste gegevensbescherming:

- **Werkbaar en zorgvuldig**: De gemeente verwerkt 1)persoonsgegevens altijd binnen de kaders van de AVG, 2)zorgt dat persoonsgegevens alleen verwerkt worden voor het doel waarvoor ze verzameld zijn, 3) dat er niet meer of minder persoonsgegevens verwerkt worden dan noodzakelijk en 4) dat er altijd een wettelijke grondslag voor verwerking is. Daarbij gebruikt de gemeente zoveel mogelijk bronsystemen (zoals de basisregistraties) zodat juistheid van de gegevens gewaarborgd is. Op die manier moeten burgers kunnen vertrouwen op een zorgvuldige verwerking van hun persoonsgegevens. Het beleid op het gebied van privacy mag niet dusdanig ingewikkeld zijn dat het zorg- en dienstverlening in de weg staat.[27]
- **Privacy op de werkvloer:** Voor de gemeente is het opstellen van beleid niet voldoende voor een zorgvuldige omgang met persoonsgegevens. Het voldoen aan de eisen van de AVG moet onderdeel zijn van de dagelijkse praktijk van de gemeentelijke organisatie. Daarom zijn er workshops en trainingen georganiseerd en is er een netwerk van privacyambassadeurs voor meer aandacht voor privacybewustzijn. Privacy is daarbij voor de gemeente onderdeel van het integriteitsbeleid. Daarom mag van een goede ambtenaar naleving van de privacyregels verwacht worden.[28]
- **Privacy vanaf de start**: Een derde uitgangspunt voor de gemeente op het gebied van privacy is het meenemen van de eisen uit de AVG in de ontwikkeling van beleid, regelgeving en nieuwe systemen. Hiermee past de gemeente het principe van *privacy by design* toe.

2.2.2. Relevante richtlijnen uit het privacybeleid

De afdelingshoofden hebben een grote verantwoordelijkheid in het privacybeleid

Het privacybeleid schrijft voor dat in de gemeentelijke organisatie de verantwoordelijkheid voor een zorgvuldige verwerking van persoonsgegevens bij de afdelingshoofden belegd is. Daarin is ieder afdelingshoofd dus verantwoordelijk voor zijn of haar afdeling. Als het nodig is kan het afdelingshoofd deze verantwoordelijkheid beleggen in de afdeling. Wanneer er sprake is van verwerking van persoonsgegevens die de afdeling overstijgt, ligt de verantwoordelijkheid bij de proceseigenaar.

Het afdelingshoofd is volgens het privacybeleid ook verantwoordelijk voor het bijhouden van het register van verwerkingen. Iedere afdeling moet een overzicht van verwerkingen van persoonsgegevens hebben. Op basis hiervan moet duidelijk zijn wie intern verantwoordelijk is voor de verwerkingen en wie eindverantwoordelijk draagt voor het totaaloverzicht.[29]

Het privacybeleid verplicht tot het aanstellen van een FG en PO

Het privacybeleid schrijft voor dat de gemeente een Functionaris Gegevensbescherming en een Privacy Officer aanstelt. In hoofdstuk 3 wordt verder ingegaan op de posities en de rolinvulling van deze functionarissen.

[27] Privacybeleid gemeente Zoetermeer, p.3.
[28] Privacybeleid gemeente Zoetermeer, p.3.
[29] Privacybeleid gemeente Zoetermeer, p.4.

Het privacybeleid zet in op passende maatregelen voor informatiebeveiliging

De gemeentelijke organisatie is verantwoordelijk voor het treffen van technische en organisatorische maatregelen voor de verwerking van persoonsgegevens. Bij incidenten zijn er procedures om gevolgen te beperken en herhaling te voorkomen. Incidenten moeten gemeld worden bij de FG, de Privacy Officer en/of de CISO. Deze personen maken, wanneer dat nodig is, melding bij de Autoriteit Persoonsgegevens van incidenten én overleggen met de afdelingsmanager of betrokkenen moeten worden ingelicht.[30]

Het beleid schrijft het vastleggen van werkprocedures en het sluiten van verwerkersovereenkomsten voor

Voor processen waarin persoonsgegevens worden verwerkt en er een hoge mate van herhaling is, moeten er werkprocedures of protocollen worden opgesteld. In deze werkprocedures moet worden opgenomen welke stappen worden doorlopen en hoe met gegevensverwerking moet worden omgegaan.

Wanneer de gemeente aan een externe vraagt om namens de gemeente persoonsgegevens te verwerken, moet de gemeente een verwerkersovereenkomst opstellen. Het sluiten van die overeenkomst is volgens het privacybeleid de verantwoordelijkheid van het afdelingshoofd. De FG ziet toe op de naleving van de overeenkomst. In het verwerkingsregister moet door de afdeling tevens worden bijgehouden welke samenwerkings- en verwerkersovereenkomsten er zijn.

Het privacybeleid heeft aandacht voor de positie en rechten van betrokkenen

Transparantie over de verwerking van persoonsgegevens is belangrijk voor de gemeente. Met het privacystatement op de gemeentelijke website worden inwoners geïnformeerd over de verwerking van hun gegevens. Verder is via de gemeentelijke website informatie beschikbaar over privacy gerelateerde onderwerpen en kunnen inwoners digitaal of telefonisch om meer informatie vragen. Ook kunnen inwoners via een speciaal mailadres contact zoeken met de FG.[31]

Naast het privacystatement op de website kent de gemeente ook een privacystatement voor het verwerken van gegevens van medewerkers. Hierin worden medewerkers op dezelfde manier geïnformeerd als inwoners in het overkoepelende privacystatement. Ook medewerkers kunnen contact zoeken met de FG met vragen of opmerkingen over de bescherming van hun gegevens.[32]

2.3. Informatiebeveiligingsbeleid

2.3.1. Toelichting op het informatiebeveiligingsbeleid

De gemeente kent een actueel strategisch beleidskader dat voldoet aan de eisen uit de BIO

De BIO verplicht gemeenten tot het vaststellen van een informatiebeveiligingsbeleid en geeft daarbij eisen waar het informatiebeveiligingsbeleid aan moet voldoen. Het door de gemeente Zoetermeer

[30] Privacybeleid gemeente Zoetermeer, p.5.
[31] Gemeente Zoetermeer, Privacystatement.
[32] Gemeente Zoetermeer, privacy statement medewerkers

vastgestelde informatiebeveiligingsbeleid is opgesteld aan de hand van de tien principes voor informatiebeveiliging van de Vereniging Nederlandse Gemeenten (VNG).[33] De eisen die de BIO stelt aan het informatiebeveiligingsbeleid zijn onderdeel van het vastgestelde beleid.

Op 15 december 2020 heeft het college van de gemeente Zoetermeer het gemeentelijk informatiebeveiligingsbeleid 2020-2023 vastgesteld. Dit beleidskader vervangt een eerder beleidskader uit 2018 dat destijds was opgesteld naar aanleiding van de invoering van de AVG. Het informatiebeveiligingsbeleid vormt het kader voor alle maatregelen die de gemeente neemt om ervoor te zorgen dat de gemeente voldoet aan relevante wet- en regelgeving.[34] Het gemeentelijk informatiebeveiligingsbeleid is een strategisch document dat voor een langere periode geldt. Op basis hiervan wordt jaarlijks een informatiebeveiligingsplan opgesteld door de CISO, onder verantwoordelijkheid van de directie. De directie is verantwoordelijk voor het uitwerken en uitvoeren van maatregelen die voortkomen uit het beveiligingsbeleid en -beleidsplan.[35]

De onderzoekers hebben begrepen dat het informatiebeveiligingsbeleid op verschillende punten zal worden geactualiseerd.

Het informatiebeveiligingsbeleid kent elf strategische doelstellingen

Centraal in het informatiebeveiligingsbeleid staan een elftal strategische doelstellingen. Deze worden hieronder weergegeven:[36]

Figuur 1: Elf strategische doelen van het informatiebeveiligingsbeleid van de gemeente Zoetermeer.

[33] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 4.; VNG (2019). Tien bestuurlijke principes voor informatiebeveiliging, pp. 4-8.
[34] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 4.
[35] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 8.
[36] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 7.

In het beleidskader informatiebeveiliging worden de verplichtingen uit de BIO en de AVG samengevat. Op basis van deze verplichtingen zijn in het beleidskader verschillende uitgangspunten geformuleerd voor de borging van informatiebeveiliging in Zoetermeer. De belangrijkste uitgangspunten zijn:[37]

- Het college van burgemeester en wethouders is bestuurlijk eindverantwoordelijk voor de informatiebeveiliging in de gemeente en schept de randvoorwaarden om deze te waarborgen;
- Uitvoering en handhaving van regels over informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Voor alle informatiebronnen en -systemen binnen de gemeente is een interne eigenaar aangewezen die primair verantwoordelijk is voor de bescherming van de betreffende informatie;
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie;
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn;
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Afdelingshoofden zijn verantwoordelijk voor het uitvoeren van QuickScans informatiebeveiliging op basis van de BIO om deze risico-afwegingen te kunnen maken. Zij worden hierin ondersteund door de tweede lijn.

2.3.2. Relevante richtlijnen uit het informatiebeveiligingsbeleid

Het beleid schrijft een jaarlijks informatiebeveiligingsplan voor

Zoals hierboven benoemd moet volgens het informatiebeveiligingsbeleid ieder jaar onder leiding van de CISO een informatiebeveiligingsplan worden opgesteld, met acties en maatregelen voor het betreffende jaar. Welke acties en maatregelen worden uitgevoerd, moet hierbij worden bepaald aan de hand van vier gegevens: een risicoanalyse op het BIO-normenkader, de uitkomsten van de jaarlijkse ENSIA-rapportage, het Dreigingsbeeld Nederlandse Gemeenten van de Informatiebeveiligingsdienst (IBD) en door afdelingshoofden aangedragen onderwerpen.[38]

Het informatiebeveiligingsbeleid hanteert het Three Lines of Defence-model

In het informatiebeveiligingsbeleid wordt voorgeschreven dat de gemeente Zoetermeer in de organisatie gebruik maakt van het zogeheten Three Lines of Defence-model (3LoD-model). Hierin wordt zoals de naam aangeeft gewerkt met drie 'lijnen' voor de gemeentelijke processen. De eerste lijn bestaat uit het lijnmanagement: de afdelingshoofden, die het managementteam vormen. De eerste lijn moet toezien op alle procedures waarmee invulling wordt gegeven aan informatiebeveiliging. De tweede lijn bestaat uit de CISO en senior adviseurs informatiebeveiliging. De tweede lijn heeft een ondersteunende, adviserende en coördinerende rol en dient te bewaken in hoeverre het lijnmanagement zijn verantwoordelijkheden neemt. De derde lijn bestaat volgens het beleid uit de Verbijzonderde Interne Controle (VIC). Hieronder wordt dit nader toegelicht.[39]

De directie is verantwoordelijk voor de aansturing, de afdelingshoofden voor de uitvoering

[37] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 7.
[38] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 9.
[39] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 13.

De directie is volgens het 3LoD-model verantwoordelijk voor de aansturing van het informatiebeveiligingsbeleid in Zoetermeer. De directie moet ervoor zorgen dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De afdelingshoofden dienen zich te verantwoorden over de uitvoering. De directie dient er verder zorg voor te dragen dat de eindverantwoordelijke portefeuillehouders binnen het college geïnformeerd worden over de uitvoering van informatiebeveiliging. Zo kan het college zich ook verantwoorden naar de raad. Tenslotte heeft de directie de taak om toe te zien op de benodigde procedures en uitvoeringsmaatregelen en deze te autoriseren. De CISO dient de directie hier in bij te staan.[40]

Afdelingshoofden vormen de eerste lijn in het 3LoD-model en dragen dus verantwoordelijkheid voor de uitvoering. Volgens het beleid kan een afdelingshoofd uitvoeringswerkzaamheden delegeren binnen de afdeling, maar blijft deze eindverantwoordelijkheid dragen voor informatiebeveiliging binnen de afdeling. Het beleid schrijft voor dat jaarlijks minimaal tweemaal in het managementteam wordt afgestemd over de inhoudelijke aanpak van informatiebeveiliging.[41]

Het informatiebeveiligingsbeleid omschrijft de volgende taken van de afdelingshoofden:[42]

- Het leveren van input voor wijzigingen van beveiligingsmaatregelen en -procedures;
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures;
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld. I&A heeft hierin een mede signalerende rol, aangezien veel van dit soort incidenten via hen worden geconstateerd;
- Bij overeenkomsten of afspraken met ketenpartners en leveranciers ook aspecten van informatiebeveiliging meenemen en vastleggen;
- Bespreken van beveiligingsincidenten en de consequenties die dat met zich meebrengt voor het beleid. De voorbereiding en coördinatie van het overleg ligt bij de CISO;'

De tweede lijn ondersteunt de organisatie bij het naleven van het beleid

De tweede lijn dient volgens het 3LoD-model de organisatie bij het naleven van het informatiebeveiligingsbeleid te ondersteunen. De tweede lijn bestaat volgens het beleid uit de CISO (ondergebracht bij de afdeling concerncontrol) en de senior adviseurs informatiebeveiliging (onderdeel van de afdeling I&A). De senior adviseurs zijn samen met de CISO verantwoordelijk voor het uitvoeren van een aantal standaard taken, waaronder:[43]

- Het uitvoeren van de risico- en GAP-analyses op basis van de BIO;
- Het opstellen van het jaarlijks informatiebeveiligingsplan;
- Het opstellen en aanpassen van het Informatiebeveiligingsbeleid;
- Het opstellen van onderwerp-specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid;
- Het adviseren over informatiebeveiliging bij grote en kleine projecten, aanbestedingen en inkooptrajecten;

[40] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 13.
[41] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 13.
[42] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, pp. 13-14.
[43] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, pp. 14.

- Het registreren en afhandelen van incidenten en vragen in Topdesk;
- Het beheer van de infrastructuur van informatiebeveiliging;
- Het uitvoeren van zogeheten pentesten en Vulnerability Assessments;
- Het organiseren van bewustwording over informatiebeveiliging middels onder andere roadshows en workshops voor medewerkers;
- Het uitvoeren van de audits: ENSIA en EDP;

De CISO dient te fungeren als toezichthouder op alle taken en maatregelen in het kader van informatiebeveiliging. De CISO draagt verantwoordelijkheid voor het opstellen van het informatiebeveiligingsbeleid, het faciliteren van afstemming en overleg binnen de organisatie en het borgen van samenhang tussen alle verschillende maatregelen en processen.[44]

Controle en verantwoording vindt plaats in de derde lijn

Volgens het 3LoD-model controleert de derde lijn, de zogeheten Verbijzonderde Interne Controle (VIC), of het toetsingsproces van informatiebeveiligingsmaatregelen aan het BIO-normenkader correct wordt doorlopen. De gemeente dient zich hierover te verantwoorden door middel van de ENSIA-systematiek. Hiervoor is een ENSIA-coördinator aangewezen, die zorgt dat alle informatie die nodig is voor de jaarlijkse toets wordt opgehaald bij de afdelingshoofden. De ENSIA-verklaring dient ieder jaar terug te komen in het jaarverslag middels de collegeverklaring informatiebeveiliging. Hierin dient te zijn vermeld welke eventuele verbetermaatregelen de gemeente zal treffen. College en raad worden via de ENSIA-verantwoording geïnformeerd over de uitvoering.[45]

Zoals aangegeven zal het informatiebeveiligingsbeleid worden geactualiseerd. Het beleid zal dan (deels) worden aangepast naar de praktijk. De VIC heeft (nog) geen of slechts een beperkte rol als het gaat om informatiebeveiliging. De derde lijn, het toezicht, wordt ingevuld door de CISO.

[44] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 14.
[45] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 15.

3. Organisatie in beeld

3.1. Inleiding

Dit hoofdstuk gaat in op de vertaling en toepassing van de AVG in de gemeentelijke organisatie. Om de stand van zaken in de organisatie in kaart te brengen zal geput worden uit de door de gemeente aangeleverde documenten en de interviews met respondenten. Allereerst wordt ingegaan op de implementatie van de AVG-richtlijnen in Zoetermeer en de manier waarop de organisatie van gegevensbescherming is ingericht. Hierna wordt ingegaan op de kennisborging in de organisatie, de inrichting van de archieffunctie en de wijze van verantwoording. Ten slotte worden de bevindingen uit de drie nader onderzochte domeinen gepresenteerd.

Naast de documenten en de interviews hebben de onderzoekers een digitale enquête onder de medewerkers van de drie domeinen uitgezet. Op verschillende punten in dit hoofdstuk zal geput worden uit de resultaten van de enquête. De enquête richt zich op het krijgen van een beeld van het kennisniveau van de AVG onder medewerkers en de mate waarin medewerkers ondersteuning vanuit de organisatie ervaren in het werken met de AVG. Er zullen op basis van alleen de uitkomsten van de enquête echter geen harde conclusies getrokken kunnen worden. Daarom wordt ook gekeken naar relevante informatie uit de documenten en de interviews, en in hoeverre deze aansluit bij de uitkomsten van de enquête.

3.2. Implementatie van de AVG in Zoetermeer

3.2.1. Stappen van het implementatieproces

De voorbereiding van implementatie is gestart in 2016

Sinds 25 mei 2018 is de gemeente Zoetermeer aanspreekbaar op de naleving van de AVG. In de twee voorafgaande jaren heeft de gemeente de mogelijkheid gehad om de AVG te implementeren in de organisatie. Uit documentatie blijkt dat de gemeente zich sinds het inwerkingtreden van de AVG in mei 2016 al voorbereidde op de implementatie van de AVG in de organisatie.[46] In de twee jaren waarin de AVG al in werking was getreden heeft de gemeente in verschillende fasen uitvoering gegeven aan de implementatie van de AVG. Dit proces is grotendeels verlopen aan de hand van het stappenplan van de Autoriteit Persoonsgegevens voor de implementatie van de AVG.

De door de gemeente verstrekte documentatie laat zien dat er gedurende de periode van twee jaar in verschillende stappen is gewerkt aan de implementatie. Hierbij zijn medewerkers op het gebied van informatie(beveiliging), securitybeleid, ICT, juridische zaken, financiën en governance betrokken geweest.

[46] Gemeente Zoetermeer (2016). Plan van aanpak compliance AVG.

De implementatie kreeg in de periode 2017-2018 concreet vorm

In februari 2018 is door de privacy officer een uitgebreide rapportage opgesteld over de stand van zaken van de implementatie van de AVG op dat moment. Hieruit komt naar voren dat de gemeente de volgende acties tot dan toe heeft ondernomen:

- Een bewustwordingsactie binnen de organisatie, met workshops voor nieuwe medewerkers, een 'roadshow' voor medewerkers en raadsleden langs alle afdelingen en het inzetten van zogeheten privacy-ambassadeurs in de organisatie;[47]
- Het vernieuwen van het privacybeleid en het updaten van een register van verwerkingen;
- Het aanstellen van een Functionaris voor de Gegevensbescherming (FG) per 5 december 2017;
- Het instellen van een vaste procedure voor het melden van datalekken bij de Autoriteit Persoonsgegevens;[48]

Daarnaast is in juni 2018 een interne presentatie gegeven over de stand van zaken op dat moment. Hierin is aangegeven welke acties op dat moment nog niet gereed, gedeeltelijk gereed, voor een belangrijk deel gereed of volledig op orde zijn. Hieruit blijkt dat alleen de Privacy Impact Assessments (PIA's) en het invulling geven aan privacy by design en privacy by default nog niet volledig gereed waren.[49]

Raad en college zijn actief geïnformeerd bij de implementatie door middel van memo's

In de periode oktober 2016 - mei 2018 zijn gemeenteraad en college door de ambtelijke organisatie periodiek geïnformeerd over de voortgang van de implementatie van de AVG. Deze informatievoorziening bestond uit memo's waarin onder andere een toelichting werd gegeven op de belangrijkste ontwikkelingen (zoals bijvoorbeeld het opzetten van een verwerkingsregister en het aanstellen van een FG). Ook werden raad en college middels deze informatiememo's geïnformeerd over de datalekken die zich in de voorgaande maanden voordeden.[50]

Het stappenplan voor implementatie is doorlopen maar nog niet geheel succesvol

In de voor dit onderzoek gevoerde gesprekken is aangegeven dat in 2022 een groot deel van de stappen uit het stappenplan van de Autoriteit Persoonsgegevens is uitgevoerd. Gesprekspartners geven aan dat volgens huidige stand van zaken de gemeente een heel eind is met de uitvoering van het stappenplan, maar dat er op onderdelen nog verbetermogelijkheden zijn. Zo geven gesprekspartners aan dat de verschillende verwerkingsregisters zijn opgezet, maar dat niet altijd alle relevante processen in die registers zijn opgenomen. Daarnaast worden mogelijk niet altijd alle datalekken als zodanig herkend en gemeld. Verder kan er volgens diverse gesprekspartners actiever worden gewerkt aan structureel

[47] Gemeenteraad Zoetermeer (2019). Roadshow informatiebeveiliging en privacy: https://zoetermeer.bestuurlijkeinformatie.nl/Agenda/Document/8c21252e-3e54-4369-9417-8baa3a83ca06?documentId=207422a4-28ca-47c7-bee6-ef125e634418&agendaItemId=614e13be-7095-48b0-8dc1-49f7486803a7.
[48] Gemeente Zoetermeer (2018). Stand van zaken implementatie AVG februari 2018.
[49] Gemeente Zoetermeer (2018). Interne presentatie stand van zaken AVG.
[50] Gemeente Zoetermeer (2016-2018). Memo's privacy voor raad en college, periode oktober 2016 – mei 2018.

bewustzijn en kennisopbouw onder medewerkers. Hieronder wordt per deelonderwerp nader ingegaan op de huidige praktijkinvulling van de AVG-richtlijnen in Zoetermeer.

