Bescherming persoonsgegevens

Rekenkameronderzoek

Rekenkamer Amersfoort

Mei 2021

Colofon

Uitgavedatum: 11 mei 2021

Rekenkamer Amersfoort
Stadhuisplein 5
3811 LM Amersfoort
033 469 43 12
rekenkamer@amersfoort.nl
www.amersfoort.nl/rekenkamer

PBLQ
Muzenstraat 120
2511 WB Den Haag
070 3763636
info@pblq.nl
www.pblq.nl

Inhoud

HOOFDSTUK 1 INLEIDING

1.1 Inleiding

De bescherming van persoonsgegevens is een belangrijk thema binnen gemeenten. Steeds meer wordt er met grote hoeveelheden data gewerkt, waar ook persoonsgegevens tussen zitten. Ook de toepassing van nieuwe technologieën maakt het thema blijvend relevant. De bescherming van persoonsgegevens is een belangrijk onderdeel van integere dienstverlening. Daarvoor moeten medewerkers de regels kennen, de betekenis daarvan hebben geïnternaliseerd, deze weten te vertalen naar processen, organisatie en techniek, en naar de wijze waarop je de inwoner bejegent. Inwoners hebben er recht op dat hun individuele rechten worden gerespecteerd, dat gegevens van hen worden gebruikt voor de doelen waarvoor ze zijn verstrekt of geregistreerd, en dat zij inzicht hebben in het gebruik van hun persoonsgegevens.
De rekenkamer wil graag inzicht verkrijgen in de bescherming van persoonsgegevens bij de gemeente Amersfoort en de toepassing van de Algemene verordening gegevensbescherming (AVG). In dat kader is PBLQ gevraagd onderzoek te doen naar de bescherming van persoonsgegevens.

1.2 Doel en vraagstelling

Het doel van het onderzoek is inzicht verkrijgen in de bescherming van privacy van de Amersfoortse inwoners. In het onderzoek is er in het bijzonder aandacht voor de AVG en de rol van derden.

De centrale onderzoeksvraag van het rekenkameronderzoek luidt:

Hoe wordt de privacy van de Amersfoortse inwoners beschermd en wordt er adequaat gebruik gemaakt van de AVG, toegespitst op derden aan wie de uitvoering van beleid is uitbesteed, of met wie anderszins persoonsgegevens worden gedeeld?

Om de centrale onderzoeksvraag te beantwoorden zijn deelvragen geformuleerd. Deze zijn te vinden in bijlage 1.

1.3 Normenkader

De bevindingen van het onderzoek zijn getoetst aan een normenkader dat hierna in een verkorte versie is opgenomen in combinatie met de onderzoeksthema's, deelvragen en methoden van onderzoek. Het uitgebreide normenkader is te vinden in bijlage 3.

Onderzoeksthema	Deelvraag	Normen
Beleid, Governance en Toezicht	1, 2, 4, 10	▪ AVG-conforme beleidskaders, regels en richtlijnen. ▪ Uitgangspunten vastgesteld in gemeenteraad. ▪ In beleidskaders wordt ingegaan op juridische aspecten, de vertaling naar beleidskaders, organisatie, taken en verantwoordelijkheden. ▪ Toezicht is vastgelegd in een controleplan. ▪ In bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan bescherming van persoonsgegevens. ▪ Er is een procedure voor datalekken. ▪ Duidelijkheid over informering raad over privacybeleid.
Praktijk, Leer- en verbetercyclus, incidenten en informatieverstrekking	2, 3, 7, 8, 10	▪ In de praktijk wordt conform het beleid gehandeld. ▪ Verwerkersovereenkomsten worden gemonitord en geverifieerd. ▪ Er is een leer- verbetercyclus (uitgevoerd). ▪ Er is een routine voor meten en verbeteren. ▪ Er is conform de datalekprocedure gehandeld. ▪ Inwoners worden op een toegankelijke en begrijpelijke wijze geïnformeerd. ▪ De gemeente verschaft schriftelijk en mondeling begrijpelijke informatie over persoonsgegevens. ▪ De raad wordt conform beleid geïnformeerd. ▪ Informatieverstrekking naar de raad biedt voldoende mogelijkheden voor sturing en controle.
Dagelijks functioneren, derden	5, 6, 9	▪ Medewerkers zijn bekend met het privacybeleid. ▪ In dagelijks functioneren handelen medewerkers naar het beleid. ▪ Medewerkers zijn proactief en transparant naar inwoners. ▪ Medewerkers bewaken actief dat ketenpartners zich conformeren aan regels, standaarden en procedures.