3.3. Organisatie van gegevensbescherming

3.3.1. Rolneming en het Three Lines of Defence-model

Het Three Lines of Defence-model wordt in de praktijk anders ingevuld

Zoals beschreven in hoofdstuk 2 beoogt de gemeente Zoetermeer volgens het informatiebeveiligingsbeleid met het Three Lines of Defence-model (3LoD-model) voor inrichting van de privacyorganisatie te werken.[51] In de praktijk wordt wel uitgegaan van het 3LoD-model als het gaat om de organisatie van informatiebeveiliging en privacy, maar wordt het model anders ingevuld dan in het informatiebeveiligingsbeleid staat omschreven. De toelichting op het 3LoD-model op het gemeentelijk intranet gaat uit van een andere verdeling van functionarissen over de drie lijnen. In het bijzonder de invulling van de tweede en derde lijn, respectievelijk 'expertise' en 'toezicht.' Gesprekspartners geven ook een verschillende uitleg van het 3LoD-model en hoe dit in de organisatie zou zijn geïmplementeerd. Rollen lijken door elkaar te lopen en verschillend te worden geïnterpreteerd. Sommige gesprekspartners geven aan tot voor kort nog niet van dit model te hebben gehoord.

Hieronder wordt een verdere toelichting gegeven op de praktijkinvulling van het 3LoD-model.

De afdelingshoofden zijn verantwoordelijk

Waar in het beleid wordt aangegeven dat de eerste lijn gevormd wordt door de afdelingshoofden, komt uit de gevoerde gesprekken naar voren dat 'de afdelingen' verantwoordelijk zijn voor de informatiebeveiliging binnen hun vakdomein. Dit stemt meer overeen met het principe dat de direct betrokken medewerkers in de eerste plaats verantwoordelijk zijn voor de uitvoering. De eerste lijn draagt volgens het beleid echter niet alleen de verantwoordelijkheid voor een goed uitvoeringsproces, maar heeft ook de taak om toe te zien of dit volgens de richtlijnen plaatsvindt (compliance). Dat gebeurt door te werken met het vier ogen principe, casusbesprekingen te organiseren en deelwaarnemingen van de kwaliteitsmedewerkers in de afdeling. In de praktijk is het volgens gesprekspartners onvoldoende duidelijk wat precies de rol van de afdelingshoofden is en wordt hier ook verschillend invulling aan gegeven. Op basis van de gesprekken is het beeld dat de afdelingshoofden momenteel minder aandacht hebben voor het werken met de AVG dan van hen verwacht wordt in het beleidskader.

Overlap tussen de tweede en de derde lijn

Volgens het 3LoD-model in het huidige informatiebeveiligingsbeleid bestaat de tweede lijn uit de CISO en de senior adviseurs informatiebeveiliging. De tweede lijn heeft een ondersteunende, adviserende en coördinerende rol en dient te bewaken in hoeverre het lijnmanagement (de eerste lijn) zijn verantwoordelijkheden neemt. De derde lijn heeft als taak te controleren of de uitgevoerde maatregelen in lijn zijn met de (wettelijke) richtlijnen, en dient hierover te rapporteren.[52]

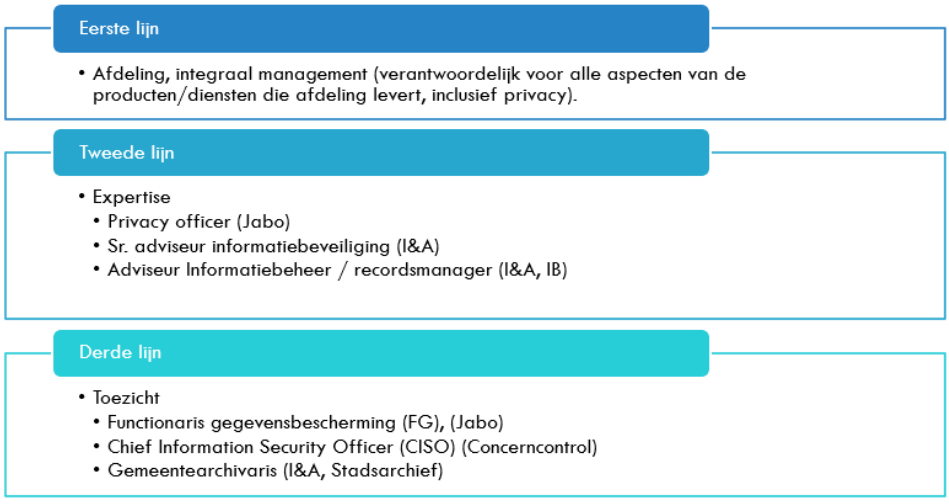
De gemeente heeft op basis van een handreiking van de Informatiebeveiligingsdienst (IBD) een functieprofiel voor de CISO opgesteld. De Ciso is onafhankelijk gepositioneerd bij concerncontrolling. In

[51] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 13.
[52] Gemeente Zoetermeer (2020). Gemeentelijk informatiebeveiligingsbeleid 2020-2023, p. 13.

het functieprofiel is opgenomen welke kerntaken de CISO volgens de landelijke richtlijn heeft.[53] In het functieprofiel wordt toegelicht dat een groot deel van deze kerntaken niet als zodanig wordt ingevuld door de CISO in Zoetermeer, maar door de senior adviseurs informatiebeveiliging. Uit de gesprekken komt naar voren dat de CISO zich in de praktijk niet alleen als toezichthouder opstelt, maar ook vanuit een meewerkende rol BIO prioriteiten op concern- en managementniveau oppakt en aanjaagt. Ook heeft de gemeente aangegeven dat de positionering van de CISO in het 3LoD-model bij de herziening van het informatiebeveiligingsbeleid zal worden geactualiseerd naar de huidige praktijkinvulling.

Uit de gesprekken komt ook naar voren dat de tweede lijn in de praktijk wordt ingevuld door de senior adviseurs informatiebeveiliging en de PO. De CISO kan zich hierdoor meer richten op de derde lijn: het controleren of de genomen maatregelen in lijn zijn met de richtlijnen, en het rapporteren hierover. In de derde lijn is ook een rol weggelegd voor de FG en voor de gemeentearchivaris. Over het beleggen van de archieffunctie in de gemeente wordt een aparte toelichting gegeven in paragraaf 3.5.

In de gevoerde gesprekken kwam naar voren dat er weliswaar ieder jaar een duidelijke prioritering is, maar dat de senior adviseurs informatiebeveiliging vaak bezig zijn met de dagdagelijkse problemen en lopende zaken. De CISO richt zich blijkens de gesprekken meer op beveiligingsmaatregelen die aandacht nodig hebben op concern- en managementniveau, zoals bijvoorbeeld het laten opstellen van continuïteitsplannen en het organiseren van trainingen ten bate van crisisbeheersing. De wens bestaat om in de tweede lijn meer aandacht te hebben voor de prioriteiten die op grotere afstand staan van de dagelijkse praktijk. In gesprekken is aangegeven dat de organisatie nog zoekende is op dit vlak en overweegt om zogeheten domein-ISO's aan te stellen. Deze domein-ISO's zouden net als de privacy-ambassadeurs een aanspreekpunt kunnen vormen voor hun eigen afdeling of domein, over informatiebeveiliging.



Figuur 2. Praktijkinvulling organisatie 3LoD-model. Bron: Gemeente Zoetermeer (2021). Presentatie DT voortgang IPI, d.d. 4 oktober 2021.

Rol van de FG vraagt om meer capaciteit

[53] Gemeente Zoetermeer (geen datering). Functieprofiel CISO.

De gemeente voldoet sinds 2017 aan de verplichting tot het aanstellen van een FG.[54] De FG is een interne onafhankelijke toezichthouder op de naleving van de AVG en de toepassing en implementatie van het privacybeleid. De FG is daardoor gepositioneerd in de derde lijn van het Three lines of defence-model. De FG heeft de mogelijkheid om maatregelen te treffen in geval van calamiteiten of gebreken en krijgt toegang tot verwerkingsactiviteiten die worden uitgevoerd. Ook maakt de FG melding van datalekken bij het college als dat nodig is.

In verschillende voor dit onderzoek gevoerde gesprekken kwam naar voren dat de FG weinig capaciteit (in aantal FTE) heeft om invulling te geven aan de rol van FG. Voor de taak van FG zijn in Zoetermeer op dit moment slechts enkele uren per week beschikbaar. De FG komt hierdoor nauwelijks toe aan het toezien op naleving van het privacybeleid, het uitbrengen van advies over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten.. Ook voor het uitvoeren van structurele controles die toezien of de AVG door de organisatie goed wordt toegepast is weinig tot geen capaciteit beschikbaar. Een auditplan of controlecyclus is er (nog) niet. Het gebrek aan capaciteit hangt samen met het gegeven dat de FG ook teammanager is en verantwoordelijkheid draagt voor een afdelingsteam. Voor de toekomst werd daarom genoemd dat het een optie zou zijn om een eigenstandige positie voor de FG in te richten en de FG onderdeel te maken van concerncontrol. Deze suggestie sluit aan bij de handreiking positionering en taken van de FG van de informatiebeveiligingsdienst, waarin de suggestie wordt gedaan om voor de FG functie een staffunctie in te richten zonder enige inbedding in de hiërarchie. Hierbij kan een voorbeeld genomen aan de positionering van de gemeentelijke concerncontroller, die ook onder het hoogste bestuurlijke gezag gepositioneerd is. Op het moment dat de FG meer capaciteit heeft is het ook beter mogelijk om toezicht te houden op de uit te voeren audits en DPIA's en kan ook worden toegekomen aan het zelf uitvoeren van audits.

De AVG geeft de gemeente een aantal plichten ten aanzien van de FG. Zo moet de gemeente als verwerkingsverantwoordelijke zorgen dat de FG de tijd en middelen tot zijn beschikking heeft om de taken van een FG te kunnen vervullen en zijn deskundigheid als FG in stand te houden.[55] In gemeenten met een vergelijkbare grootte zoals Zwolle, Leiden[56], Leeuwarden en Ede is de FG een fulltime functie[57] In de gevoerde interviews komt naar voren dat de zeer beperkte beschikbaarheid van de FG een knelpunt is.

De invulling van de rol van FG komt niet overeen met de AVG

Door het combineren van de rol van FG met die van teammanager is niet alleen sprake van een gebrek aan tijd, maar ontstaat er ook een positie voor de FG waarbij de onafhankelijkheid in het geding komt. Als het gaat om het combineren van werkzaamheden met de functie van FG stelt de AVG dat de FG andere taken of plichten kan vervullen maar dat deze taken en plichten niet mogen leiden tot een belangenconflict. De *Guidelines on Data Protection Officers* van de Europese privacytoezichthouders verduidelijkt deze bepaling door aan te geven dat belangenconflicten in ieder geval optreden wanneer de FG voor deze andere verantwoordelijkheden doelstellingen van of middelen voor de verwerking van persoonsgegeven moet bepalen.[58] De Handreiking positionering en taken van de FG van de

[54] Artikel 37 lid 1, Algemene verordening gegevensbescherming.
[55] Artikel 38 lid 2, Algemene verordening gegevensbescherming.
[56] De FG van de gemeente Leiden bedient ook drie omringende kleine gemeenten.
[57] Zo volgt uit navraag bij deze gemeentes.
[58] Guidelines on Data Protection Officers (‘DPOs’), p.16.

informatiebeveiligingsdienst voegt daaraan toe dat een FG ook geen andere taken of plichten mag vervullen waarin er sprake is van een aanzienlijke operationele verantwoordelijkheid voor gegevensverwerkingsprocessen.[59] Concreet betekent het dat de FG niet ook verantwoordelijke voor (privacy) compliance mag zijn of mag beslissen over de aanschaf van IT-systemen. De FG is als teammanager JaBo rechtstreeks leidinggevende van de subteams privacy - waar de PO werkzaam is- , inkoop en onderzoek & statistiek. Daarmee lijkt de verantwoordelijkheid van de teammanager bij het bepalen van doelstellingen of middelen voor de verwerking van persoonsgegevens en de operationele verantwoordelijkheid voor gegevensverwerkingsprocessen een feit. Daarmee is per saldo sprake van ongewenste rolvermenging.

Tot slot verplicht de AVG de FG tot het uitbrengen van rechtstreeks verslag aan de hoogste leidinggevende van de gemeente.[60] Uit de voor dit onderzoek gevoerde gesprekken kwam naar voren dat de FG geen rapportages maakt voor de gemeentesecretaris, maar wel tweemaal per jaar samen met de CISO en gemeentearchivaris aansluit bij het directieteam en een mondeling toelichting geeft op gedane bevindingen. De al eerder genoemde *Guidelines on Data Protection Officers* plaatst deze plicht van de FG in context. De guideline stelt dat de rapportages van de FG aan de gemeentesecretaris ook een middel is om het hogere management de opvatting van de FG mede te delen op het moment dat de organisatie beslissingen neemt tegen het advies van de FG in. Om te zorgen dat het verslag van de FG deze functie kan vervullen is het belangrijk om schriftelijk te rapporteren.

Concluderend beschikt de FG momenteel over te weinig capaciteit om zowel teammanager als toezichthouder te kunnen zijn. Hierdoor kan de FG cruciale taken op het gebied van toezicht en monitoring niet vervullen. Daarmee voldoet de gemeente niet aan deze verplichting uit de AVG en lopen rollen door elkaar.

De PO is veel tijd kwijt aan het adviseren bij acute vraagstukken

Naast de FG kent de gemeente een PO (privacy officer). De positie van de PO is niet wettelijk vastgelegd zoals bij de FG en kent daardoor meer vrijheid in de rolinvulling. In de gemeente Zoetermeer voorziet de PO de organisatie van advies in het verwerken van persoonsgegevens. Zo is de PO verantwoordelijk voor de beoordeling van datalekken, is de PO betrokken als adviseur bij de DPIA's die uitgevoerd moeten worden en heeft de PO een faciliterende rol.[61] In veel organisaties is de PO daarnaast een belangrijk aanspreekpunt als het gaat om AVG-gerelateerde zaken. Naarmate een organisatie groter wordt en/of naarmate er meer persoonsgegevens moeten worden verwerkt, zullen er meer vragen ontstaan over de verwerking daarvan. In Zoetermeer is dit niet anders. Dit betekent dat de PO zowel veel taken heeft die zien op het borgen van de privacyrichtlijnen, als op het gebied van advisering en ondersteuning.

In de gemeente zijn er twee personen die invulling geven aan de taken van de PO, een voor 27 uur in de week en een voor 8 uur in de week, zo blijkt uit de gevoerde gesprekken. Daarmee heeft de gemeente net iets minder dan 1 fte aan PO capaciteit beschikbaar. Gezien de omvang van de gemeente is dat relatief weinig. Daardoor heeft de PO, net als de FG, een capaciteitsprobleem. Navraag bij de gemeenten Leiden, Leeuwarden en Ede leert dat zij respectievelijk over PO capaciteit beschikken van 2,3 FTE (met streven naar 3 FTE), 2 FTE (waarvan 1 FTE juridisch ingestoken en 1 FTE managementgericht) en 0,89

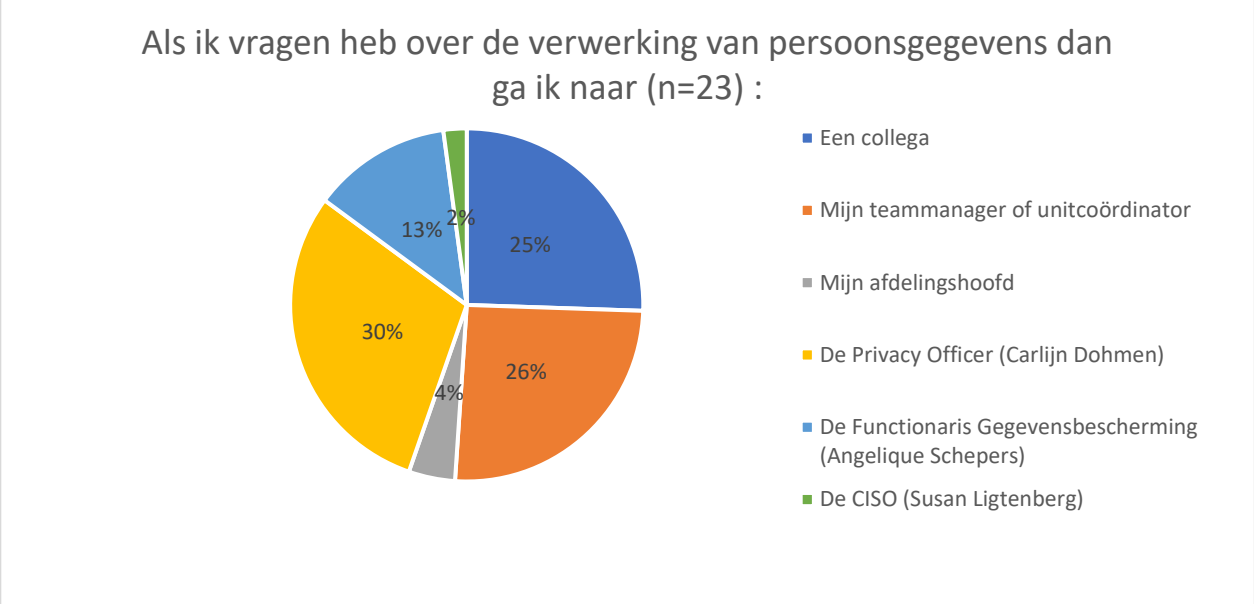
[59] Handreiking Positionering en taken van de FG.
[60] Artikel 38 lid 3, Algemene verordening gegevensbescherming.
[61] Privacybeleid gemeente Zoetermeer, pp. 4-5.

FTE. In de gevoerde gesprekken kwam naar voren dat er relatief weinig tijd is voor de PO om meer beleidsmatige taken voor de middellange termijn op te pakken, en dat de PO vaak druk is met acute (operationele) vraagstukken vanuit de afdelingen.

Om te zorgen dat de PO zich meer kan richten op de strategische taken is de PO bezig met het versterken van het privacynetwerk met privacy-ambassadeurs, zo kwam in de gesprekken naar voren. Het privacynetwerk is inmiddels opgezet en heeft als voornaamste doel te fungeren als platform waarin de privacy-ambassadeurs elkaar op de hoogte houden van privacyvraagstukken en actuele ontwikkelingen. Door de privacy-ambassadeurs meer als eerste aanspreekpunt voor hun eigen afdeling te laten fungeren, hoeft de PO pas betrokken te worden bij afdelingsoverstijgende vraagstukken of wanneer er specifiek tweedelijns advies nodig is. Door deze doorontwikkeling van het privacynetwerk zou de PO kunnen worden ontlast. Binnen de gemeente wordt momenteel onderzocht of per afdeling één aanspreekpunt voor alle IPI-gerelateerde onderwerpen kan worden aangewezen. De doorontwikkeling van het privacynetwerk met privacy-ambassadeurs komt momenteel nog niet goed van de grond, zo blijkt uit de gevoerde gesprekken. Dit heeft onder andere te maken met de verschillende invulling die de privacy-ambassadeurs aan hun rol (willen) geven.

Medewerkers richten zich bij vragen tot de PO, teammanager of een collega

In de gevoerde gesprekken kwam naar voren dat de PO een belangrijk eerste aanspreekpunt is voor de organisatie en dat de drempel voor medewerkers richting de PO laag is. Hoewel het fijn is voor de organisatie om een goed aanspreekpunt te hebben voor vragen, staat dit gegeven niet in lijn met het 3LoD-model en de ambitie van de PO om meer tijd te besteden aan beleidsmatige taken. De onder de medewerkers van de drie eerder genoemde domeinen uitgezette enquête laat ook zien dat medewerkers hun vragen relatief vaak stellen aan de PO, de teammanager/unitcoördinator of een directe collega. Daarbij moet opgemerkt worden de privacy-ambassadeurs nog niet in deze vragenlijst als optie zijn meegenomen. Het is daardoor niet duidelijk welke deel van de categorie 'collega' gericht is aan de privacy-ambassadeurs. Opvallend is ook dat medewerkers zich relatief vaak tot de FG richten met vragen.



Figuur 3: Resultaten enquête onder medewerkers: vragen over verwerking van persoonsgegevens.

Zoals benoemd zijn afdelingshoofden volgens het beleidskader verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens binnen hun afdeling. Blijkens de enquête en de gevoerde gesprekken gaan medewerkers in het geval van vragen meestal naar de PO, een collega of de teammanager of unitcoördinator. In zowel de gesprekken als de enquête komt naar voren dat de PO relatief vaak (in 30 procent van de gevallen) het eerste aanspreekpunt vormt. Hierdoor is de PO veel tijd kwijt aan het beantwoorden van vragen van medewerkers en blijft er minder tijd over voor een structurele aanpak van privacybescherming.

3.3.2. Integrale samenwerking tussen informatiebeveiliging, privacy en informatiebeheer

De gemeente kent een hechte samenwerking in het team IPI

Na het doorlopen van het implementatiestappenplan voor de AVG in 2018 heeft de gemeente Zoetermeer niet stilgezeten. Vanaf 2021 is de organisatie begonnen met een meer integrale samenwerking tussen de vakgebieden Informatiebeveiliging, Privacy en Informatiebeheer (hierna: IPI).[62] Waar medewerkers informatiebeveiliging en privacy al een langere samenwerking kennen, is ook informatiebeheer sinds het najaar van 2020 betrokken in deze samenwerking. De aanleiding voor deze samenwerking lag in de uitdaging met het gemeentelijke werkbedrijf De Binnenbaan. Bij de uitdaging van de gegevensuitwisseling met het werkbedrijf De Binnenbaan hebben de drie vakgebieden nauw samengewerkt. Uit de gesprekken komt naar voren dat de PO, de senior adviseurs informatiebeveiliging, de adviseurs informatiebeheer en de CISO regelmatig met elkaar en met de gemeentearchivaris overleggen.

De IPI-samenwerking wordt blijkens de gevoerde gesprekken doorgezet door onder meer het gezamenlijk opzetten van trainingen en maandelijkse workshops voor medewerkers, het inrichten van de

[62] Jaarverslag gemeente Zoetermeer 2021, pp. 163-165.

online learning zaakgericht werken en het zorg dragen voor de DPIA's. Uit de gesprekken komt naar voren dat IPI als onderwerp ook een vast onderdeel is geworden van de beoordelings- en voortgangsgesprekken ('Op-koers-gesprekken') met medewerkers. Medewerkers worden daardoor getoetst op hun functioneren vanuit de samenhang van de drie vakgebieden. Daarnaast is IPI een vast onderdeel geworden van de collegevoorstellen, door een vaste paragraaf voor IPI op te nemen in de sjablonen die medewerkers kunnen gebruiken bij het opstellen van voorstellen.[63]

IPI moet nog verder geworteld worden in de afdelingen

Hoewel er intensief wordt samengewerkt tussen de vakgebieden van IPI, is er blijkens de gesprekken behoefte aan het sterker onderbrengen van IPI binnen de afdelingen. Lopende dit onderzoek werkt de PO aan het doorontwikkelen van een netwerk met aanspreekpunten voor privacy per afdeling (dit voornemen komt in het beleid terug onder de noemer privacy-ambassadeurs). Overwogen wordt of deze functionarissen ook het aanspreekpunt zouden kunnen zijn voor de vakgebieden informatiebeveiliging en -beheer. Op die manier zou er per afdeling één aanspreekpunt zijn voor IPI. Dit vergt wel uitbreiding van capaciteit of het herschikken van taken.

Op het intranet van de gemeente Zoetermeer (Zoetermeer Enzo) is een pagina ingericht waarin een toelichting wordt gegeven op het team IPI. Hierbij wordt aangegeven dat samenwerking tussen de vakgebieden informatiebeveiliging, privacy en informatiebeheer ertoe moet leiden dat de organisatie sneller en beter kan worden ondersteund. Op de IPI-pagina zijn ook links opgenomen naar de relevante beleidskaders en functionarissen die kunnen worden benaderd. Daarnaast wordt een korte toelichting gegeven op het 3LoD-model. Dit komt overeen met het model zoals weergegeven in figuur 2.

3.4. Kennisborging in de organisatie

3.4.1. Kennisniveau onder medewerkers

Toelichting op de enquête onder medewerkers

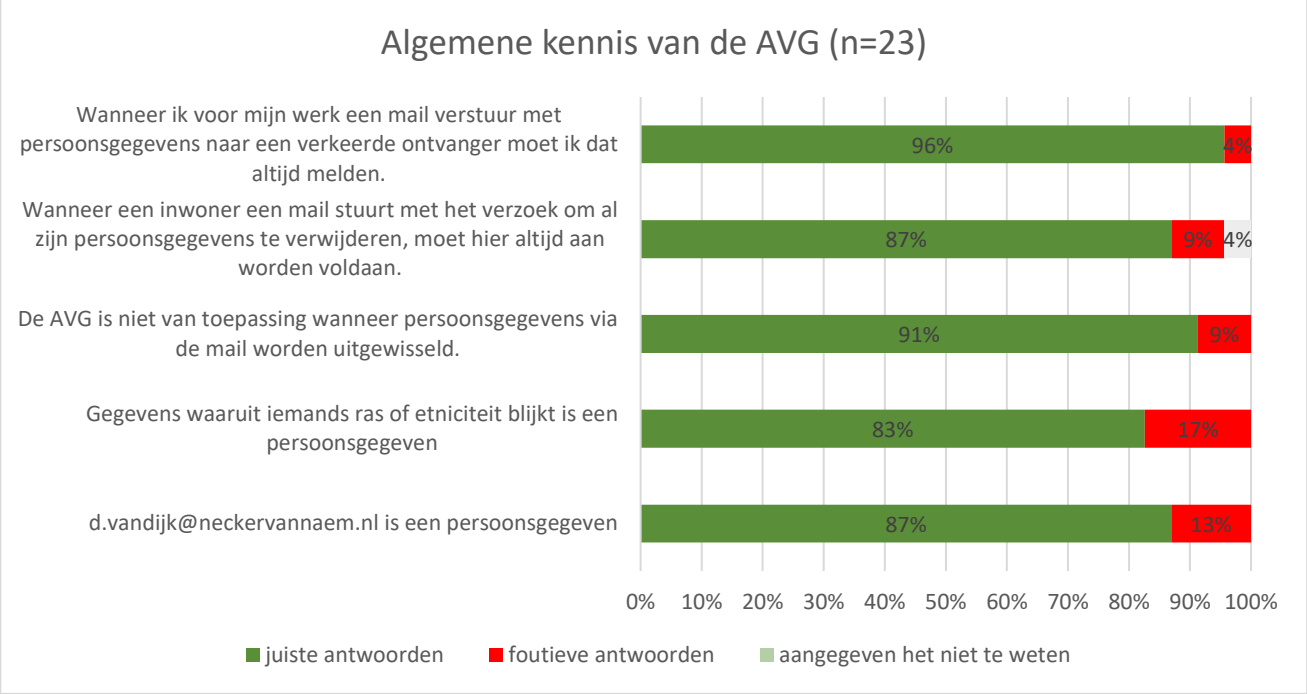
Er is een digitale enquête uitgezet om een beeld te krijgen van het kennisniveau van de AVG onder medewerkers en de mate waarin medewerkers ondersteuning vanuit de organisatie ervaren in het werken met de AVG. De enquête is op 20 mei 2022 uitgezet onder 36 medewerkers uit het sociaal domein, het publieksplein en veiligheidsdomein. Op 31 mei 2022 hebben de medewerkers een reminder ontvangen voor het invullen van de enquête. Daarnaast is er intern in de gemeentelijke organisatie een herinnering verzonden aan medewerkers om de enquête in te vullen. De lijst met gestelde vragen is opgenomen in de bijlage.

Dit heeft geleid tot 23 volledig ingevulde vragenlijsten. Daarvan zijn er 5 afkomstig van medewerkers uit het sociaal domein, 8 uit het veiligheidsdomein, 7 van het publieksplein en 3 medewerkers hebben aangegeven op geen van de drie afdelingen te werken. Zoals al bij de inleiding van dit hoofdstuk aangegeven, geeft dit een indicatie van de stand van zaken in de organisatie. Daarom worden de resultaten uit de enquête naast bevindingen uit de documentatie en interviews gepresenteerd.

Het niveau van algemene kennis van de AVG onder medewerkers lijkt op orde

[63] Jaarverslag gemeente Zoetermeer 2021, pp. 163.

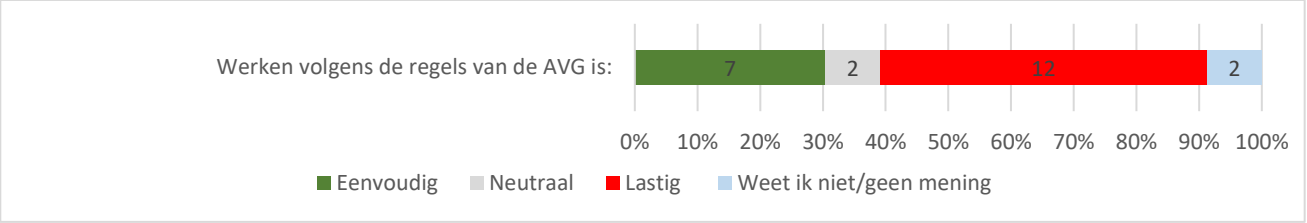
In de enquête die is uitgezet onder de medewerkers van het sociaal domein, het publieksplein en het veiligheidsdomein zijn vijf vragen gesteld die gaan over de algemene kennis van de AVG. Zo is er bijvoorbeeld gevraagd of een mailadres een persoonsgegeven is en of een medewerker melding moet maken van het versturen van persoonsgegevens naar een verkeerd mailadres. Bij elk van de vijf vragen was de beantwoording door de medewerkers voor meer dan 80 procent juist.



Figuur 4. Resultaten enquête onder medewerkers: vragen over algemene kennis van de AVG.

Werken volgens de regels van de AVG is een uitdaging voor medewerkers

Hoewel de kennis van medewerkers ten aanzien van de AVG op orde lijkt te zijn, laten de resultaten van de enquête zien dat het werken volgens de regels van de AVG voor een relatief groot deel van de medewerkers een uitdaging blijft. Van de 23 respondenten geeft ongeveer de helft (12) aan het werken volgens de regels van de AVG te ervaren als '*lastig*' tot '*zeer lastig*'. In paragraaf 3.7 wordt verder ingegaan op de ervaringen van medewerkers uit de drie onderzochte domeinen.

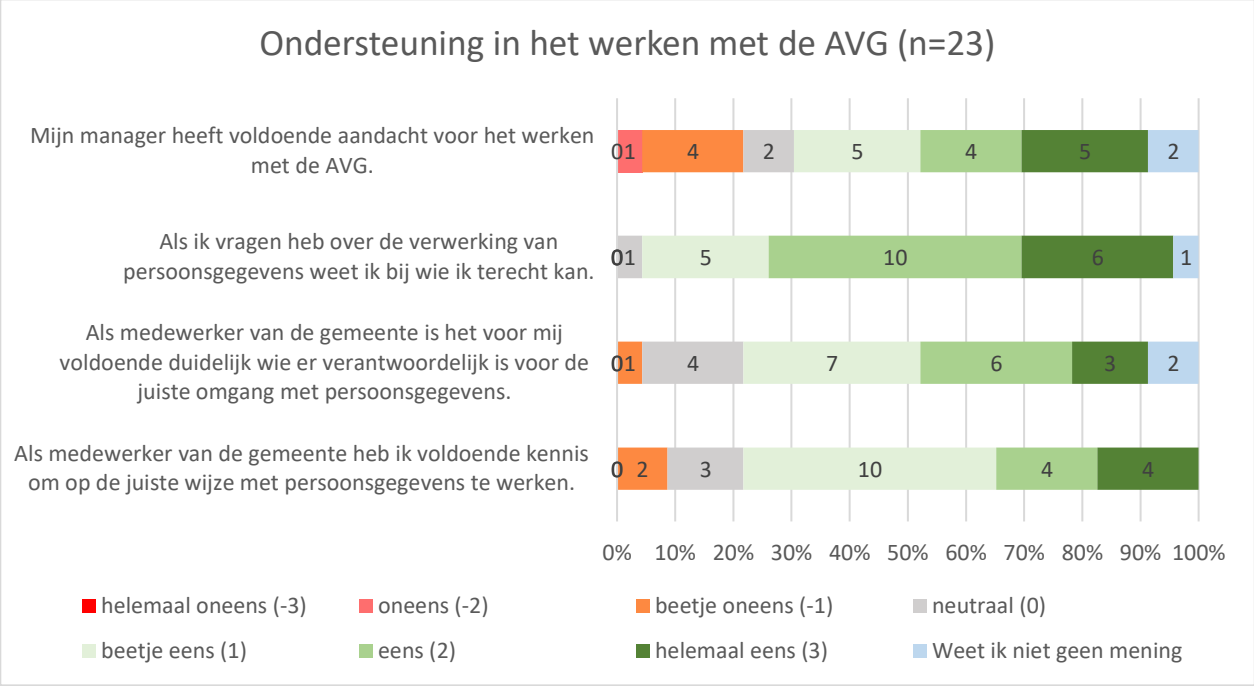


Figuur 5. Resultaten enquête onder medewerkers: vraag over werken volgens de regels van de AVG.

3.4.2. Ondersteuning van medewerkers

Medewerkers hebben grotendeels positieve ervaringen met ondersteuning

De resultaten van de enquête bieden ook inzicht in de ervaringen van medewerkers ten aanzien van ondersteuning. Het grootste deel van de respondenten (18) geeft aan dat zij voldoende kennis hebben om op de juiste wijze met persoonsgegevens te werken. Datzelfde geldt voor kennis over wie verantwoordelijk is voor de juiste omgang met persoonsgegevens (16). Vrijwel alle respondenten (twee uitgezonderd) geven aan in meer of mindere mate te weten bij wie zij terecht kunnen bij vragen over de verwerking van persoonsgegevens. Bij al deze resultaten moet wel de kanttekening worden gemaakt dat veel respondenten kiezen voor de optie 'beetje eens', in plaats van voor 'eens' of 'helemaal eens.'

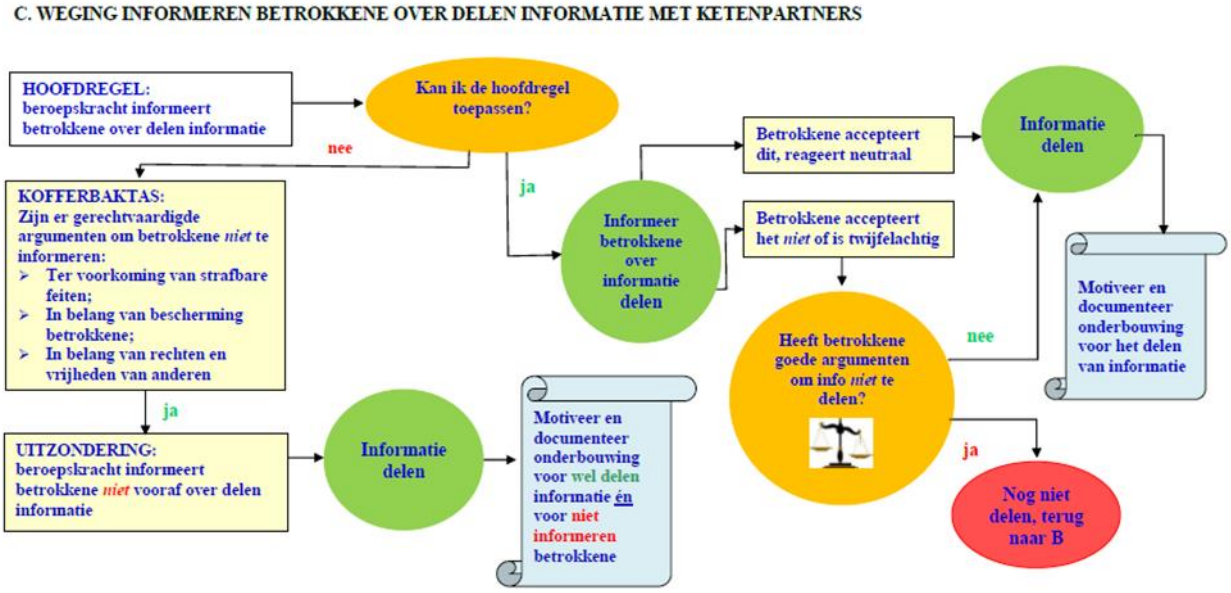


Figuur 6. Resultaten enquête onder medewerkers: vragen over ondersteuning in het werken met de AVG.

Zoals eerder benoemd zijn de afdelingshoofden in de eerste lijn verantwoordelijk voor het toezien op het werken met de AVG. De enquête lijkt een knelpunt aan te geven in de aandacht van managers voor het werken met de AVG. Vijf respondenten zijn het oneens met de stelling dat hun manager voldoende aandacht heeft voor het werken met de AVG. Uit de gesprekken komt ook naar voren dat de managers in de praktijk in wisselende mate de ruimte hebben om structureel aandacht te schenken aan de AVG-taken.

Er zijn voor medewerkers uitgebreide handreikingen en protocollen beschikbaar

De gemeente Zoetermeer kent een groot aantal handreikingen, protocollen en instructies die medewerkers bij het verwerken van gegevens kunnen raadplegen[64]. Er zijn zowel overkoepelende documenten die voor de gehele organisatie zijn opgesteld: zo is er een stroomschema opgesteld wat medewerkers kunnen hanteren bij het afwegen of en in hoeverre gegevens worden gebruikt en verstrekt aan derden. In deze handreiking wordt schematisch weergegeven welk stappenplan medewerkers moeten doorlopen om conform de AVG informatie te delen met ketenpartners, en in hoeverre betrokken personen van wie gegevens worden gedeeld hierover moeten worden geïnformeerd:[65]



Figuur 7: Stroomschema voor het informeren van betrokken personen over het delen van persoonsgegevens.[66]

Ook zijn er, zoals eerder benoemd, protocollen beschikbaar voor het uitvoeren van DPIA's. Daarnaast kent de gemeente verschillende werkinstructies en protocollen die voor een specifiek domein of een specifieke afdeling zijn opgesteld. Op deze laatste categorie wordt ingegaan in paragraaf 3.7.

Medewerkers worden gefaciliteerd middels workshops en trainingen

Naast de ondersteuning door onder meer de PO en de verschillende handreikingen en protocollen, worden periodiek workshops en trainingen georganiseerd om medewerkers te ondersteunen. Het doel van deze workshops of trainingen is tweeledig: het borgen van structurele kennis over de AVG en de implementatie hiervan in de organisatie, en het faciliteren van een plek waar medewerkers vragen kunnen stellen en met elkaar sparren over de praktijkinvulling van de AVG-richtlijnen. Het faciliteren van dergelijke workshops is in lijn met de BIO-norm om bewustzijn, opleiding en training over informatiebeveiliging te organiseren.[67]

[64] Een overzicht van de instructies en protocollen die in het kader van dit onderzoek ontvangen zijn, is opgenomen in bijlage 5.
[65] Gemeente Zoetermeer (g.d.). Stroomschema delen informatie met derden.
[66] Gemeente Zoetermeer (g.d.). Stroomschema delen informatie met derden.
[67] Baseline Informatiebeveiliging Overheid, norm 7.2.2.

In het kader van de implementatie van de AVG in de periode 2016-2018 is onder meer een bewustwordingsactie voor medewerkers georganiseerd, evenals verschillende workshops. Blijkens de gesprekken wordt er iedere maand een workshop informatiebeveiliging en privacy georganiseerd voor nieuwe medewerkers. Deze workshop wordt gegeven door de PO en een senior adviseur informatiebeveiliging. Daarnaast is er volgens de gesprekken een online e-learning zaakgericht werken beschikbaar op intranet. Deze e-learning gaat onder meer in op het werken met het gemeentelijk zaaksysteem volgens de AVG.

In paragraaf 3.7 wordt verder ingegaan op de leertuinen privacy in het sociaal domein.

3.4.3. Datalekken

De verwerkingsverantwoordelijke moet een datalek melden

Zoals beschreven is in hoofdstuk 1 stelt de AVG het melden van datalekken verplicht, tenzij het onwaarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.[68] De betekent dat de verwerkingsverantwoordelijke in het geval een datalek een inschatting moet maken van de effecten. De Guideline meldplicht datalekken geeft de criteria voor de beoordeling van de ernst van een datalek.[69] Daarnaast heeft de Autoriteit Persoonsgegevens een stappenplan gegeven voor de stappen die gezet moeten worden in het geval van een datalek.[70]

Het grootste deel van de datalekken ontstaat door onjuiste adressering

De PO van de gemeente Zoetermeer maakt ieder jaar een overzicht van alle datalekken.[71] Op basis daarvan kan worden geconstateerd dat er in de gemeente Zoetermeer in de jaren 2020 en 2021 in totaal 68 intern gemelde datalekken zijn geweest. 57 procent van deze datalekken is ontstaan door het versturen van gegevens naar een verkeerde ontvanger.[72] In 14 van de 68 gevallen is er naast een interne melding ook een melding bij de Autoriteit Persoonsgegevens gedaan. In de rapportage over de datalekken van 2020 en 2021 maakt de gemeente de aantekening dat er mogelijk meer datalekken in de gemeentelijke organisatie zijn maar dat medewerkers geen melding maken van deze datalekken of het lek niet als dusdanig herkennen.[73] Door middel van informatievoorziening via intranet en handreikingen wordt getracht dit zo veel mogelijk te voorkomen.[74]

Wanneer er sprake is van een datalek bij de gemeente is het interne proces datalekken van toepassing.[75] Het door de gemeente opgestelde stappenplan in het geval van een datalek is uitvoerig en komt overeen met het stappenplan van de Autoriteit Persoonsgegevens. Medewerkers die een datalek willen melden kunnen dat doen via drie wegen: in Topdesk, via datalekken@zoetermeer.nl of via een lid van het datalekkenteam (de PO, adviseurs inormatiebeveiliging, FG en CISO). Na melding vindt er een beoordeling van het risico plaats en beoordeelt de PO of er melding moet worden gemaakt bij de Autoriteit Persoonsgegevens.