De resultaten van het onderzoek worden afgezet tegen deze normen en op de volgende wijze weergegeven:

+	De praktijk komt (nagenoeg) volledig overeen met de norm.
+/-	De praktijk komt gedeeltelijk overeen met de norm.
-	De praktijk komt niet of onvoldoende overeen met de norm.

1.4 Onderzoeksopzet

Om de centrale onderzoeksvraag en de deelvragen te beantwoorden zijn verschillende onderzoeksmethoden ingezet. Aan het begin van het onderzoek zijn diverse relevante documenten geraadpleegd. Daarnaast zijn interviews afgenomen bij verschillende medewerkers van de gemeente. In twee workshops, met een aantal medewerkers, is de omgang met persoonsgegevens in het kader van de Wet verplichte geestelijke gezondheidszorg (Wvggz) en privacyoverwegingen bij de inzet van algoritmen onderzocht. De workshops hadden het doel inzicht te verkrijgen in de cultuur van de

organisatie en hoe er in de dagelijkse praktijk met privacydilemma's wordt omgegaan. Om een goede indruk te krijgen van het perspectief van inwoners is er in het kader van dit onderzoek gesproken met organen waarin inwoners zich hebben verenigd. Tot slot is er een raadsessie gehouden om de input van de raad op te halen. Het conceptrapport is beschikbaar gesteld voor ambtelijk wederhoor. Voor meer informatie over deze onderzoeksmethoden wordt verwezen naar bijlage 2 met de onderzoeksopzet en verantwoording.

1.5 Scope en afgrenzing

Het onderzoek concentreert zich op het door de gemeente gevoerde beleid in de huidige collegeperiode, gestart in 2018 tot en met januari 2021. Ontvangen documentatie is tot en met maart 2021 meegenomen. Daar waar uitgangspunten voor het beleid in eerdere collegeperioden zijn vastgelegd, zijn deze in het onderzoek betrokken.

1.6 Indeling rapport

Dit rapport is als volgt ingedeeld. In hoofdstuk 2 worden de deelvragen beantwoord met behulp van het normenkader. In hoofdstuk 3 worden de belangrijkste conclusies uiteengezet en de hoofdvraag beantwoord. In hoofdstuk 4 worden de aanbevelingen beschreven. Een uitgebreide toelichting van de deelvragen, het normenkader, de onderzoeksmethoden, de onderbouwing en de interviewlijst staan in de bijlagen.

HOOFDSTUK 2 BEANTWOORDING DEELVRAGEN

In dit hoofdstuk worden de deelvragen beantwoord. De belangrijkste bevindingen worden beschreven en getoetst aan het normenkader. Een nadere onderbouwing van de onderzoeksbevindingen staat in bijlage 4.

2.1 Het gemeentelijk beleid

Deelvraag 1 Hoe biedt de gemeente Amersfoort bescherming aan inwoners als het gaat om privacy?
Deelvraag 2 Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid betrokken geweest?
Deelvraag 4 Wat heeft de FG (functionaris gegevensbescherming) nodig van de gemeente om haar werk te kunnen doen? In hoeverre is dit in Amersfoort geregeld?
Deelvraag 10 Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?

Normen voor deelvragen 1, 2, 4 en 10	**Beoordeling**
AVG-conforme beleidskaders, regels en richtlijnen.	+
De algemene uitgangspunten en kaders zijn besproken in en vastgesteld door de gemeenteraad.	+
In de verschillende beleidskaders wordt ingegaan op: ○ Juridische aspecten op basis van de AVG en de materie wetten. ○ Vertaling naar de beleidskaders privacy. ○ Organisatie, taken en verantwoordelijkheden.	+
Er is een procedure vastgelegd hoe de gemeente handelt in het geval van geconstateerde ‘datalekken’.	+