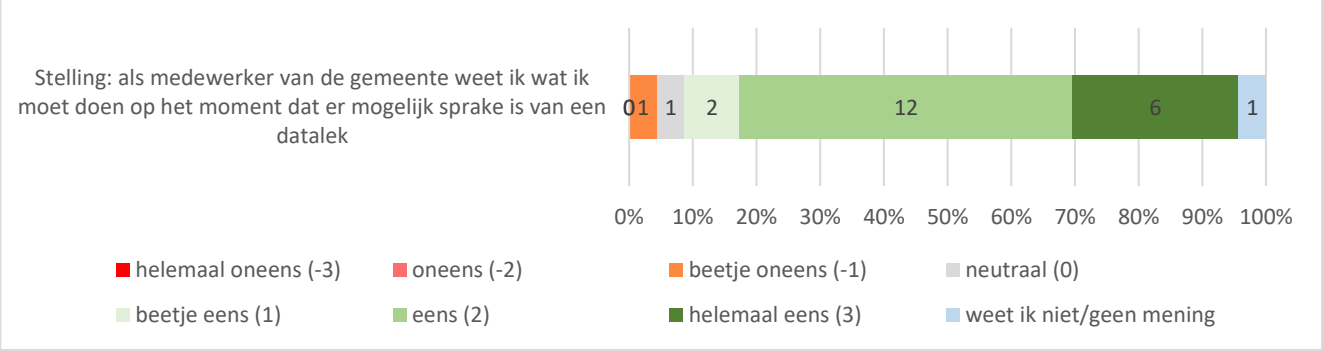
---

[68] Artikel 33 Algemene verordening gegevensbescherming.
[69] Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679.
[70] Stappenplan: kom in actie bij een datalek.
[71] Datalekken Gemeente Zoetermeer in 2020 (infographic); Datalekken Gemeente Zoetermeer in 2021 (infographic).
[72] Datalekken 2020 en 2021.
[73] Datalekken 2020 en 2021.
[74] Beschrijving proces datalekken.
[75] Beschrijving proces datalekken.

De beoordeling van de vraag of datalekken ook gemeld moeten worden aan de Autoriteit Persoonsgegevens is in de gemeente Zoetermeer neergelegd bij de PO. In het geval van datalekken die een grote publieke impact hebben of politiek gevoelig zijn moeten ook de gemeenteraad en het college geïnformeerd worden. In de praktijk wordt hier ook de FG bij betrokken, zo blijkt uit de gevoerde gesprekken. Voor het melden van datalekken aan het college en de raad zijn de afdelingen verantwoordelijk. In gesprekken werd aangegeven dat het voor medewerkers niet altijd eenvoudig is om in te schatten in hoeverre een datalek politiek gevoelig is of al dan niet een grote publieke impact heeft. Daarom stemt de FG hierover af met de betrokken bestuurder.

Medewerkers geven aan dat het duidelijk is wat ze moeten doen in het geval van een datalek

Het grootste deel van de respondenten van de enquête (20) geeft aan te weten wat ze moeten doen in het geval van een datalek. Dit gegeven kan op verschillende manieren worden geduid. Het feit dat medewerkers weten wat ze moeten doen kan enerzijds komen door kennis van het protocol, maar dat kan anderzijds ook komen door een meervoudige ervaring met datalekken. In paragraaf 3.7 wordt verder ingegaan op het melden van datalekken binnen de drie onderzochte domeinen.



Figuur 8. Resultaten enquête onder medewerkers: vragen over handelingen bij een datalek.

De Basisregistratie Personen kent een eigen procedure voor onjuiste gegevensverstrekkingen en incidenten

De regels en richtlijnen uit de AVG gelden ook voor het werken met de Basisregistratie Personen (BRP) in de gemeente. Het publieksplein, waar de BRP in beheer is, heeft een eigen procedure voor misstanden. Op het moment dat er sprake van onjuist verstrekte gegevens uit de basisregistratie dan moet er melding gemaakt worden bij een BRP-specialist, de functioneel beheerder BRP of de manager publieksplein. Via de beoordeling van de consequenties wordt in overleg met de melder afgewogen hoe er wordt omgegaan met de misstand. Onderdeel van deze afweging is de vraag of het nodig is om melding te maken van een datalek. Over de incidenten met betrekking tot de BRP wordt jaarlijks gerapporteerd aan het managementteam Publieksplein.[76]

3.4.4. Verwerking van persoonsgegevens

De gemeente houdt actief verwerkingsregisters bij

[76] Gemeente Zoetermeer (2021). Procedure incidentenmelding BRP; ibid. (2021). Procedure onjuiste verstrekkingen

Op basis van de AVG is de gemeente verplicht om verwerkingsregisters bij te houden van alle persoonsgegevens die zij verwerkt. Hierin moeten de volgende onderdelen zijn opgenomen:

- De naam en contactgegevens van: de gemeente of de vertegenwoordiger van de gemeente; eventuele andere organisaties met wie gezamenlijke doelen en middelen van de verwerking zijn vastgesteld; de FG en eventuele internationale organisaties waarmee persoonsgegevens worden gedeeld;
- De doelen waarvoor de persoonsgegevens worden verwerkt.
- Een beschrijving van de categorieën van personen van wie gegevens worden verwerkt, bijvoorbeeld uitkeringsgerechtigden, klanten of patiënten.
- Een beschrijving van de categorieën van persoonsgegevens, zoals het BSN, NAW-gegevens, telefoonnummers, camerabeelden of IP-adressen.
- Bewaartermijn: de datum waarop de gegevens moeten worden gewist (indien bekend).
- De categorieën van ontvangers aan wie persoonsgegevens worden verstrekt.
- Een algemene beschrijving van de technische en organisatorische maatregelen die zijn genomen om de persoonsgegevens die worden verwerkt te beveiligen.[77]

Voor dit onderzoek hebben de onderzoekers de verwerkingsregisters in kunnen zien van het sociaal domein, het publieksplein en het veiligheidsdomein. Deze registers bevatten de categorieën aan informatie die de registers volgens de AVG zouden moeten bevatten.[78]

In het implementatieproces van de AVG in de gemeente Zoetermeer hebben zich blijkens de gesprekken verschillende knelpunten voorgedaan met betrekking tot de verwerkingsregisters. Iedere afdeling binnen de gemeente is verantwoordelijk voor het opstellen van een eigen register. In de praktijk werden de registers niet altijd tijdig voorzien van de correcte informatie, of waren de registers onvolledig. Doordat de verantwoordelijkheid voor het invullen van de verwerkingsregisters relatief laag in de organisatie ligt, kan het voorkomen dat informatie niet klopt, niet volledig is of niet actueel is. Uit de gesprekken kwam het voorbeeld naar voren dat het handhavingsproces van de boa's niet is verwerkt in het verwerkingsregister van het veiligheidsdomein.

Momenteel worden de verwerkingsregisters volgens gesprekspartners voornamelijk gebruikt voor registratie, en minder voor het in beeld brengen van mogelijke risico's van verwerking op de lange termijn. Binnen de afdeling informatiebeheer wordt lopende dit onderzoek overwogen om een I-navigator in te zetten die hier zorg voor zou kunnen dragen.

De gemeente kent geen actueel overzicht van verwerkersovereenkomsten

Om te zorgen voor een juiste verwerking van persoonsgegevens is het nodig om verwerkersovereenkomsten te sluiten tussen de verwerkingsverantwoordelijke en de verwerker. Hierin is de gemeente meestal de verwerkingsverantwoordelijke. In de praktijk verwerkt de gemeente de verwerkersovereenkomsten in de hoofdovereenkomst die de gemeente sluit met een externe partij.

[77] Autoriteit Persoonsgegevens (2022). Verantwoordingsplicht, vereisten voor verwerkingsregisters: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht#wat-moet-er-in-het-verwerkingsregister-staan-7193.
[78] Gemeente Zoetermeer: verwerkingsregisters publieksplein, sociaal domein en veiligheid, vergunningen en handhaving.

Voor het opstellen van aparte verwerkersovereenkomsten is een VNG-model aanwezig dat medewerkers als basis kunnen hanteren.[79]

Een actueel overzicht van alle verwerkersovereenkomsten die de gemeente heeft gesloten is blijkens de gesprekken niet aanwezig, mede doordat afspraken over verwerking van gegevens met derden vaak niet zijn opgenomen in een aparte overeenkomst. Volgens het privacybeleid dient de FG toe te zien op de naleving van verwerkersovereenkomsten en moet in het verwerkingsregister worden bijgehouden welke verwerkersovereenkomsten er zijn gesloten. Momenteel voldoet de gemeente Zoetermeer dus niet aan deze richtlijn in het gemeentelijk kader.[80]

Privacy by design of privacy by default?

In het privacybeleid vormen privacy by design en default uitgangspunten voor de gemeente in de uitvoering en naleving van de AVG. Deze principes zijn onderdeel van de ontwikkeling van nieuwe diensten of de inkoop nieuwe software. In de gesprekken werd aangegeven dat privacy en informatiebeheer een vaste plaats hebben in het proces van ontwikkeling of aankoop van nieuwe software. In de praktijk worden privacy en informatiebeheer hierbij echter niet altijd betrokken, zo blijkt uit de gevoerde interviews. In aanbestedingstrajecten zijn de betreffende afdelingen wel altijd betrokken. Daarnaast werd aangegeven dat het niet altijd eenvoudig is om de juiste technische kennis in huis te halen om deze twee uitgangspunten in de praktijk te brengen.

3.5. Archieffunctie binnen de gemeente

De gemeentearchivaris ziet toe op het informatiebeheer

De gemeentearchivaris heeft binnen de gemeente een toezichthoudende rol op het archief- en informatiebeheer door de organisatie. Op basis van de gemeentelijke Archiefverordening 2020 legt de gemeentearchivaris ieder jaar verantwoording af aan het college aan de hand van een KPI-verslag. Het KPI-verslag van het jaar 2020 was beschikbaar. De gemeentearchivaris werkt lopende dit onderzoek nog aan het KPI-verslag over 2021. Hieronder wordt ingegaan op enkele relevante bevindingen van de gemeentearchivaris en bevindingen van de onderzoekers ten aanzien van het gemeentelijk informatiebeheer.

De lokale regelingen zijn actueel

Doordat de gemeentearchivaris in een eerder stadium constateerde dat de Archiefverordening en het Besluit Informatiebeheer verouderd waren, zijn deze documenten in 2020 beide vervangen en opnieuw vastgesteld. Daarnaast is er in 2020 gewerkt aan het vastleggen van de verantwoordelijkheden op het gebied van archief- en informatiebeheer van het nieuwe gemeentelijk werkbedrijf De Binnenbaan. Die verantwoordelijkheden zijn vastgelegd in een dienstverleningsovereenkomst.[81]

De gemeentearchivaris vraagt om aandacht voor de archieffunctie

[79] Gemeente Zoetermeer (geen datering). Model verwerkersovereenkomst.
[80] Gemeente Zoetermeer (2021). Privacybeleid, p. 5.
[81] Ambtelijke stuurgroep Zoetermeer – Binnenbaan (2021). Memo Eindadvies verzelfstandiging informatievoorziening Binnenbaan.

Uit de voor dit onderzoek gevoerde gesprekken komt naar voren dat er binnen de gemeentelijke organisatie nog onvoldoende zicht is op waar informatie is opgeslagen. Er staat in digitale structuren op meerdere plekken informatie waarvan niet duidelijk is of het om het originele document gaat of om een kopie. Door dit gebrek aan overzicht is het niet mogelijk om de wettelijke bewaartermijnen na te leven en blijven er persoonsgegevens in de gemeentelijke archieven staan waarvan de bewaartermijn is verlopen. Er vindt namelijk nog nauwelijks vernietiging van digitale informatie plaats. Daarbij is het ook de vraag of wel alle informatie in het zaaksysteem terechtkomt.

Een verbetering in dit proces is het nieuwe zaaksysteem dat er sinds 1 januari 2022 is in de gemeente. In tegenstelling tot het oude zaaksysteem is er in dit systeem wel een mogelijkheid om gegevens te koppelen aan een bewaartermijn. De gemeente werkt echter ook met andere applicaties die geen beheermogelijkheden hebben als het gaat om de bewaartermijn. Het blijkt binnen de organisatie niet helemaal duidelijk te zijn welke applicaties over de juiste beheermogelijkheden beschikken. Bij de aankoop van nieuwe applicaties worden sinds 2021 informatiebeheer en privacy betrokken om te checken of de applicaties aan de eisen voldoen. Dit gebeurt echter nog niet altijd en soms pas achteraf.

De archieffunctie vraagt om nieuwe competenties

Het KPI- verslag van de gemeentearchivaris over 2020 beschrijft een gat tussen de gewenste- en de beschikbare kennis en competenties als het gaat om het team informatiebeheer. De laatste jaren heeft zich in de archieffunctie een ontwikkeling voorgedaan van papier naar digitaal. Deze ontwikkeling vraagt andere competenties van medewerkers. Het ordenen en sorteren van dozen met papieren archiefbescheiden is iets anders dan het beheren van digitale systemen en het uitvoeren van advieswerkzaamheden voor de organisatie. In 2016 is daarom ingezet op een strategische personeelsplanning om de juiste competenties aan boord te halen. In 2020 is de constatering echter dat medewerkers weliswaar een andere functie hebben gekregen maar in grote lijnen nog dezelfde werkzaamheden uitvoeren. Vanaf 2020 heeft de gemeente echt ingezet op de transitie naar nieuwe werkzaamheden die zich richten op digitaal informatiebeheer. Het advies van de gemeentearchivaris luidt desondanks dat het nodig is om structureel extra middelen beschikbaar te stellen voor het team en de komende jaren externe medewerkers in te huren met het vereiste niveau.[82] De gemeente is blijkens gesprekken momenteel bezig met het werven van nieuwe medewerkers die hieraan voldoen.

3.6. Verantwoording en rapportages

Verantwoording aan de gemeenteraad neemt toe maar is op hoofdlijnen

De verantwoording richting de gemeenteraad ten aanzien van gegevensbescherming verloopt via de P&C-cyclus. In het jaarverslag legt het gemeentebestuur verantwoording af over het gevoerde privacybeleid, stelt de raad op de hoogte van ontwikkelingen en maakt melding van eventuele bijzonderheden zoals een inbreuk of het verlies van persoonsgegevens en bij incidenten. In de jaarverslagen van 2018 tot en met 2021[83] is te zien dat er een steeds uitgebreidere behandeling op het onderwerp privacy is. Het jaarverslag 2021 bevat een uitgebreide toelichting op de onderwerpen informatiebeveiliging, privacy en informatievoorziening. Daarnaast wordt er onder meer ingegaan op de

[82] KPI-verslag 2020, p.9.
[83] Gemeente Zoetermeer (2018-2021). Jaarverslagen periode 2018-2021.

ENSIA-rapportages, de privacyleertuinen en de hoeveelheid datalekken (inclusief het aantal datalekken dat gemeld is bij de Autoriteit Persoonsgegevens) per jaar.[84]

Zoals eerder benoemd, is de gemeenteraad in de periode 2016 - 2018 periodiek geïnformeerd over de voortgang van de implementatie van de AVG door de organisatie. Uit de ontvangen documenten blijkt niet dat deze vorm van informatievoorziening sinds 2018 is voortgezet.

De FG stelt geen rapportages op over gegevensbescherming

In veel Nederlandse gemeenten speelt de FG een belangrijke rol in de verantwoording en rapportage over gegevensbescherming. De Autoriteit Persoonsgegevens geeft aan dat intern toezicht houden op gegevensbescherming een belangrijke taak is van de FG. De FG kan hieraan invulling geven door informatie te verzamelen over gegevensverwerking binnen de organisatie, dit te analyseren en te toetsen aan de wettelijke vereisten, en hierover ''informatie, adviezen en aanbevelingen [te] geven.''[85]

Binnen de gemeente Zoetermeer brengt de FG geen schriftelijke rapportage uit aan de gemeentesecretaris of het college. Wel is er een paragraaf in het jaarverslag opgenomen. Ook vindt er tweemaal per jaar een toelichting plaats in het directieteam in de vorm van een presentatie door het IPI-team (de FG, de CISO, de PO en de gemeentearchivaris). Tijdens deze toelichting worden de belangrijkste bevindingen op het gebied van gegevensbescherming gedeeld en waar mogelijk vertaald naar doelstellingen voor het komende halfjaar.[86] Uit de interviews komt naar voren dat op basis van de bevindingen van onder meer de FG, de paragraaf informatiebeveiliging, privacy en informatiebeheer (IPI) sinds begin 2022 als standaard onderwerp is opgenomen in de collegevoorstellen.

Jaarlijks wordt verantwoording afgelegd in de ENSIA-rapportages

In paragraaf 2.3 is al een toelichting gegeven op de ENSIA-systematiek. Jaarlijks wordt de ENSIA-rapportage opgeleverd voor de audit van DigiD en SUWInet (digitale infrastructuur die overheden hanteren voor het uitwisselen van gegevens). In de collegeverklaring ENSIA geeft het college jaarlijks aan dat bij de gemeente de beheersingsmaatregelen voor het voorgaande jaar voldoen aan de geselecteerde normen voor DigiD en SUWInet. Ook wordt, indien van toepassing, in de collegeverklaring aangegeven welke onderdelen van de uitvoering niet aan de normen voldoen en welke eventuele verbetermaatregelen de gemeente gaat treffen. De collegeverklaring wordt jaarlijks getoetst door een auditor die verifieert of de door de gemeente gesignaleerde bevindingen uit de ENSIA-rapportage ook een vervolg krijgen door een verbeterplan met actiepunten. Die moeten vervolgens expliciet zijn belegd in en gemonitord door de organisatie.[87]

Vooraf aan risicovolle verwerkingen wordt een DPIA uitgevoerd

Eén van de verplichte handelingen die uit de AVG voortkomen is het uitvoeren van zogeheten DPIA's[88] voorafgaand aan risicovolle verwerkingsactiviteiten. Door het uitvoeren van een DPIA wordt beoordeeld wat de mogelijke effecten van een verwerking zijn op de bescherming van persoonsgegevens. Het

[84] Gemeente Zoetermeer (2022). Jaarstukken 2021, pp. 164-165.
[85] Autoriteit Persoonsgegevens: Functionaris Gegevensbescherming (FG): https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg#:~:text=Overheden%20en%20publieke%20organisaties,om%20bijvoorbeeld%20zorg%2D%20en%20onderwijsinstellingen.
[86] Gemeente Zoetermeer (2021). Presentatie DT voortgang IPI, d.d. 4 oktober 2021.
[87] Gemeente Zoetermeer (2021). Verslag auditor assurance ENSIA 2021.
[88] DPIA staat voor Dataprotection impact assessment.

uitvoeren van DPIA's is als vaste stap opgenomen in het stappenplan voor de implementatie van de AVG, dat door de PO is opgesteld.

Voor medewerkers is er een (via intranet beschikbaar) document opgesteld waarin wordt toegelicht wanneer een DPIA moet worden uitgevoerd. Tevens is er een format voor een DPIA-rapportage beschikbaar, dat medewerkers kunnen gebruiken. In dit format zijn alle stappen opgenomen die moeten worden doorlopen bij het uitvoeren van een DPIA, met de verschillende afwegingen die hierbij in het kader van de AVG moeten worden gemaakt.[89] Uit de gevoerde interviews komt naar voren dat de PO de organisatie adviseert over de noodzaak van het uitvoeren van DPIA's, en waar nodig medewerkers bij het uitvoeren van een DPIA ondersteunt. Uit de interviews blijkt echter ook dat niet voor iedere medewerker duidelijk is wanneer een DPIA moet worden uitgevoerd.

3.7. Drie domeinen in beeld

3.7.1. Sociaal domein

Met de leertuinen privacy kregen medewerkers inzicht in de werking van de AVG

Om medewerkers te helpen meer (praktijk)kennis te vergaren heeft de gemeente Zoetermeer het initiatief genomen om zogeheten leertuinen privacy in het sociaal domein te organiseren. Deze leertuinen bestonden uit hoorcolleges en trainingen waarbij medewerkers wegwijs werden gemaakt in de richtlijnen van de AVG en de wijze waarop deze in het sociaal domein worden toegepast. In 2019 is het besluit genomen om te starten met de leertuinen privacy onder de begeleiding van het Innovatiecentrum Zorg en Veiligheid Coöperatie U.A.. De insteek van de leertuinen privacy was om de AVG niet als een belemmering te zien voor werkzaamheden maar juist als een manier om gegevensdeling mogelijk te maken voor een integrale aanpak.[90]

Als gevolg van het coronavirus heeft dit traject vertraging opgelopen. Daardoor konden de geplande hoorcolleges, trainingen en action learning sessies pas in 2021 van start gaan. Voorafgaand daaraan zijn de bestuurders, managers, unit-coördinatoren en andere relevante betrokkenen binnen het sociaal domein op de hoogte gesteld van de inhoud van de leertuinen en hun rol in het traject. Vervolgens hebben er in totaal 270 medewerkers van de gemeente en 16 medewerkers van werkbedrijf De Binnenbaan deelgenomen aan de bijeenkomsten. In de hoorcolleges hebben de medewerkers aan de hand van methoden en stroomschema's onder meer uitleg gekregen over wanneer het is toegestaan om gegevens te delen en of wanneer betrokkenen daarover geïnformeerd moeten worden. De beginselen en principes zoals een gerechtvaardigd doel, subsidiariteit, proportionaliteit en doelmatigheid kregen daarbij aandacht.[91]

Het traject van de leertuinen begon met de hoorcolleges en de training, op een later moment werden ook *action learning sessies* onderdeel van het traject. In deze sessies is met de medewerkers teruggekeken op hun ervaring met het werken volgens de geleerde methode. Dit werd mede gedaan aan de hand van dossiers die door FG steekproef waren geselecteerde. Op basis van deze sessies zijn er door

[89] Gemeente Zoetermeer (g.d.). Format voor DPIA; moet ik een DPIA uitvoeren?
[90] Memo stavaza leertuinen privacy, d.d. 24 maart 2022
[91] Stroomschema Leertuin.

het projectteam leertuinen privacy verschillende knelpunten geformuleerd voor het werken met de AVG in het sociaal domein:

- **Het hanteren van onnodige toestemmingsformulieren:** Binnen de organisatie waren er verschillende onnodige toestemmingsformulieren in gebruik. Het advies op basis van het traject van de leertuinen was om te stoppen met deze formulieren.
- **De onmogelijkheid om persoonlijke aantekening te maken in het zaaksysteem:** Het was in de systemen niet mogelijk voor medewerkers om persoonlijke werkaantekeningen te maken die buiten een inzageverzoek kunnen worden gehouden.
- **Ondersteuning van medewerkers:** niet alle medewerkers voelden zich voldoende gefaciliteerd in het werken met AVG.
- **De ketenpartners hebben andere werkwijzen:** Medewerkers van de gemeente gaven aan dat ketenpartners andere werkwijzen hanteerden en dat dit samenwerking in de keten bemoeilijkte.
- **Er is behoefte aan een bredere kring van medewerkers die kunnen ondersteunen:** Een van de knelpunten die naar voren kwam uit de leertuinen was dat de kring van medewerkers met kennis van de AVG en de mogelijkheid om ondersteuning te bieden niet groot genoeg is.
- **Het opstellen van een beleid voor gegevensuitwisseling:** Om zowel intern als extern duidelijk te maken op welke wijze de gemeente omgaat met gegevensuitwisseling is het wenselijk om een beleidskader op te stellen waarin duidelijk omgeschreven wat de visie van de gemeente is op gegevensdeling.
- **De medewerkers ervaren de leertuinen als vrijblijvend:** Ondanks dat het bijwonen van de bijeenkomsten verplicht was waren er regelmatig medewerkers die niet deelgenomen hebben aan de trainingen.[92]

De leertuinen hebben het beeld van medewerkers over de AVG veranderd

In de gehouden interviews gaven de gesprekspartners aan de leertuinen privacy als behulpzaam te hebben ervaren. Toen de AVG net in werking was getreden en werd geïmplementeerd in de organisatie leefde de gedachte binnen de organisatie dat het bijna niet meer mogelijk zou zijn om gegevens te delen. De initiatieven die binnen de gemeente zijn ondernomen om het kennisniveau omhoog te brengen en methoden aan te reiken voor de praktijk hebben dat beeld kunnen kantelen, zo gaven de gesprekspartners aan. In de enquête die is uitgezet onder medewerkers van het sociaal-, het veiligheidsdomein en het publieksplein, gaven de medewerkers uit het sociaal domein een positief antwoord op de vraag of de leertuinen privacy hebben geholpen bij het werken met de AVG. Een enkeling noemde de leertuinen zelfs een eyeopener.

Er bestaan nog knelpunten ten aanzien van het delen van gegevens

In de gevoerde gesprekken kwamen echter enkele van de aan de hand van het traject leertuinen geformuleerde knelpunten opnieuw naar voren. Zo gaven medewerkers aan nog aan te lopen tegen de andere werkwijzen die ketenpartners hanteren. Hierbij kwam vooral het voorbeeld van de gehanteerde toestemmingsformulieren naar voren. Waar de ketenpartners nog met deze formulieren werken is de gemeente gestopt deze te gebruiken. De gemeente hanteert inmiddels een nieuwe werkwijze voor informatiedeling in het sociaal domein, waarbij gewerkt wordt vanuit het principe van transparantie. Dit houdt in dat samen met de betrokken inwoner wordt bepaald welk doel de hulp- of dienstverlening

[92] Memo stavaza leertuinen privacy, d.d. 24 maart 2022

heeft, en welke informatieverwerking hierbij nodig is. De betrokken inwoner wordt hier mondeling of schriftelijk over geïnformeerd, en wordt niet gevraagd om een toestemmingsformulier te tekenen.[93] Dit is soms lastig voor medewerkers in de samenwerking met externe partijen, omdat voor medewerkers niet duidelijk is hoe ze met deze discrepantie van werkwijzen moeten omgaan. Ook kwam het eerdergenoemde knelpunt over de onmogelijkheid om persoonlijke aantekening te maken in het zaaksysteem terug. De noodzaak tot eenduidig beleid over gegevensuitwisseling werd ook opnieuw genoemd. De medewerkers gaven aan dat het soms ontbreekt aan duidelijkheid als het gaat om het delen van gegevens en dat het gevolg daarvan is dat medewerkers besluiten om vooral geen gegevens te delen. Dit levert soms moeilijk werkbare situaties op.

Er vinden verschillende periodieke controles plaats

Uit de gesprekken komt naar voren dat er binnen het sociaal domein veel (periodieke) controles plaatsvinden om te toetsen of aan de AVG wordt voldaan. In het kader van de implementatie van de AVG zijn verschillende DPIA-controles uitgevoerd. Medewerkers geven aan dat het uitvoeren van een DPIA een moeizaam proces is, ook al is duidelijk welke procedures hiervoor gehanteerd moeten worden. Nu de AVG inmiddels is geïmplementeerd worden er blijkens de gesprekken in ieder geval binnen de afdelingen Jeugd en Participatie regelmatig kwaliteitscontroles uitgevoerd. In de praktijk betekent dit dat van iedere medewerker een willekeurig dossier wordt doorgenomen dat hij of zij in behandeling heeft. Hierbij wordt gekeken of de juiste stappen zijn doorlopen conform de wettelijke en gemeentelijke regelgeving. Deze kwaliteitscontroles vinden ieder kwartaal plaats.

Ondersteuning medewerkers kan worden versterkt

Binnen het sociaal domein wordt volgens gesprekspartners een hoge werkdruk ervaren. Er is sprake van een hoog personeelsverloop, waardoor eenmaal opgedane AVG-kennis de organisatie relatief snel weer verlaat. Daarom is het te meer van belang dat nieuwe medewerkers vanaf de start worden meegenomen in het werken met de AVG en actief worden gewezen op de verplichting om binnen drie maanden de hiervoor beschikbare cursus te volgen. Dat gebeurt nu niet altijd. Gesprekspartners die al langer binnen het Sociaal Domein werkzaam zijn geven aan meer behoefte te hebben aan structurele kennis-updates, bijvoorbeeld via fysieke 'bijspijkermomenten' eens per zes maanden. Het actiever inzetten van privacyambassadeurs als aanjagers van kennis en bewustzijn over de AVG en/of uitbreiding van de capaciteit van de PO zou volgens medewerkers ook nadrukkelijk in een behoefte voorzien.

3.7.2. Publieksplein

Medewerkers publieksplein kunnen gebruikmaken van aparte werkinstructies

Medewerkers publieksplein werken veel met de Basisregistratie Persoonsgegevens (BRP). De Wet BRP schrijft voor dat de gemeente regelgeving (een verordening BRP) moet opstellen voor de verstrekking van gegevens aan gemeentelijke organen. Daarnaast dient de verstrekking aan derden in de verordening

[93] Het document Nieuwe werkwijze informatiedeling gemeente Zoetermeer (g.d.) benoemt dit als volgt: '' De nieuwe werkwijze voldoet volledig aan de eisen van de AVG, maar ziet er misschien iets anders uit dan u gewend bent. Dat komt doordat we binnen het sociaal domein niet kunnen werken vanuit 'toestemming'. Er is namelijk geen sprake van vrije toestemming in de zin van de AVG; als mensen geen toestemming geven voor het verwerken van hun persoonsgegevens dan kan dat gevolgen hebben voor de gewenste voorziening.''

geregeld te worden. Het college van burgemeester en wethouders is verantwoordelijk voor de uitvoering van de Wet BRP. Uit de gevoerde interviews komt naar voren dat bij de implementatie van de AVG aanvankelijk onduidelijk was hoe deze zich verhield tot het BRP. Volgens de Autoriteit Persoonsgegevens zijn aanvullende plichten over persoonsgegevens die niet in het BRP zijn opgenomen: het bijhouden van een register van verwerkingen, het melden van datalekken en het aanwijzen van een FG.[94]

Binnen de gemeente Zoetermeer zijn er verschillende werkinstructies, protocollen en procedures opgesteld om een goed verloop van de BRP-taken te kunnen waarborgen. Het gaat hier onder meer over het verwijderen van gegevens en het melden van incidenten als datalekken of onjuiste verstrekkingen. De gemeente kent verder een apart informatiebeveiligingsplan voor de BRP-taken met beleidsdoelstellingen en bijbehorende maatregelen die moeten worden uitgevoerd.[95]

Medewerkers zijn alert op de wettelijke verplichtingen

Medewerkers publieksplein hebben gegeven de aard van hun werk in de praktijk veel te maken met richtlijnen uit de AVG en de wet BRP. Uit de gevoerde interviews komt naar voren dat er bij de betrokken medewerkers daarom doorlopend aandacht is voor de bescherming van persoonsgegevens. Alle medewerkers die werken met de BRP tekenen jaarlijks een convenant voor inzage in de BRP, en nieuwe medewerkers worden actief voorgelicht over de verplichtingen die de relevante wet- en regelgeving met zich meebrengt. De aandacht voor het onderwerp wordt tevens gefaciliteerd door dit periodiek te bespreken in teamoverleggen en de voortgangsgesprekken met individuele medewerkers. Tijdens deze overleggen is het ook mogelijk om te sparren en dilemma's te delen.

Knelpunten in het zaaksysteem

Medewerkers ervaren als belangrijk knelpunt in hun werk dat het gebruikte zaaksysteem voor contact met inwoners nog niet geoptimaliseerd is in het kader van de AVG. Sinds de inwerkingtreding van de AVG zijn er wel stappen gezet om het zaaksysteem in lijn te brengen met regelgeving, maar er moet nog meer worden gedaan om bescherming van persoonsgegevens te optimaliseren. Dat heeft met name te maken met de inzage die medewerkers hebben in bepaalde zaakgegevens. Deze gegevens zijn momenteel niet altijd even goed beschermd, waardoor meer medewerkers deze kunnen inzien dan de bedoeling is. Lopende dit onderzoek wordt er in samenwerking met de FG onder andere gewerkt aan het wegnemen van knelpunten hierbij. Een aandachtspunt is het onderscheid tussen informatie die ''need to know'' is en informatie die ''nice to know'' is.

Medewerkers kunnen terecht bij de PO en FG voor vragen

Uit de interviews komt naar voren dat medewerkers publieksplein over het algemeen goed op de hoogte zijn van de richtlijnen uit de AVG. De vele werkinstructies, protocollen, periodieke workshops en de beschikbaarheid van online trainingen op intranet maken dat het informatieniveau bij medewerkers op peil blijft. Toch is ook aangegeven dat er regelmatig privacy kwesties 'op gevoel' in plaats van op basis

[94] Autoriteit Persoonsgegevens (2022). Basisregistratie Personen: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/overheid/basisregistratie-personen-brp#faq

[95] Gemeente Zoetermeer (2022). BRP-reglement; ibid. (2021). Informatiebeveiligingsplan BRP; ibid. (g.d.). Inzage en protocollering BRP; ibid. (2021). Procedure incidentenmelding BRP; ibid. (2021). Procedure onjuiste verstrekkingen; ibid. (2019). Privacy- en beheerregeling BRP.

van kennis worden opgelost. Wanneer er vragen zijn of er twijfel rijst, kunnen medewerkers conform het beleidskader in eerste instantie terecht bij de afdelingshoofden of teammanagers. Wanneer die het antwoord op een vraag niet weten, kan worden doorgeschakeld naar de PO of de FG. Vaak komt het echter voor dat medewerkers direct contact zoeken met de PO of de FG wanneer zij vragen hebben.

Er worden veel controles en checks uitgevoerd

Binnen het publieksplein worden veel checks en zelfevaluaties uitgevoerd ten aanzien van bescherming van persoonsgegevens. In het informatiebeveiligingsplan BRP is opgenomen welke zelfevaluatie en controles in het kader van de BRP jaarlijks moeten worden uitgevoerd. Daar hoort onder meer het controleren van de lijsten met persoonsgegevens door een kwaliteitsmedewerker bij. Daarnaast wordt jaarlijks een extra risicoanalyse uitgevoerd van de gebruikte systemen en applicaties. Uit die risicoanalyse volgt een score met bijbehorende aandachtspunten. Hieruit is onder meer het eerder behandelde knelpunt van inzichtelijkheid van gegevens naar voren gekomen.

Zoals in paragraaf 2.2.3. over datalekken toegelicht, werkt de BRP met een aparte procedure voor het melden van datalekken. Wanneer zich een datalek voordoet, wordt dit gemeld bij de teammanagers en de PO. De PO maakt de afweging of datalekken al dan niet gemeld moeten worden bij de Autoriteit Persoonsgegevens.

3.7.3. Veiligheidsdomein

In het veiligheidsdomein worden veel gegevens gedeeld

Binnen het veiligheidsdomein wordt veel gewerkt met persoonsgegevens. De gemeente Zoetermeer kent een scala aan samenwerkingspartners met wie persoonsgegevens worden gedeeld. Dat maakt het noodzakelijk om hierover met deze samenwerkingspartners afspraken te maken. De gemeente Zoetermeer heeft dan ook verschillende samenwerkingsovereenkomsten en convenanten gesloten met veiligheidspartners op zowel regionaal als lokaal niveau, onder andere met de politie, het Openbaar Ministerie (OM), het Landelijk en Regionaal Informatie en Expertise Centrum, het Zorg- en Veiligheidshuis Haaglanden en de Raad voor de Kinderbescherming.

In de verschillende convenanten met deze partners wordt verwezen naar de richtlijnen uit de AVG. Zo moet bij het delen van persoonsgegevens een duidelijke grondslag worden gemeld, waarbij er goed moet zijn afgewogen of verstrekking proportioneel is. Ook zijn er in de convenanten onder meer afspraken gemaakt over de verantwoordelijkheid voor en organisatie van gegevensverwerking, over het bewaren van gegevens en over de rechten van betrokkenen.[96] Uit de interviews komt naar voren dat het convenant voor het uitvoeringsoverleg Veiligheid en Zorg momenteel wordt geüpdatet omdat deze zijn gesloten voordat de AVG in werking trad.

Medewerkers uit het veiligheidsdomein geven aan dat partners van de gemeente goed op de hoogte zijn van de richtlijnen uit de AVG. In de praktijk worden richtlijnen soms wel verschillend geïnterpreteerd. De ene partner kent een stringentere interpretatie van de AVG dan de andere. Dat maakt het soms lastig

[96] Convenant aanpak georganiseerde criminaliteit, handhavingsknelpunten en integriteitsbeoorelingen (september 2014); Convenant aanpak drugscriminaliteit politie-eenheid Den Haag (27 mei 2020); Convenant uitvoeringsoverleg Veiligheid en Zorg Zoetermeer (18 januari 2017); Samenwerkingsconvenant ketenpartners Zorg- en Veiligheidshuis Haaglanden (g.d.).

om in de praktijk effectief te kunnen handelen. Over het algemeen wordt mondeling meer informatie verstrekt dan schriftelijk. Het is daarom belangrijk dat medewerkers alert zijn wat er in het kader van de AVG wel of niet mag worden gedeeld. Daarbij is er veel afhankelijk van de eigen inschatting van de betrokken medewerkers.

Andere knelpunten in het veiligheidsdomein

Net als in het publieksdomein zijn er in de afgelopen jaren verschillende stappen gezet om de gebruikte systemen en applicaties in lijn te brengen met de AVG. Inmiddels blijkt uit de verschillende checks als de verplichte DPIA's dat de meeste systemen inmiddels in lijn zijn met de AVG-richtlijnen. In de praktijk maakt het volgen van de AVG het werk er niet altijd eenvoudiger op, omdat er veel extra checks en tussenstappen zijn ingebouwd voordat gegevens inzichtelijk zijn. Dit terwijl de aard van een casus soms vraagt om snel handelen. Dit laatste knelpunt komt ook veelvuldig voor waar de gemeente afhankelijk is van de informatie van derden.

Anders dan in het sociaal domein wordt er in het veiligheidsdomein veel gewerkt met informatie over personen die geen expliciete toestemming hebben gegeven voor inzicht in hun gegevens. Dat geldt met name op het gebied van de samenwerking met politie en het OM, met het oog op het voorkomen van bijvoorbeeld strafbare feiten of met het oog op bescherming van derden.

Trainingen over privacy worden gezien als waardevol

Medewerkers in het veiligheidsdomein geven aan veel waarde te hechten aan de verschillende trainingen en workshops die in de afgelopen jaren zijn gegeven over privacy en gegevensbescherming. Enkele medewerkers uit het veiligheidsdomein wiens werk ook het sociaal domein raakt, hebben ook de leertuinen privacy in het sociaal domein gevolgd. Volgens de medewerkers die de leertuinen hebben gevolgd, bood deze veel verheldering in de mogelijkheden om de AVG-richtlijnen in de praktijk invulling te geven.

Medewerkers doen een beroep op collega's of de PO

Zoals omschreven is er in het veiligheidsdomein veel afhankelijk van de eigen inschatting van betrokken medewerkers. Dat maakt het proces van gegevensdeling soms kwetsbaar. Medewerkers geven aan dat zij daarom vaak een beroep doen op de kennis van directe collega's en niet enkel op eigen inzicht te steunen. Hoewel afdelingshoofden volgens het informatiebeveiligingsbeleid de eerste aanspreekpersoon zijn voor vragen over gegevensdeling, wordt in de praktijk door medewerkers met vragen of twijfels vaak direct contact gezocht met de PO.

3.8. Keuzes en bewustzijn op het gebied van privacy en gegevensbescherming

Aandacht voor privacy richt zich nog vooral op compliance

Tijdens de gevoerde gesprekken kwam op verschillende momenten naar voren dat er binnen de gemeente aandacht is voor gegevensbescherming. Voor een groot deel is de aandacht echter nog gericht op compliance. Dat wil zeggen dat de tijd en aandacht van de medewerkers in de drie onderzochte domeinen en de medewerkers met een specifieke taak binnen de privacy-organisatie van de gemeente

zoals de PO en de CISO, vooral gaat naar het voldoen aan de gestelde eisen en richtlijnen. In gesprekken werd aangegeven dat sommige afdelingen de AVG als een belemmering zien waaraan voldaan moet worden. Zo worden bijvoorbeeld de verwerkingsregisters wel gebruikt voor het registeren van verwerkingsactiviteiten, maar benut de gemeente de verwerkingsregisters niet voor het in kaart brengen van risico's die verbonden zijn aan de verwerkingsactiviteiten en de maatregelen die bij die risico's horen. De verwerkingsregisters zijn hierdoor vooral administratief van aard maar leveren nog geen bijdrage aan de risicoanalyse. Ook werd in gesprekken aangegeven dat de PO relatief veel tijd kwijt is met acute vragen vanuit de organisatie. Hierdoor komt de rolinvulling van de PO niet verder dan het zorgen dat acute vraagstukken worden opgelost en voldoen aan eisen en richtlijnen. Er is daardoor minder aandacht voor toekomstige ontwikkelingen en de mogelijke risico's daarvan.