De gemeente Amersfoort beschermt de privacy van inwoners door middel van het opstellen van beleid, het inzetten op een goede naleving van het beleid en het communiceren van dit beleid naar inwoners. Het privacybeleid wordt door de afdeling Juridische Dienstverlening en Advies (JDA) opgesteld conform de AVG en op de gemeente toepasselijke richtlijnen zoals de BIO[1]. Dit blijkt uit de aangeleverde documentatie.[2] De uitgangspunten voor het beleid zijn in de gemeenteraad besproken en vastgesteld. In beleidskaders wordt ingegaan op de juridische aspecten en de vertaling van de AVG naar andere beleidskaders. De governance, waaronder de rollen, taken en verantwoordelijkheden, is in een apart document uitgebreid toegelicht. Het beleid wordt door de hele organisatie uitgevoerd. Er is een procedure voor datalekken.[3] Het aantal beveiligingsincidenten en datalekken wordt

[1] Baseline Informatiebeveiliging Overheid

[2] In het bijzonder ‘Jaarplan Privacy 2020’, ‘Privacy Governance 2020 v. 1.0’, ‘Jaarstukken 2019’, ‘Informatiebeveiligingsbeleid 2019-2022’, ‘Privacyverklaring gemeente Amersfoort’, ‘Programma standaard VWO, rapportage december 2019’ en verschillende protocollen zoals ‘Protocol Afhandelteam Incidentenmeldingen’ en het ‘Protocol Veilig delen van informatie’

[3] ‘Protocol Afhandelteam Incidentenmeldingen’ en ‘Werkwijze Afhandelteam Incidentenmeldingen’

geregistreerd. De Functionaris Gegevensbescherming (FG) rapporteert hier elk kwartaal over aan de kerngroep privacy en informatieveiligheid en de directie. Algemene informatie hierover wordt ook opgenomen in het gemeentelijk jaarverslag, en maakt als zodanig deel uit van de P&C cyclus.[4]

Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan.	+
In bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.	+

Het toezicht op het gebruik van persoonsgegevens ligt primair bij de FG. De FG kan adequaat toezicht houden en doet hier in principe jaarlijks verslag van. Het jaarverslag over 2019 en 2020 is in maart 2021 opgesteld. De FG moet haar werk onafhankelijk kunnen doen. Zij moet zich dan ook in haar hoedanigheid vrij voelen om ongevraagd en gevraagd advies uit te brengen. Ook moet ze toegang hebben tot de stukken en contact kunnen leggen met relevante personen binnen de gemeente.

Formeel hoort de FG bij de afdeling JDA, maar in praktijk is hier geen sprake van enige hiërarchische relatie. De FG geeft ongevraagd advies en sluit aan bij overleggen op het gebied van privacy, zoals het sleutelpersonenoverleg. Ze kan naar eigen inzicht aangeven wanneer dit relevant is en wordt hierin gefaciliteerd door de ambtelijke organisatie. Ze heeft regelmatig contact met andere personen in de organisatie met een toezichtsfunctie, zoals de concern information security officer (CISO), de archivaris en de concerncontroller.

Deze vier ‘toezichthouders’ spreken elkaar regelmatig in het zogenaamde ‘vierhoeksoverleg’. Hierin wordt gekeken waar overlap ligt tussen de thema’s waarop zij toezicht houden en of zij risico’s hebben geconstateerd die de thema’s van de andere toezichthouders ook raken. Ze letten ook op of er opvolging is gegeven aan eerder gestelde maatregelen, bijvoorbeeld maatregelen die uit DPIA’s[5] naar voren zijn gekomen. In de loop van 2020 kwamen zij tot de conclusie dat er zogeheten ‘tooling’ nodig is om de risico’s en maatregelen, die onder andere in de DPIA’s zijn gesignaleerd, in de gaten te kunnen houden, waarna deze is aangeschaft. Dit betreft een softwareapplicatie waarin normenkaders, risico’s, audits en ENSIA-controles[6] worden samengebracht. De software biedt dan ook de mogelijkheid om vervolgactiviteiten op eerder gebleken tekortkomingen en aandachtspunten te volgen.

Er is vastgelegd hoe de raad wordt geïnformeerd over (de ontwikkelingen in) het privacybeleid.	+
Uitgangspunten worden vastgesteld in de gemeenteraad.	+
In de praktijk wordt de raad conform de overeengekomen systematiek geïnformeerd over de ontwikkelingen in het privacybeleid.	+
De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.	+

[4] K. Eefsting en J. Roest, ‘Jaarverslag Functionaris Gegevensbescherming 2019-2020’, februari 2021

[5] Data Protection Impact Assessment is een door de AVG verplicht onderzoek waarin risico’s en beoogde (mitigerende) maatregelen op het gebied van privacy in kaart worden gebracht.