De overwegingen ten aanzien van privacy krijgen te weinig gewicht

Samenhangend met de meer compliance- gerichte insteek van de gemeente is de benadering van keuzes ten aanzien van privacy en informatiebeveiliging. De compliance-achtige aanpak binnen de gemeente maakt dat de gemeente zich vooral richt op bijvoorbeeld het invullen van en bijhouden van de verwerkingsregisters of het uitvoeren van de benodigde DPIA's. Hoewel compliance een belangrijk onderdeel van gegevensbescherming is, is het ook van belang dat er meer fundamentele aandacht komt voor privacy als basiswaarde voor de organisatie. In de gevoerde gesprekken werd bijvoorbeeld aangegeven dat overwegingen in de gemeente ten aanzien van de aankoop van bijvoorbeeld nieuwe software vaak (alleen) technisch of beleidsmatig van aard zijn. Daarin is het voldoen aan de AVG een spreekwoordelijk vinkje dat gezet moet worden. Niet door alle gesprekspartners is dit beeld overigens herkend. De aard van het onderwerp gegevensbescherming vraagt naast compliance ook om een principiële overweging. Daarin is het belangrijk om privacy en gegevensbescherming meer als grondwettelijke basiswaarde van de organisatie te positioneren. Dit heeft als consequentie dat de bescherming van privacy geen argument is dat afgewogen moet worden tegen andere voor- en nadelen, maar een basiswaarde vormt die voorafgaat aan de overweging zelf. Het advies luidt dan ook om in het management een gezamenlijk gedeelde visie op het thema privacy te ontwikkelen.

4. Toekomstige ontwikkelingen

4.1. Inleiding

In de voorgaande hoofdstukken is vooral aandacht geweest voor de huidige stand van zaken binnen de gemeentelijke organisatie op het gebied van gegevensbescherming. Daarbij is er gekeken naar het beleid en de uitvoering op het gebied van privacy en gegevensbescherming. In dit hoofdstuk zal allereerst ingegaan worden op de belangrijkste toekomstige ontwikkelingen in wet- en regelgeving. Daarna zal naar de bredere ontwikkelingen op het gebied van gegevensbescherming gekeken worden en de mogelijke risico's die daarbij horen.

4.2. Ontwikkelingen in wet- en regelgeving

4.2.1. Belangrijkste toekomstige ontwikkelingen in wet- en regelgeving

Voor de komende jaren staan er verschillende ontwikkelingen op de rol als het gaat om wet- en regelgeving. De al lang op zich laten wachtende ePrivacy verordening lijkt er de komende jaren te komen, er komt met de Wet meervoudige problematiek sociaal domein (Wams) een wijziging van de Wmo 2015 en in 2023 zal de Wet modernisering elektronisch bestuurlijk verkeer (WMEBV) in werking treden.[97] Daarnaast ligt de Wet gegevensverwerking voor samenwerkingsverbanden (WGS) in de Eerste Kamer.[98] In dat licht is ook de wijziging van de BRP voor het project Landelijke Aanpak Adreskwaliteit relevant.[99] Tot slot lag in het voorjaar van 2022 de Verzamelwet gegevensbescherming bij de Raad van State.[100] Deze laatste wet heeft vooral consequenties voor het sociaal domein. Hieronder lichten we deze verschillende wetsvoorstellen en de status hiervan nader toe.

Wanneer we kijken naar de gevolgen die deze wetsontwikkelingen voor de gemeente met zich zullen brengen, dan geldt dat daarover op dit moment nog veel onduidelijk is. Vaak is het bij dergelijke wetsontwikkelingen pas bij de definitieve vaststelling duidelijk wat de exacte implicaties zijn voor de praktijk in de gemeente. Als gemeente is het daarom belangrijk om niet volledig te koersen op voorlopige wetteksten. Tegelijkertijd is het van belang om goed voorbereid te zijn op komende veranderingen. Zodra de kaders van nieuwe wet- en regelgeving vaststaan, is het verstandig om te starten met het organiseren van informatiesessies en bijscholing voor de betrokken medewerkers. Met de Leertuinen Privacy heeft de gemeente hiermee ervaring opgedaan. Ten slotte is het de overweging waard om een risicoparagraaf in de begroting op te nemen, waarin wordt ingegaan op mogelijke

[97] Zie: https://www.eerstekamer.nl/wetsvoorstel/35261_wet_modernisering; https://wetgevingskalender.overheid.nl/regeling/WGK010837 .
[98] https://wetgevingskalender.overheid.nl/regeling/wgk008727
[99] https://wetgevingskalender.overheid.nl/Regeling/WGK009588
[100] https://wetgevingskalender.overheid.nl/Regeling/WGK011059

wettelijke veranderingen. Dit aangezien het wel zeker is dát er veranderingen zullen komen, maar de concrete gevolgen daarvan nog lastig in te schatten zijn.

ePrivacy verordening
Hoewel het de bedoeling was dat de Europese ePrivacy verordening er tegelijkertijd met de AVG zou komen, laat deze verordening nog op zich wachten. Ondanks dat de definitieve tekst voor de ePrivacy verordening nog niet is vastgesteld lijkt de grootste implicatie betreffende de werkwijzen van gemeenten betrekking te hebben op de omgang met elektronische communicatie.[101] Het uitgangspunt van de ePrivacy verordening is dat zowel communicatie als de metadata van die communicatie vertrouwelijk worden. Beide zijn daarom alleen toegankelijk voor partijen die direct bij de communicatie betrokken zijn. De reikwijdte en exacte implicatie van dit uitgangspunt is door de status van de verordening nog onduidelijk.

Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams)
Een wetsvoorstel dat al in een verder stadium is, is dat van de Wams.[102] Dit wetsvoorstel vormt een wijziging van de Wet maatschappelijke ondersteuning 2015 (Wmo) en de relevante spiegelbepalingen in de Jeugdwet, Participatiewet en de Wet gemeenschappelijke schuldhulpverlening. De aanleiding voor deze wetswijziging ligt in de moeilijkheden voor gemeenten bij het bieden van integrale ondersteuning in het sociaal domein en de daarbij benodigde domeinoverstijgende gegevensuitwisseling. Een duidelijke wettelijke basis voor deze uitwisseling van gegevens ontbreekt nu nog. Aangezien deze wetswijziging nog duidelijker de verantwoordelijkheid voor het bieden van een gecoördineerde aanpak bij de gemeenten neerlegt, is deze grondslag nodig. Deze wijziging moet helpen om gegevens uit te wisselen tussen het sociaal domein en de aanpalende domeinen: zorg en ggz, welzijn, onderwijs, wonen, openbare orde en veiligheid, werk en inkomen, inburgering.[103] Deze wetswijziging zou de gemeente vooral een extra instrument moeten geven om te werken aan integrale hulpverlening in het sociaal domein. In maart 2020 is het wetsvoorstel van de Wams ter consultatie gelegd.[104] De gemeente Zoetermeer heeft bijgedragen aan het wetsvoorstel door met een uitvoerige schriftelijke reactie deel te nemen aan de internetconsultatie en heeft daarin aangegeven blij te zijn met het voorstel dat grondslagen schept om het delen van gegevens bij meervoudige complexe problematiek mogelijk te maken.[105] Daarin plaatst de gemeente wel enkele kanttekeningen bij de wettekst en wijst bijvoorbeeld op de toenemende verantwoordelijkheid van de gemeente ten opzichte van externe partijen. Verder heeft de Raad van State een advies uitgebracht waarin zij onder meer de noodzaak van deskundigheidsbevordering bij professionals benadrukt, waaronder de gemeenten.

Hoewel de ontwikkeling van dit wetsvoorstel in een verder stadium is, is het nog lastig te zeggen welke gevolgen het voor de organisatie gaat krijgen. Zo loopt er nog een onderzoek naar de mogelijke opzet van een PrivacyApp voor het gehele sociale domein en er wordt nagedacht over een verdieping van het

[101] De stand van het Europese wetgevingsproces is te volgen via: https://eur-lex.europa.eu/legal-content/NL/HIS/?uri=CELEX:52017PC0010. Na vaststelling van de tekst van de verordening, zullen de lidstaten nog een periode van twee jaar krijgen voordat de regels van toepassing worden.
[102] Het Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams) wordt na de zomer van 2022 naar de tweede kamer verzonden.
[103] Concept Wet aanpak samenhangende meervoudige problematiek in het sociaal domein (Wams).
[104] VNG (2022). Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams): https://vng.nl/artikelen/wetsvoorstel-aanpak-meervoudige-problematiek-in-het-sociaal-domein-wams.
[105] Gemeente Zoetermeer (2020). Reactie wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams), d.d. 14 mei 2020.

wetsvoorstel waarbij er wordt gekeken naar verbindingen met verschillende uitvoeringspraktijken (zoals wijkteams, onderwijs, wonen, werk en inkomen, Wvggz).[106]

Wet modernisering elektronisch bestuurlijk verkeer (WMEBV)
In 2023 zal de Wet modernisering elektronisch bestuurlijk verkeer (WMEBV) in werking treden. De WMEBV brengt een wijziging van wettelijke bepalingen ten aanzien van de elektronisch bestuurlijk verkeer tot stand. Hierdoor worden onder meer verschillende bepalingen uit de Algemene wet bestuursrecht gewijzigd. Deze wijziging heeft betrekking op het elektronisch bestuurlijke verkeer tussen overheden en burgers. Uit deze wijziging volgen twee consequenties voor gemeentelijke bestuursorganen. Allereerst moet er voor ieder elektronisch formeel bericht gericht aan het bestuursorgaan een digitale weg openstaan. Dat betekent dat iedere formele communicatie-uiting ook digitaal moet kunnen plaatsvinden. Daarbij zullen digitale kanalen van het bestuursorgaan moeten voldoen aan de wettelijke eisen op het gebied van toegankelijkheid en de noodzakelijkheid van het vragen van gegevens.[107]

Digitaal volwassen bestuursorganen, zoals de gemeente Zoetermeer, met al diverse digitale kanalen om elektronische berichten te ontvangen, zullen scherp moeten kijken waar er aanpassingen nodig zijn. De verwachting is dat de volgende afdelingen betrokken zijn moeten worden om op een correcte manier aan de verplichten te voldoen, zodra die helder zijn: juridische zaken, informatie afdeling/ICT afdeling, communicatie-experts, data- en informatiebeveiliging, programmamanagers, front office , de backoffice-verwerking en de financiële deskundigen. De investeringskosten voor materiaal zal naar verwachting beperkt zijn, aldus de VNG.[108]

Wet gegevensverwerking samenwerkingsverbanden (WGS)
Een andere aankomende wetswijziging die voor de gemeente relevant is, is die van de Wet gegevensverwerking samenwerkingsverbanden (WGS). Dit voorstel is aangenomen door de Tweede Kamer en ligt nu bij de Eerste Kamer. Deze wet moet een specifieke wettelijke grondslag gaan bieden voor de uitwisseling van persoonsgegevens tussen samenwerkingsverbanden voor de bestrijding van fraude en ondermijnende criminaliteit. Deze wet zal de gemeente vooral van extra instrumentarium voorzien op dit terrein. Daarmee samenhangend ligt er een wijziging van de BRP in de Eerste Kamer in verband met het project Landelijke Aanpak Adreskwaliteit (LAA).[109] Deze wijziging van de BRP moet een structurele inbedding bieden voor de werkwijze van het project LAA waarin gemeenten aan een centraal punt melding maken over uitkomsten van onderzoeken naar adreskwaliteit. Deze wijziging geeft daar een grondslag voor.

In de Memorie van Toelichting van het wetsvoorstel LAA staat dat de verwachting is dat de administratieve handeling zal overeenkomen met een regulier adresonderzoek. Daarbij blijft het uitvoeren van een onderzoek naar adreskwaliteit een eigenstandige bevoegdheid van het college en wordt het college niet verplicht om onderzoek uit te voeren op het moment dat er signalen komen van

[106] VNG (2022). Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams): https://vng.nl/artikelen/wetsvoorstel-aanpak-meervoudige-problematiek-in-het-sociaal-domein-wams.
[107] Handreiking implementatie Wet modernisering elektronisch bestuurlijk verkeer.
[108] Handreiking implementatie Wet modernisering elektronisch bestuurlijk verkeer (Awb) 2020. Wat betekenen de veranderingen voor uw als bestuursorgaan?
https://vng.nl/sites/default/files/2022-03/handreiking-implementatie-wmebv-versie-okt.-2020.aanvullinghf.pdf
[109] https://wetgevingskalender.overheid.nl/Regeling/WGK009588

de minister.[110] Uit een impactanalyse van VNG blijkt echter dat de werkwijze van het project LAA gemeenten wel meer tijd en werk zullen kosten. Tot deze conclusie kwam de VNG door uit te gaan van de financiële gevolgen en uitvoeringlasten die rechtstreeks voortvloeien uit het wetsvoorstel zelf.[111]

Verzamelwet gegevensbescherming
Tot slot lag in het voorjaar van 2022 de Verzamelwet gegevensbescherming bij de Raad van State voor advisering. De Verzamelwet gegevensbescherming brengt – in de huidige conceptversie – onder meer een wijziging van enkele bepalingen uit de UAVG tot stand. Die wijzigingen zijn voor de gemeente met name relevante als het gaat om de uitoefening van de rechten van betrokkenen. Artikel 5 van de UAVG bepaalt dat er voor de verwerking van persoonsgegevens van betrokkenen onder de 16 jaar toestemming nodig is van de wettelijke vertegenwoordiger. Dit blijft ook zo na de wetswijziging. De betrokkene die ouder is dan 12 jaar maar jonger dan 16 jaar krijgt wel het recht om de verleende toestemming in te trekken.[112] Daarnaast zal de wetswijziging jongeren van 12 jaar en ouder de mogelijkheid geven om zelfstandig de rechten uit hoofdstuk 3 van de AVG uit te oefenen. Dit betekent bijvoorbeeld dat jongeren vanaf 12 jaar zich zelfstandig op het recht op rectificatie, inzage of vergetelheid kunnen beroepen zonder de instemming van hun wettelijk vertegenwoordiger. Verder zal rechtspositie van onder curatele staande en onder bewindvoering of mentorschap vallende betrokkene worden versterkt.

Ook hier is er – in de huidige conceptversie – sprake van een uitbreiding van het recht om toestemming voor gegevensverwerking in te trekken.[113] Bij de samenwerking rondom een specifieke casus zijn de deelnemende partijen verantwoordelijk voor de bevoegdheden en taken.[114]

4.3. Toekomstige ontwikkelingen en bijbehorende risico's voor de gemeente

4.3.1. Aandachtspunten van de AP voor de toekomt van gegevensbescherming

Voor de periode 2020-2023 heeft de Autoriteit Persoonsgegevens (hierna: AP) drie focusgebieden voor haar toezichthoudende rol geformuleerd. Een van die drie focuspunten is het functioneren van de digitale overheid.[115] In haar focus op de digitale overheid heeft de AP onder meer aandacht voor databeveiliging bij overheden, de ontwikkeling van slimme technologieën in bijvoorbeeld *Smart Cities* en het delen van persoonsgegevens in samenwerkingsverbanden.[116]

---

[110] VNG (2022). VNG Inbreng plenair debat Wijzigingswet BRP 35.772 over Landelijke Aanpak Adreskwaliteit 3 februari https://vng.nl/sites/default/files/2022-01/20220128_brief-parlement_VNG-Inbreng-plenair-debat-Wijzigingswet-BRP-35772-over-Landelijke-Aanpak-Adreskwaliteit-3-februari.pdf
[111] Wijziging van de Wet basisregistratie personen in verband met de invoering van een centrale voorziening ter ondersteuning van de colleges van burgemeester en wethouders bij het onderzoek of een persoon als ingezetene in de basisregistratie personen op een adres in de gemeente dient te worden ingeschreven alsmede naar de juistheid van de gegevens betreffende het adres van een ingezetene in de basisregistratie personen MEMORIE VAN TOELICHTING, pag. 20 (2020-2021)
[112] De verankering van dit recht van de betrokkene zal in art. 5lid 3 UAVG worden opgenomen.
[113] Zie: https://www.internetconsultatie.nl/verzamelwetgegevensbescherming voor het wijzigingsdocument van de UAVG als gevolg van de Verzamelwet gegevensbescherming.
[114] VNG (2020). Gegevensuitwisseling bij samenwerking rond casuïstiek in het zorg- en veiligheidsdomein https://vng.nl/sites/default/files/2020-08/handvat-gegevensuitwisseling-zvh-versie-2.2.pdf, pagina 83
[115] De andere twee focusgebieden betreffen de thema's datahandel en artificiële intelligentie & algoritmen.
[116] Focus AP 2020-2023.

De beveiliging van persoonsgegevens laat volgens de AP bij overheden vaak nog te wensen over, terwijl overheden juist veel bijzondere en gevoelige persoonsgegevens verwerken. Blijvende aandacht van gemeenten op dit onderwerp is daarom van belang. De AP meldt aan overheden te willen gaan controleren op hun beveiligingsniveau en te willen stimuleren dat overheidsorganisaties aandacht besteden aan privacyrisicomanagement en IT-audits.[117]

Een tweede punt van aandacht van de AP is de ontwikkeling van "slimme oplossingen voor vraagstukken op het gebied van mobiliteit, energie, veiligheid en huisvesting".[118] Door op een slimme manier verschillende databronnen te koppelen of op een geavanceerde manier data te gebruiken kunnen overheden vraagstukken op het gebied van bijvoorbeeld afval of energieverbruik oplossen. Zogenaamde *smart cities* zijn hier een voorbeeld van. Volgens de AP is het wel nodig dat overheden zich tijdig realiseren wat de risico's in dergelijke manieren van werken zijn en wat er nodig is om daarbij te blijven voldoen aan de eisen van de AVG. Hierin is de AP niet de enige. In een recent rapport noemt ook belangenorganisatie *Bits of Freedom* het risico van vormen van datagedreven werken door gemeenten. De stelling van *Bits of Freedom* is daarbij dat gemeenten niet moeten beginnen aan datagedreven werken of andere slimme vormen van datatoepassing wanneer een gemeente de basis voor informatiebeveiliging niet op orde heeft.[119]

Tot slot heeft de AP aandacht voor de toenemende mate waarin overheden informatie uitwisselen in samenwerkingsverbanden om dienstverlening te verbeteren of criminaliteit op te sporen. Hoewel de intenties vaak goed zijn, kan dit problemen geven met het beginsel van doelbinding.[120] In dit kader zijn ook de ontwikkelingen rond de Wet gegevensverwerking door samenwerkingsverbanden relevant. Dit wetvoorstel moet gaan voorzien in een wettelijke grondslag voor het verwerken van gegevens door samenwerkingsverbanden voor de bestrijding van fraude en criminaliteit.[121] Daarbij kan bijvoorbeeld gedacht worden aan misbruik van de gemeentelijke voorzieningen of vormen van woonfraude.

4.3.2. De gemeente werkt aan het worden van een Smart City

De afgelopen jaren heeft de gemeente op verschillende manieren gewerkt aan de ambitie om een '*smart city*' te worden. De Initiatievenlijst Zoetermeer Smart City geeft een weergave van de 27 initiatieven die de gemeente sinds 2018 heeft ondernemen om een Smart City te worden.[122] Zo heeft de gemeente bijvoorbeeld gewerkt aan het inzetten van slimme technieken voor parkeertellingen en de inzet van slimme techniek om het onderhoud aan de openbare ruimte te voorspellen.

De AP doet de aanbeveling om beleid voor Smart City-toepassingen vast te stellen

Hoewel slimme technieken en de inzet van data de gemeente verder kunnen helpen op allerlei gebieden, brengt de inzet daarvan ook altijd risico's met zich mee. Zoals bovenstaand beschreven, wijzen de AP en het recente rapport van *Bits of Freedom* beide op de risico's die samenhangen met vormen van datagedreven werken en de toepassing van slimme technologieën. De AP wijst daarbij vooral op risico's en stelt dat het voor gemeenten belangrijk is om de risico's in beeld te brengen. Het rapport van *Bits of*

[117] Focus AP 2020-2023, p.23.
[118] Focus AP 2020-2023, p.23.
[119] Bits of Freedom, De staat van privacy bij gemeenten (2022), p.11.
[120] Focus AP 2020-2023
[121] https://wetgevingskalender.overheid.nl/regeling/wgk008727.
[122] Initiatievenlijst Zoetermeer smart city.

Freedom benadrukt dat het belangrijk is om eerst de basis van gegevensbescherming in de gemeente op orde te hebben voordat een gemeente begint aan vormen van datagedreven werken.

Naast de door de AP opgestelde focusgebieden, heeft de AP ook een onderzoeksrapport naar de bescherming van persoonsgegevens in Smart Cities opgesteld.[123] Hierin doet de AP verschillende aanbevelingen voor het werken van Smart City-toepassingen. Net zoals het rapport van *Bits of Freedom* stelt de AP dat het belangrijk is om eerst de basisbeginselen van gegevensbescherming op orde te hebben. Belangrijk daarbij is het vaststellen van de verwerkingsgronden bij de toepassing in een Smart City. Daarnaast geeft de AP aan dat het belangrijk is om tijdig een DPIA uit te voeren op Smart City-toepassingen en de uitkomsten daarvan vaker te publiceren. Verder doet de AP de aanbeveling om beleid vast te stellen voor de inzet van Smart City-toepassingen. Dit beleid moet concrete handvatten bevatten voor de praktijk. Voor zover de onderzoekers hebben kunnen zien heeft de gemeente geen apart beleid voor de Smart City-toepassingen.

4.3.3. Dreigingsbeeld informatiebeveiliging geeft aan waar belangrijkste risico's liggen

De Informatiebeveiligingsdienst (IBD) stelt ieder jaar een zogeheten Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten op.[124] In dit dreigingsbeeld wordt een actueel inzicht geboden in de belangrijkste risico's voor gemeentelijke informatiebeveiliging. Het dreigingsbeeld voor 2021-2022 identificeert ambtelijke, politieke en maatschappelijke risico's. Enkele voorbeelden die genoemd worden zijn:

- Integriteit van gegevens niet gewaarborgd: wanneer verantwoordelijkheden in informatiesystemen niet goed zijn belegd, bestaat het risico dat kwaadwillenden gegevens kunnen wijzigen, wissen of toevoegen;
- Vertrouwelijke gegevens in verkeerde handen: door e-mails aan een verkeerd e-mailadres of fouten in de toegangsrechten van gebruikte systemen kan vertrouwelijke informatie onder ogen komen van ongeautoriseerde personen - dit zijn de meest voorkomende vormen van datalekken;
- Imagoschade: wanneer blijkt dat niet zorgvuldig is omgegaan met (vertrouwelijke) informatie, wordt dit het gemeentebestuur aangerekend; dit kan het vertrouwen sterk aantasten;
- Schade aan democratische processen: inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen kunnen leiden tot aantasting van het democratisch proces, bijvoorbeeld wanneer bij het tellen van stemmen onveilige software wordt gebruikt;
- Afhankelijkheid van de overheid: wanneer informatie van de overheid in verkeerde handen komt zijn mogelijke gevolgen voor inwoners en ondernemers bijna niet te overzien, bijvoorbeeld bij informatie over ontvangers van jeugdzorg;

Om tegemoet te kunnen komen aan deze risico's verstrekt de IBD verschillende aanbevelingen voor overheden om bescherming van gegevens goed te kunnen borgen:

- Voer regie over risicomanagement: het voorkomen van menselijke of technische fouten of opzettelijk handelen wordt pas mogelijk wanneer zorgvuldig wordt gekeken naar de risico's. Dit is in de eerste plaats een taak voor het management, wat geadviseerd kan worden door de CISO.

[123] Smart City, Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities (2021).
[124] Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022.

Zorgvuldig risicomanagement kenmerkt zich door periodiek een cyclus van plannen, uitvoeren, controleren en bijstellen te doorlopen;

- Techniek is niet de belangrijkste factor: een informatiesysteem kan technisch nog zoveel mogelijkheden bieden; als de rollen en rechten niet goed zijn belegd zijn er nog steeds zwakke schakels. Houd daarom naast de techniek oog voor het werkproces en de menselijke factor;
- Bied veilige gereedschappen: bekijk wat medewerkers nodig hebben en faciliteer hen om net dat stapje meer te zetten om de veiligheid te waarborgen (leuker kunnen we het niet maken, maar wel veiliger).
- Zorg voor een open cultuur: medewerkers moeten zich veilig weten wanneer er sprake is van onveilige situaties of wanneer er zich incidenten voordoen. Zorg ervoor dat medewerkers kunnen leren van incidenten door hen te stimuleren om incidenten te melden en hen te belonen wanneer zij veilig werken.
- Oefen en bereid je voor: zorg als management en directie voor een gedegen incidentenmanagement. Weet wie wanneer nodig is wanneer een incident dreigt of optreedt. Zorg er daarnaast voor dat regelmatig wordt geoefend met een crisisstructuur en gebruik hierbij scenario's die herkenbaar zijn voor de betrokken medewerkers.

5. Beantwoording onderzoeksvragen/conclusies en aanbevelingen

5.1. Beantwoording onderzoeksvragen

In dit laatste hoofdstuk zal ingegaan worden op de beantwoording van de onderzoeksvragen en trekken we conclusies. Op basis daarvan zal dit hoofdstuk afsluiten met verbeterpunten. Deze verbeterpunten bevatten ook aanbevelingen voor de toekomst.

5.1.1. Overkoepelende conclusie

Hoofdvraag: *In hoeverre is de AVG succesvol geïmplementeerd binnen de gemeente Zoetermeer, zodat burgers volledige gegevensbescherming genieten en de medewerkers van de gemeente kunnen voldoen aan de eisen van de AVG?*

> De richtlijnen van de AVG zijn geïmplementeerd, maar bij de uitvoering zijn kanttekeningen te maken.

De gemeente Zoetermeer heeft veel inspanningen geleverd om de AVG te implementeren in de organisatie; in het beleid, de gehanteerde werkwijzen en de gebruikte systemen. Tegelijkertijd is er nog veel ruimte voor verbetering op het gebied van het toezien op, rapporteren over en evalueren van de wijze waarop de gemeente invulling geeft aan de verplichtingen uit de AVG. Bijzondere aandacht verdient daarbij de verdeling van rollen en verantwoordelijkheden binnen de organisatie en de verantwoordelijkheden die daar liggen op het gebied van toezicht en rapportage.

De basiskennis over de AVG onder medewerkers lijkt op basis van de enquête op orde. Wel worden AVG-richtlijnen soms nog als een belemmering gezien. Werkdruk, capaciteitsproblemen en verloop in de organisatie staan in de weg aan structurele kennisopbouw en monitoring. Doordat er veel tijd en inzet wordt gestoken in het ondersteunen bij acute vraagstukken, is er daarnaast beperkte ruimte voor prioritering en anticipatie op toekomstige ontwikkelingen.

5.1.2. Conclusies waarborgen

Deelvraag 1: *Zijn binnen de organisatie voldoende waarborgen aanwezig die voorzien in een betrouwbare bescherming van persoonsgegevens van betrokkenen, conform de AVG?*

> Het beleid biedt voldoende waarborgen, de uitvoering in de praktijk vraagt om meer invulling.

Sinds de inwerkingtreding van de AVG in 2016 heeft de gemeente Zoetermeer een groot aantal maatregelen genomen om een betrouwbare gegevensbescherming te waarborgen. Door middel van een implementatieprogramma zijn verschillende beleidskaders opgesteld waarin uiteengezet is hoe taken en verantwoordelijkheden binnen de organisatie zijn verdeeld. Centraal staan het informatiebeveiligingsbeleid en het privacybeleid. Uit deze beleidskaders volgen verschillende vastgestelde procedures en werkwijzen die worden gehanteerd om invulling te geven aan de AVG-taken, waaronder de beveiliging van persoonsgegevens middels digitale infrastructuur, het bijhouden van verwerkingsactiviteiten in een register, het delen van gegevens met derden en de omgang met datalekken. Daarnaast zijn er functionarissen aangesteld om toe te zien op het uitvoeren van de taken die uit de AVG volgen: de Functionaris Gegevensbescherming (FG), de Privacy Officer (PO) en de Chief Information Security Officer (CISO). Hoewel in het beleidskader is aangegeven dat de verantwoordelijkheden binnen de organisatie zijn verdeeld volgens het 3LoD-model, zijn er verschillende knelpunten aan te wijzen in de manier waarop die verantwoordelijkheden in de praktijk tot uitvoering komen. De verdeling van verantwoordelijkheden volgens het 3LoD-model, zoals in het informatiebeveiligingsbeleid benoemd, wordt in de praktijk op een andere manier ingevuld. In de beantwoording van de volgende deelvragen wordt verder ingegaan op knelpunten ten aanzien van de rolverdeling.

Om betrouwbare gegevensbescherming te kunnen waarborgen, is het van belang dat de gehanteerde werkwijzen worden nagevolgd, periodiek worden geëvalueerd en dat hierover ook wordt gerapporteerd. Binnen de gemeente Zoetermeer vinden audits, controles en evaluaties plaats, waaronder de volgens de AVG verplichte DPIA- en ENSIA-controles. Daarnaast wordt door de FG, Privacy Officer en CISO halfjaarlijks mondeling gerapporteerd aan het directieteam over de bevindingen uit de praktijk, op basis waarvan nieuwe doelstellingen voor het komend halfjaar worden bepaald.

Een belangrijke schakel die mist binnen de waarborgen die er nodig zijn voor een betrouwbare gegevensbescherming is het onafhankelijke toezicht van de FG. De functiecombinatie van de FG met de functie van teammanager geeft de FG meer betrokkenheid bij de organisatie maar doet af aan de onafhankelijkheid van de FG, en zou in de praktijk tot een belangenconflict kunnen leiden. Daarnaast doet deze combinatie van functies af aan de beschikbare capaciteit voor toezicht. In vergelijkbare gemeenten is de invulling van de FG qua capaciteit fors omvangrijker dan in Zoetermeer. Tot slot missen ook de onafhankelijke schriftelijke rapportages van de FG aan de gemeentesecretaris. Deze schriftelijke rapportages zouden bestuurlijk inzicht moeten geven in de opvattingen van de FG, de adviezen van de FG aan de organisatie en het besluit van de organisatie om wel of geen gehoor te geven aan dat advies. De rol van onafhankelijk toezichthouder krijgt om bovengenoemde redenen onvoldoende invulling.

Deelvraag 2: *Is bij incidenten (datalekken) sprake van zorgvuldige afhandeling conform de AVG?*

Incidenten (datalekken) worden zorgvuldig en conform de AVG afgehandeld.

Wanneer er sprake is van een datalek bij de gemeente is het interne proces datalekken van toepassing. Het door de gemeente opgestelde stappenplan in het geval van een datalek is uitvoerig en komt overeen met het stappenplan van de AP. Dit wordt aangevuld door verschillende gemeentelijke handreikingen die medewerkers kunnen raadplegen bij afwegingen omtrent datalekken. Het proces omtrent datalekken is in de gemeente eenduidig toegepast. Na melding vindt er een beoordeling van het risico plaats en beoordeelt de PO of er melding moet worden gemaakt bij de AP. De FG heeft de mogelijkheid

om maatregelen te treffen in geval van calamiteiten of gebreken en krijgt toegang tot verwerkingsactiviteiten die worden uitgevoerd. In het geval van datalekken die een grote publieke impact hebben of politiek gevoelig zijn moeten ook de gemeenteraad en het college geïnformeerd worden. De FG maakt hier melding van bij het college.

De Privacy Officer rapporteert jaarlijks over de datalekken die zich dat jaar hebben voorgedaan, zodat er overkoepelend inzicht is in de aard en omvang van de datalekken. Op basis van de cijfers lijkt het aantal datalekken van de afgelopen jaren klein in verhouding tot de omvang van de gemeente. Belangrijk is daarom om de kanttekening is te maken dat datalekken door medewerkers mogelijk niet altijd als zodanig herkend worden of niet worden gemeld. Dit is een kwetsbaarheid in het proces, die voortkomt uit de verantwoordelijkheid van direct betrokken medewerkers om een datalek ook als zodanig te herkennen.

5.1.3. Conclusies organisatie

Deelvraag 3: *Worden de medewerkers bij de uitvoering van hun taken voldoende gefaciliteerd in het efficiënt en effectief werken conform de AVG?*

> Medewerkers hebben een duidelijk aanspreekpunt voor vragen over de AVG. Toch ervaren medewerkers het werken volgens de AVG soms als lastig.

Om een juiste uitvoering van de AVG-taken te waarborgen, heeft de gemeente Zoetermeer verschillende handreikingen, protocollen en werkwijzen opgesteld die medewerkers kunnen hanteren. Zo is in de bestuursvoorstellen het geven van een toelichting ten aanzien informatiebeveiliging, privacy en informatiebeheer een vaste stap geworden. Wanneer er vragen of onduidelijkheden zijn omtrent de AVG-taken, kunnen medewerkers volgens het beleidskader in de eerste plaats terecht bij de afdelingshoofden en in de tweede plaats bij de PO of FG . De praktijk wijst echter uit dat medewerkers bij vragen vaak al in eerste instantie een beroep doen op de PO. Medewerkers ervaren de ondersteuning van de PO als zeer positief en behulpzaam. Hoewel vragen hierdoor snel beantwoording krijgen, legt de hoeveelheid vragen wel beslag op de tijd en capaciteit van de PO. De PO is hierdoor relatief veel tijd kwijt met het oplossen van acute vraagstukken en het voldoen aan eisen en richtlijnen (compliance). Er is daardoor minder aandacht voor evaluatie van privacyvraagstukken en beleidsontwikkeling. Op het terrein van efficiëntie en effectiviteit is derhalve nog winst te boeken.

Zowel in de vragenlijst als in de gevoerde gesprekken geven medewerkers aan het soms als lastig te vinden om te werken volgens de AVG. Die moeilijkheid zit daarbij soms voor medewerkers in de onduidelijkheid over de rolverdeling in de organisatie en soms in de beschikbare (software) programma's waarin medewerkers moeten werken. In sommige gevallen kunnen de medewerkers gegevens inzien waartoe zij eigenlijk geen toegang zouden mogen hebben. Ook is benoemd dat richtlijnen uit de AVG door enkele samenwerkingspartners van de gemeente anders worden geïnterpreteerd en toegepast.

Deelvraag 4: *Hoe wordt ervoor gezorgd dat binnen de organisatie structureel voldoende kennis en kunde aanwezig is op het gebied van gegevensbescherming?*

> Er is veel inzet op kennis en kunde van medewerkers. De borging van kennis vraagt echter om een meer structurele programmering van (bij)scholing.

Medewerkers lijken blijkens de enquête en de gevoerde interviews op de hoogte van de basisrichtlijnen uit de AVG en de taken en verantwoordelijkheden die hieruit volgen. De gemeente doet dan ook veel om ervoor te zorgen dat de kennis over de AVG op peil blijft, onder meer door middel van (online) workshops, trainingen, en de leertuinen privacy voor het sociaal domein. In het kader van de implementatie van de AVG hebben daarnaast verschillende bewustwordingsacties binnen de organisatie plaatsgevonden. Onderdelen hiervan waren workshops voor nieuwe medewerkers, een 'roadshow' langs alle afdelingen en het inzetten van privacy-ambassadeurs. Binnen de afdelingen is er daarnaast ruimte voor kennisdeling en overleg over privacydilemma's tijdens voortgangsgesprekken of afdelingsoverleggen, al verschilt de aandacht hiervoor per afdeling. Tegelijkertijd geven verschillende medewerkers aan dat voor hen desondanks niet altijd duidelijk is hoe te handelen in het kader van de AVG. Hiervoor worden redenen gegeven als de hoge mate van verloop in de organisatie, de werkdruk of onduidelijkheid over de onderlinge rol- en taakverdeling.

Deelvraag 5: *Hoe wordt ervoor gezorgd dat, als vervolg op de Leertuinen privacy voor het Sociaal Domein, medewerkers gegevensbescherming als onderdeel van hun werkzaamheden zien en niet als belemmering?*

De leertuinen hebben geholpen in de werkwijzen ten aanzien van de AVG, vervolginzet is nodig

De basiskennis van medewerkers ten aanzien van de AVG lijkt op orde, en inmiddels is er binnen de afdelingen veel ervaring opgebouwd in het werken volgens de AVG. De leertuinen privacy voor het sociaal domein worden door medewerkers die hieraan deelnamen gezien als een goed hulpmiddel om kennis en ervaring op te doen met de AVG en vraagstukken die gepaard gaan met het vertalen van de richtlijnen naar de praktijk. Daarnaast wordt het als positief ervaren dat de onderwerpen informatiebeveiliging, privacy en informatiebeheer gezamenlijk terugkomen bij de voortgangsgesprekken met medewerkers.

Ondanks de inzet die de gemeente heeft geleverd met de leertuinen blijven veel medewerkers het werken volgens de AVG-richtlijnen als een uitdaging zien, en soms zelfs als een belemmering. Dat laatste geldt voor de samenwerking met externe partners, die verder of juist minder ver zijn in het implementeren van de AVG dan de gemeente, of die andere methoden en processen hanteren dan de gemeente. Daarnaast vinden veel medewerkers dat het werken volgens de AVG-richtlijnen belemmeringen met zich meebrengt in de vorm van extra stappen die moeten worden doorlopen om gegevens te kunnen achterhalen of te kunnen delen. Gegeven de hoge ervaren werkdruk en het verloop in de organisatie ervaren medewerkers dat zij onvoldoende aandacht kunnen geven aan wat de AVG van hen vraagt. Daar komt bij dat de workshops en trainingen die voor medewerkers worden georganiseerd om hen te faciliteren in kennisopbouw over de AVG niet door alle medewerkers die veel met de AVG werken worden gevolgd.

5.1.4. Conclusies lessen voor de toekomst

Deelvraag 6: *Welke verbeterpunten zijn er ten aanzien van bovenstaande vragen?*

De verbeterpunten ten aanzien van de onderzoeksvragen zijn onder 5.2 geformuleerd.

Deelvraag 7: *Is de huidige organisatie voldoende toegerust om de toekomstige ontwikkelingen (zoals aankomende wet- en regelgeving, nieuwe technologieën etc.) aan te kunnen en zijn er eventuele verbeterpunten? Wat is daar eventueel nog voor benodigd (qua organisatie, middelen e.d.)?*

> Voor het zijn van een toekomstbestendige organisatie is er meer inzet nodig op het gebied van toezicht en het in kaart brengen van risico's

Als het gaat om de bestendigheid ten aanzien van de toekomstige ontwikkelingen, is er meer inzet nodig in de organisatie op het gebied van het in kaart van brengen van risico's en het toezicht op de organisatie. Het vaststellen van beleid kan daarin een belangrijke stap zijn. Momenteel richt de organisatie zich nog vooral op het organiseren van de basis van gegevensbescherming zoals het rapporteren van datalekken, het inrichten van verwerkingsregisters en de door medewerkers gehanteerde werkwijzen om te voldoen aan de AVG. Om toekomstbestendig te zijn is er echter meer inzet nodig op het proactief in kaart brengen van risico's die komen kijken bij nieuwe technologieën of werkwijzen. Hier is nu nog weinig aandacht voor in de gemeente. Daarnaast draagt onafhankelijk toezicht op de organisatie bij aan het kunnen opvangen risico's. De onafhankelijke advisering van de FG kan de gemeente behoeden voor het maken van fouten en het opvangen van het risico.

5.2. Verbeterpunten

Stel een gezamenlijke visie op voor de omgang met privacy en de inrichting van de privacy-organisatie

Er is nog veel ruimte voor verbetering op het gebied van het toezien op, rapporteren over en evalueren van de wijze waarop de gemeente invulling geeft aan de verplichtingen uit de AVG. Een goede omgang met privacy en gegevensbescherming vereist een eenduidige aanpak, die kan rekenen op draagvlak in de organisatie. Momenteel is er wel een beleidskader, maar de invulling in de praktijk verschilt op onderdelen van wat er in dat kader is voorgeschreven. En die praktijkinvulling kent nog diverse knelpunten en dilemma's. De leertuinen privacy waren en zijn een instrument om medewerkers te faciliteren bij het adresseren en oplossen hiervan. In de leertuinen werden de doelen van de AVG sterk benadrukt: iedereen wil dat zijn of haar persoonsgegevens goed worden beschermd, en dat betekent dan ook dat de gemeente hier als overheidsinstelling zorg voor draagt. Als meer vanuit dit uitgangspunt wordt gewerkt met de AVG, in plaats van vanuit het gevoel dat de AVG extra belemmeringen met zich meebrengt, wordt het draagvlak onder medewerkers groter.

Aanbevolen wordt om dit uitgangspunt door te trekken naar een gezamenlijke visie op de omgang met privacy en de inrichting van de privacy-organisatie. Zo'n gedeelde visie kan helderheid bieden over de gezamenlijke doelen en prioriteiten, en kan onduidelijkheden over rolverdeling wegnemen. Neem als management het initiatief voor het opstellen van zo'n visie op privacy, en betrek medewerkers uit de verschillende domeinen hier actief bij.

Actualiseer het beleidskader

Hoewel de gemeente met het informatiebeveiligings- en privacybeleid een compleet beleidskader heeft voor gegevensbescherming, is dit beleid in de loop der jaren nog niet geëvalueerd. Uit dit onderzoek komen verschillende knel- en verbeterpunten naar voren die meegenomen zouden kunnen worden in het verbeteren en actualiseren van het beleidskader. In het licht van de onderzoeksbevindingen is het

vooral van belang dat er helderheid ontstaat over de onderlinge rol- en taakverdeling, en dat medewerkers betrokken worden bij de keuzes die hierin worden gemaakt.