[6] ENSIA staat voor Eenduidige Normatiek Single Information Audit. Bij een ENSIA-audit legt een gemeente in één keer verantwoording af over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO.

Ten behoeve van dit onderzoek is er met de raadsleden gesproken over hun rol en informatiepositie bij het privacybeleid. In deze sessie bleek dat de raadsleden bewust en actief bezig zijn met het onderwerp privacy. Datalekken geven wat hen betreft met name aanleiding om breder na te denken over hoe de bewustwording rondom privacy blijvend kan worden versterkt. De raad denkt op dit moment na over verdere uitdagingen omtrent privacy. Raadsleden gaven daarbij aan dat goede privacybescherming als een onderdeel van de gemeentelijke dienstverlening wordt gezien en rekenen erop dat de gemeente ook op dat aspect de dienstverlening op orde heeft. De raad wil hierop sturen en wil hier ook over geïnformeerd worden. In de raad wordt er met interesse gekeken naar informatiebeveiliging als belangrijke bouwsteen voor een goede omgang met gegevens. De raad vindt het belangrijk dat de gemeente ook op dit vlak aandacht besteedt aan de steeds geraffineerdere bedreigingen van de systemen.

Door raadsleden wordt verschillend gedacht over hoe zij geïnformeerd willen worden over privacy. Sommigen zijn van mening dat het beter is om per thema over privacy te worden geïnformeerd, omdat het een organisatiebreed vraagstuk is. Anderen zijn tevreden met hoe het nu gaat.

De raad kan zijn controlerende taken het beste uitvoeren als hij een beeld krijgt van zaken waar de gemeente tegenaan loopt. Hiervoor is informatie nodig over de ontwikkelingen rondom het privacy- en beveiligingsbeleid. Deze informatie wordt met de raad gedeeld. Over het algemeen zouden verschillende raadsleden nog meer informatie willen ontvangen over de hiaten en dilemma's die de gemeente tegenkomt.

De gemeenteraad wordt van het privacybeleid op de hoogte gehouden via de reguliere P&C-cyclus, jaarstukken, jaarrekening, FG-verslagen en presentaties. Voorheen is de raad over het privacybeleid geïnformeerd via raadsinformatiebrieven. Dat zij op de hoogte worden gehouden blijkt uit verschillende documenten[7]. Bij de toelichting van de privacy governance wordt toegelicht hoe de raad dient geïnformeerd te worden over het privacybeleid.[8] De raad is actief betrokken bij de uitgangspunten waarop het huidige privacybeleid nog steeds is gestoeld.[9] De raad wordt direct geïnformeerd bij ernstige datalekken. Bij minder grote datalekken wordt de raad middels reguliere bijeenkomsten en stukken geïnformeerd.

2.2 Uitvoering van het gemeentelijk beleid

Deze paragraaf richt zich op de uitvoering van het gemeentelijk beleid, en heeft daarmee betrekking op de volgende onderzoeksvragen:

[7] 'Jaarplan Privacy 2020', 'Privacy Governance 2020 v. 1.0', 'Jaarstukken 2019',

[8] 'Privacy governance 2020, versie 1.0'

[9] 'Uitgangspuntennotitie ten behoeve van de ronde op 8 oktober 2019'. Dezelfde uitgangspunten komen terug in het jaarplan Privacy 2020

Deelvraag 2 Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid betrokken geweest?
Deelvraag 3 Waar knelt de AVG, waar zitten beperkingen en risico's?
Deelvraag 7 Wat zijn ongewenste neveneffecten van de AVG: gebeurt het bijvoorbeeld dat informatie niet wordt gedeeld met een (oneigenlijk) beroep op de AVG?
Deelvraag 8 Welke privacyschendingen zijn er bij de gemeente en de samenwerkingspartners sinds de invoering van de AVG geweest/gemeld, hoe is de gemeente daarmee omgegaan?
Deelvraag 10 Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?