Momenteel wordt het 3LoD-model op een andere wijze toegepast dan in het informatiebeveiligingsbeleid is geformuleerd. Actualisatie van het beleidskader door zowel in het informatiebeveiligingsbeleid als het privacybeleid een eenduidige beschrijving van dit model op te nemen die ook voldoet aan de huidige praktijkinvulling is een eerste stap om meer helderheid te bieden. Niet omdat het model een doel op zich is, maar omdat dit een instrument kan zijn aan de hand waarvan begrijpelijk kan worden gemaakt wat er van hen verwacht wordt en welke mogelijkheden er zijn om advies te vragen. Maak de verdeling van verantwoordelijkheden volgens het model kenbaar en zie er ook op toe dat deze op een eenduidige manier wordt toegepast. Ook de positionering van de CISO kan bij de actualisering in lijn met de realiteit worden gebracht, zoals al het voornemen is. Een actievere inzet van het privacynetwerk met privacyambassadeurs, dan wel het werken met domein-ISO's kan medewerkers verder ondersteuning bieden, en zal het takenpakket van de PO verlichten.

Het privacybeleid wijkt daarnaast momenteel op twee punten af van wat de Autoriteit Persoonsgegevens van een privacybeleid vraagt. Allereerst kent het privacybeleid geen omschrijving van de categorieën van persoonsgegevens die door de gemeente worden verwerkt. Daarnaast koppelt het gemeentelijke privacybeleid de verwerking van de verschillende categorieën van persoonsgegevens niet aan doeleinden en grondslagen voor verwerking. Aanbevolen wordt om bij de actualisatie van het privacybeleid deze onderdelen expliciet op te nemen. Een optie is ook om deze transparantie te bieden in een privacyverklaring of privacystatement.

Vervolledig de waarborgen voor een zorgvuldige gegevensverwerking

Bij het implementatieproces van de AVG zijn er veel stappen gezet om de gemeente te laten voldoen aan de vereisten voor een zorgvuldige gegevensbescherming. Naast actualisatie van het beleidskader zijn er nog enkele specifieke acties die gepleegd kunnen worden om hier een verbeterslag in te maken. Zo wordt aanbevolen om te inventariseren in hoeverre alle relevante processen en verwerkersovereenkomsten in de verwerkingsregisters opgenomen zijn. Ook wordt aanbevolen om maatregelen te nemen die ervoor zorgen dat er meer overzicht komt in hoe informatie wordt beheerd. De gemeentearchivaris heeft hier verschillende suggesties voor gedaan die momenteel nog onvoldoende opvolging hebben gekregen. Een ander knelpunt wat zowel door de gemeentearchivaris als verschillende medewerkers is aangedragen, is het gebruik van applicaties. Zorg ervoor dat voor de aanschaf van nieuwe applicaties wordt nagegaan in hoeverre deze voldoen aan de eisen van de AVG. En zorg ervoor dat de medewerkers in de zaaksystemen niet meer toegang hebben tot gegevens dan zij nodig hebben.

Het projectteam leertuinen privacy heeft verschillende relevante knelpunten gesignaleerd die ook in de interviews zijn bevestigd. Knelpunten die de gemeente mogelijk op korte termijn kan adresseren zijn het creëren van de mogelijkheid om persoonlijke aantekeningen te maken in de gebruikte zaaksystemen, en intern het gesprek voeren over het delen van gegevens met derden (samenwerkingspartners) zodat hier meer duidelijkheid over- en comfort bij ontstaat.

Maak van de FG een echt onafhankelijke functionaris

Volgens de AVG moet de FG zijn of haar taken vanuit een onafhankelijke rol kunnen uitvoeren. De FG moet immers ook toezicht houden en dan niet 'het eigen vlees' hoeven te keuren. In Zoetermeer is de

FG-functie maar enkele uren in de week ingevuld, en wordt deze functie vervuld door de teammanager JaBo. Op dit moment is de FG voornamelijk gericht op compliance en het faciliteren van medewerkers. De FG stelt ook geen eigen rapportages op over de mate waarin de gemeente voldoet aan de AVG-eisen. Aanbevolen wordt om de FG veel meer in positie te brengen en vanuit een onafhankelijke positie onderzoek te laten doen naar de wijze waarop de gemeente invulling geeft aan de AVG-taken, hierover te rapporteren en aanbevelingen te doen. Dat is mogelijk door de FG een functionaris te laten zijn die, anders dan nu het geval is, geen andere taken dan de FG-taken heeft. En die substantieel meer - en bij voorkeur, net zoals in andere gemeenten met een gelijk inwoneraantal, fulltime - ruimte heeft om de vanuit de AVG vereiste taken te vervullen. Daarbij is de aanbeveling om de FG onafhankelijk te positioneren onder concern control.

Zorg voor meer capaciteit voor de PO

De PO vormt voor veel medewerkers een belangrijk aanspreekpunt als het gaat om vragen over de AVG. Hierdoor is de PO relatief veel tijd kwijt aan het beantwoorden van vragen en is er minder tijd voor de meer beleidsmatige taken. Het verder uitbreiden van het privacynetwerk, zoals het voornemen is, moet zorgen voor meer aanspreekpunten binnen de gemeente als het gaat om vragen over de AVG. Het uitbreiden en verder implementeren van het privacynetwerk is daarom een goed voornemen.

De huidige bezetting van de PO binnen de gemeente is momenteel 35 uur (27 uur en 8 uur). Vergelijking van deze bezetting met de PO omvang in vergelijkbare gemeenten laat zien dat daar meer capaciteit voor de PO beschikbaar is. Zo hebben de gemeenten Leiden, Leeuwarden en Ede respectievelijk 2,3 fte (met streven naar 3 fte), 2 fte (waarvan 1 fte juridisch ingestoken en 1 fte managementgericht) en 0,89 fte aan fte. Hoewel het niet altijd eenvoudig is om deze capaciteit uit te breiden, verdient het aanbeveling om meer capaciteit voor de PO te realiseren.

Ga aan de slag met cyclisch monitoren en rapporteren

Momenteel wordt in de organisatie vooral gefocust op compliance van de AVG-richtlijnen. Er is een start gemaakt met monitoring en rapportage door het IPI-team die periodiek bevindingen presenteert aan directie en management en prioriteiten voor de komende periode identificeert. Er kan echter meer gedaan worden op het gebied van structurele, cyclische monitoring en rapportage. Op het gebied van informatiebeheer worden al jaarlijkse verslagen met relevante bevindingen en aanbevelingen opgesteld door de gemeentearchivaris. Put hier inspiratie uit voor de domeinen informatiebeveiliging en privacy. Stel periodiek (bijvoorbeeld ieder halfjaar) schriftelijke rapportages op met relevante bevindingen over waar het goed gaat en waar zich risico's bevinden, en formuleer naar aanleiding daarvan aanbevelingen voor de komende periode. Op basis hiervan kunnen in overleg met directie en management prioriteiten met concrete doelstellingen worden geformuleerd. Zo ontstaat er een programmatische cyclus van plannen, uitvoeren, controleren en bijstellen. Door op deze manier te werken kan er gerichter en zorgvuldiger worden ingegrepen bij risico's. Overweeg hierbij om het IPI-team periodiek langs te laten komen bij afdelings- of teamoverleggen om de bevindingen en aanbevelingen te bespreken en waar mogelijk in gezamenlijkheid met de teams te vertalen in concrete acties.

Blijf regelmatig (verplichte) workshops en trainingen organiseren

De gemeente Zoetermeer doet al veel op het gebied van training en faciliteren van medewerkers. Tegelijkertijd blijkt uit dit onderzoek dat het structurele kennisniveau over de AVG en de bijbehorende

interne procedures punt van aandacht is. Er zijn verschillende acties mogelijk om dit structurele kennisniveau te versterken. Zorg er in de eerste plaats voor dat nieuwe medewerkers zo snel mogelijk de basiskennis van de AVG en relevante interne procedures beheersen en beloon hen wanneer dit het geval is, bijvoorbeeld met een intern AVG-diploma. Ga daarnaast werken met periodiek terugkerende kennistrajecten en 'opfrismomenten' voor medewerkers die al langer met de AVG werken. Door interne leer- en kennistrajecten een verplicht karakter te geven, kan beter worden voorkomen dat kennis vervliegt en zo wordt er een natuurlijk moment gecreëerd waarop kan worden gespard over de AVG en waar vragen kunnen worden gesteld. Het resultaat van zo'n kennissessie zou verwerkt kunnen worden in een Q en A over regelmatig voorkomende dilemma's, die daarna in de organisatie kan worden gedeeld. Overweeg daarnaast om op meerdere momenten in het jaar een datalek of gegevensincident te simuleren aan de hand van scenario's uit de praktijk. Hierdoor kan geoefend worden met opgestelde procedures en werkwijzen en wordt de praktijkkennis van medewerkers vergroot, ook wanneer zij bijvoorbeeld nog niet met een datalek van doen hebben gehad.

Anticipeer op wettelijke ontwikkelingen en zet waar mogelijk alvast acties op

Eerder in deze rapportage is ingegaan op de verschillende toekomstige wetten en andere ontwikkelingen die relevant zijn voor gegevensbescherming en privacy. Er is bij veel van deze ontwikkelingen nog veel onduidelijk. Bij de wetsvoorstellen is vaak pas bij de definitieve vaststelling duidelijk wat de implicaties voor Zoetermeer zullen zijn. Tegelijkertijd kan de gemeente alvast anticiperen op deze wettelijke ontwikkelingen door de behandeling van de wetsvoorstellen te monitoren en om, zoals bij het wetsvoorstel Wams, een bijdrage te leveren aan de maatschappelijke discussie hierover. Zodra de kaders van nieuwe wet- en regelgeving daadwerkelijk vaststaan, is het verstandig om te starten met het organiseren van informatiesessies en bijscholing voor de betrokken medewerkers. Het is daarnaast de overweging waard om een risicoparagraaf in de begroting op te nemen, waarin wordt ingegaan op mogelijke wettelijke veranderingen.

Bij enkele toekomstige ontwikkelingen kan de gemeente wel alvast van start gaan met enkele concrete (voorbereidende) acties. Schroom ook niet om partijen als de AP of de Informatiebeveiligingsdienst te vragen de gemeente hierbij van advies te voorzien. In lijn met de aankondiging van de AP dat gemeenten meer aandacht moeten hebben voor risicomanagement met privacy kan de gemeente vast voorbereidende werkzaamheden verrichten in het ontwikkelen van cyclisch risicomanagement, zoals de Informatiebeveiligingsdienst adviseert. Zoals eerder genoemd werkt de gemeente daarnaast sinds enkele jaren met verschillende slimme technieken en heeft de ambitie om een Smart City te worden. Het advies van de AP is om speciaal voor deze ambitie een beleid vast te stellen. Dit beleid moet handvatten bieden voor het werken met Smart City-toepassingen. Door als gemeente tijdig beleid vast te stellen kan er een betere borging van het fundamentele belang van privacy worden vormgegeven waarin de kaders voor de praktijk duidelijk zijn.

Bijlage 1. Bronnen

Tabel 1: Lijst met geïnterviewden

Functie	Datum
Gemeentesecretaris	1-07-2022
CISO	26-04-2022
Privacy Officer	28-04-2022
Concerncontroller	4-07-2022
Functionaris gegevensbescherming	26-04-2022
Gemeentearchivaris	28-04-2022
Adviseur informatiebeveiliging	27-06-2022
Adviseur informatiebeveiliging	27-06-2022
Afdelingshoofd inkomen en sociale zekerheid	7-07-2022
Afdelingshoofd zorg, jeugd en gezinshulp	7-07-2022
Teammanager openbare orde en veiligheid	7-07-2022
Afdelingshoofd publieksplein	7-07-2022

Voor de geraadpleegde schriftelijke bronnen verwijzen wij naar de voetnoten in de rapportage.

Bijlage 2. Analysekader

Voor het beantwoorden van de onderzoeksvragen wordt gebruik gemaakt van een analysekader. Dit analysekader is gebaseerd op de Privacy Baseline CIP[125] en op eerdere analysekaders bij onderzoeken naar de implementatie van de AVG.

Deelvraag	Analysekader
1. Zijn binnen de organisatie voldoende waarborgen aanwezig die voorzien in een betrouwbare bescherming van persoonsgegevens van betrokkenen, conform de AVG?	- De gemeente heeft een informatieveiligheidsbeleid en een privacybeleid vastgesteld, waarin is vastgelegd hoe invulling wordt gegeven aan de AVG. - De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen zijn door de organisatie vastgelegd en vastgesteld. - Er zijn vaste procedures en registers voor de verwerking van persoonsgegevens vastgesteld. - Er vindt periodiek evaluatie van de huidige werkwijze plaats en hierover wordt gerapporteerd. De gemeente hanteert hierbij een gecertificeerd toetsingskader als de privacy baseline van het CIP.
2. Is bij incidenten (datalekken) sprake van zorgvuldige afhandeling conform de AVG?	- Bij datalekken rapporteert de gemeente conform de meldplicht datalekken aan de autoriteit persoonsgegevens, documenteert de inbreuk en informeert de betrokken personen.
3. Worden de medewerkers bij de uitvoering van hun taken voldoende gefaciliteerd in het efficiënt en effectief werken conform de AVG?	- Er zijn richtlijnen, handleidingen of vergelijkbare kaders over werken conform de AVG vastgelegd die medewerkers kunnen raadplegen. - Er zijn vaste functionarissen die toezien op het werken conform de AVG door medewerkers, en die door medewerkers geraadpleegd kunnen worden.
4. Hoe wordt ervoor gezorgd dat binnen de organisatie structureel voldoende kennis en kunde aanwezig is op het gebied van gegevensbescherming?	- Er is sprake van periodieke en incidentele (bij)scholing en training van medewerkers in de uitvoering van hun taken conform de AVG.
5. Hoe wordt ervoor gezorgd dat medewerkers gegevensbescherming als onderdeel van hun werkzaamheden zien en niet als belemmering, in vervolg op de Leertuinen privacy voor het Sociaal Domein?	- Geen kader, dit is een beschrijvende vraag
6. Welke verbeterpunten zijn er ten aanzien van bovenstaande vragen?	- Geen kader, dit is een beschrijvende vraag
7. Is de huidige organisatie voldoende toegerust om de toekomstige ontwikkelingen (zoals aankomende wet- en regelgeving, nieuwe technologieën, etc.) aan te kunnen en zijn er eventuele verbeterpunten? Wat is daar eventueel nog voor benodigd (qua organisatie, middelen e.d.)?	- De organisatie anticipeert aan de hand van vastgestelde kaders op toekomstige ontwikkelingen op het gebied van informatieveiligheid en privacybescherming.

[125] Centrum Informatiebeveiliging en Privacybescherming (2020). De Privacy Baseline: https://www.cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/privacy-bescherming/.

Bijlage 3. Digitale Enquête

Introductievraag:

Ik werk voor de afdeling: (vier opties)

- Sociaal domein
- Veiligheidsdomein
- Burgerzaken
- Geen van allen

KENNIS VAN DE AVG

De volgende vragen gaan over de AVG

Vraag 1:

d.vandijk@neckervannaem.nl is een persoonsgegeven

Kies één van de volgende opties

Drie opties:

Waar, niet waar of weet ik niet

Vraag 2:

Gegevens waaruit iemands ras of etniciteit blijkt is een persoonsgegeven

Kies één van de volgende opties

Drie opties:

Waar, niet waar of weet ik niet

Vraag 3:

De AVG is niet van toepassing wanneer persoonsgegevens via de mail worden uitgewisseld.

Kies één van de volgende opties

Drie opties:

Waar, niet waar of weet ik niet

Vraag 4:

Wanneer een inwoner een mail stuurt met het verzoek om al zijn persoonsgegevens te verwijderen, moet hier altijd aan worden voldaan.

Kies één van de volgende opties

Drie opties:

Waar, niet waar of weet ik niet

Vraag 5:

Wanneer ik voor mijn werk een mail verstuur met persoonsgegevens naar een verkeerde ontvanger moet ik dat *altijd* melden.

Kies één van de volgende opties

Drie opties:

Waar, niet waar of weet ik niet

TOERUSTING AVG

Vraag 6:
Als medewerker van de gemeente heb ik voldoende kennis om op de juiste wijze met persoonsgegevens te werken.

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
-
-
-
-
-
- helemaal eens
- weet ik niet/ geen mening

Vraag 7:
Als medewerker van de gemeente is het voor mij voldoende duidelijk wie er verantwoordelijk is voor de juiste omgang met persoonsgegevens

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
-
-
-

-
-
- helemaal eens
- weet ik niet/ geen mening

Vraag 8:
Als ik vragen heb over de verwerking van persoonsgegevens weet ik bij wie ik terecht kan.

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
-
-
-
-
-
- helemaal eens
- weet ik niet/ geen mening

Vraag 9:
Als medewerker van de gemeente verwerk ik persoonsgegevens zonder dat ik weet of dat wel mag

Kies op de schuifbalk de positie die het best bij uw mening past.

- Heel vaak
-
-
-
-
-
- helemaal nooit
- weet ik niet/ geen mening

Vraag 10a:
Mijn manager heeft voldoende aandacht voor het werken met de AVG

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
-
-
-

- helemaal eens
- weet ik niet/ geen mening

Vraag 10b:
Wilt u uw antwoord toelichten?

[tekstvak]

Vraag 11:
Werken volgens de regels van de AVG is

Kies op de schuifbalk de positie die het best bij uw mening past.

- Zeer lastig
- Zeer eenvoudig
- weet ik niet/ geen mening

UITVOERING

Vraag 12:
Als ik vragen heb over de verwerking van persoonsgegevens dan ga ik naar: een collega, mijn teammanager/unitcoördinator, mijn afdelingshoofd, de Privacy Officer (Carlijn Dohmen), de Functionaris Gegevensbescherming (Angelique Schepers) of de CISO (Susan Ligtenberg)

Kies één of meerdere van de opties

*6 opties: (**niet** mutually exclusive)*

een collega; mijn teammanager of unitcoördinator; mijn afdelingshoofd; de Privacy Officer (Carlijn Dohmen); de Functionaris Gegevensbescherming (Angelique Schepers) of de CISO (Susan Ligtenberg)

Vraag 13:
Als medewerker van de gemeente weet ik wat ik moet doen op het moment dat er mogelijk sprake is van een datalek

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
-
-
-
-
-
- helemaal eens
- weet ik niet/ geen mening

Vraag 14a:
Wat de gemeente van mij als medewerker aan inzet vraagt als het gaat om werken met de AVG is haalbaar

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
-
-
-
-
-
- helemaal eens
- weet ik niet/ geen mening

Vraag 14b:
Wilt u uw antwoord toelichten?

[tekstvak]

Vraag 15a:
De huidige applicaties en programma's maken het werken volgens de AVG:

Kies op de schuifbalk de positie die het best bij uw mening past.

- Moeilijk
-

- Eenvoudig
- weet ik niet/ geen mening

Vraag 15b:
Wilt u uw antwoord toelichten?

[tekstvak]

SUCCES- EN VERBETERPUNTEN

Vraag 16a

Wat ervaart u als positief in de gemeentelijke organisatie, uw afdeling, uw team of unit als het gaat om het werken met de AVG?

[tekstvak]

Vraag 16b

Wat ziet u als verbeterpunten voor de gemeentelijke organisatie, uw afdeling, uw team of unit als het gaat om het werken met de AVG?

[tekstvak]

Vraag 17a: (alleen als antwoord bij introductievraag 'Sociaal domein' is)
Het project leertuinen privacy heeft mij geholpen bij het werken met de AVG

Kies op de schuifbalk de positie die het best bij uw mening past.

- helemaal oneens
- helemaal eens

- weet ik niet/ geen mening

Vraag 17b:
Wilt u uw antwoord toelichten?

[tekstvak]

Eindscherm

Hartelijk dank voor het invullen van de vragenlijst.

Bijlage 4. Toerusting van medewerkers

Dit overzicht toont documentatie, berichtgeving en andere informatie die binnen de gemeente Zoetermeer gehanteerd wordt om medewerkers toe te rusten over de AVG. Het gaat hierbij om de door de onderzoekers ontvangen documenten. Dit overzicht behoeft daarmee niet volledig te zijn.

- AVG stroomschema delen gegevens (g.d.);
- Inzage en protocollering BRP (g.d.);
- Nieuwe werkwijze gegevensverwerking en informatiedeling gemeente Zoetermeer (g.d.);
- Presentatie persoonsgegevens en de Wmo (g.d.);
- Stroomschema delen informatie met derden (g.d.);
- Procedure onjuiste verstrekkingen (2019);
- Bericht ‘’Moet ik een DPIA doen?’’ (2020);
- Beschrijving proces datalekken melden (2020);
- Format DPIA (2020);
- Handreiking inzageverzoeken AVG (2020);
- Model verwerkersovereenkomst (2020);
- Nieuwsbrieven sociaal domein (periode 2020-2021);
- VNG-nota AVG Privacy in het Sociaal Domein (2020);
- Memo veilig e-mailen met Office365 (2021);
- Privacy- en beheerregeling BRP (2021);
- Procedure incidentenmelding BRP (2021);
- BRP-reglement (2022);
- Diverse berichten Privacy Officer, o.a. over het herkennen van datalekken, databescherming, phishing, workshops informatiebeveiliging en privacy, (2022);
- Teampagina IPI (2022);