Normen voor deelvragen 2, 3, 7, 8, 10	**Beoordeling**
In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.	+

Er wordt in praktijk conform de AVG gehandeld. De AVG wordt over het algemeen niet als onnodig knellend ervaren. Uit de gesprekken en de workshops is gebleken dat werknemers handelen in overeenstemming met het privacybeleid en dat het privacybeleid is verweven in de cultuur van de organisatie.

De AVG stelt (noodzakelijke) beperkingen aan in hoeverre de gemeente persoonsgegevens mag verwerken. Deze beperkingen zijn beschreven in het privacybeleid en uitgewerkt in een e-learning module[10]. Medewerkers leren wanneer ze gegevens mogen verwerken en als ze deze verwerken hoe zij hiermee om moeten gaan. De AVG stelt eisen aan de inrichting van systemen en vereist soms dat bedrijfsprocessen anders moeten worden ingericht, ook met betrekking tot de snelheid van de bedrijfsprocessen.

Over het algemeen wordt privacy niet als beperkend ervaren. In het veiligheidsdomein wordt de AVG soms als beperkend ervaren, bijvoorbeeld bij het delen of ontvangen van informatie in de samenwerking met derden. Soms is het onduidelijk hoe bepaalde wetten met elkaar stroken, bijvoorbeeld de AVG en de Wvggz. In zo'n geval wordt er altijd gekeken naar een oplossing: wanneer iets niet kan door eisen uit de AVG houdt men zich hieraan. Door onduidelijkheden in wetgeving moeten medewerkers in individuele gevallen soms een afweging maken tussen verschillende belangen (denk aan belangen van inwoners ten opzichte van een algemeen belang van de overheid) op welke manier de waarborging van de bescherming van persoonsgegevens moet worden meegenomen. Bij nieuwe wetgeving is er meestal nog geen gestolde (juridische) praktijk. Bij de specifieke toevoeging van die wetgeving is het daarom lastig exact te weten hoe een bepaalde toepassing moet plaatsvinden. Dit is een te verwachten effect bij nieuwe wetgeving.

[10] Deze module wordt op het moment van het schrijven van dit rapport vernieuwd.

Risico's

Voordat een verwerking met persoonsgegevens start, worden privacyrisico's systematisch in kaart gebracht door middel van DPIA's. Deze DPIA's worden regelmatig uitgevoerd en wanneer nodig geëvalueerd, bijvoorbeeld omdat er relevante nieuwe ontwikkelingen zijn. Om te bepalen of een DPIA moet worden uitgevoerd, is er een Quickscan opgesteld. Bij het uitvoeren van de DPIA zelf kan er een leidraad worden gevolgd.[11] DPIA's zijn daarmee relevant voor de beantwoording van deelvraag 3.
De jaarlijkse ENSIA-audit[12] is een belangrijk instrument voor de verantwoording over informatiebeveiliging. Deze audit, een self-assessment, wordt onder verantwoordelijkheid van een afdelingsmanager per afdeling die specifiek binnen de BIO een plek inneemt, uitgevoerd door een beveiligingsbeheerder (een aangewezen contactpersoon per afdeling). Er is een Information Security Management System (ISMS) aangeschaft voor de beheersings- en verbetercyclus voor informatiebeveiliging. In de ISMS-tooling kunnen beveiligingsbeheerders informatie gerelateerd aan beveiligingsnormen vastleggen. De tooling moet bijdragen aan de eenduidigheid in de genomen maatregelen en het aantoonbaar maken of er aan een norm wordt voldaan. De tooling helpt overzicht te krijgen op of maatregelen zijn doorgevoerd in werkprocessen, op de verdeling van verantwoordelijkheden en op maatregelen ter verbetering van de beveiliging van informatiesystemen.

Afspraken in verwerkersovereenkomsten met derden worden door de gemeente gemonitord en geverifieerd.	-/+

De gemeente heeft haar monitoring op de afspraken met derden in de afgelopen jaren verbeterd. Bij de uitwisseling van persoonsgegevens met derden vereist de AVG dat hier duidelijke afspraken over moeten worden gemaakt.[13]

In 2019 is een project afgerond dat als doel had een goed overzicht te verkrijgen over alle verwerkersovereenkomsten of waar deze overeenkomsten er hadden moeten zijn. De aanleiding was dat het overzicht op de verwerkersovereenkomsten ontbrak. Tijdens het project zijn bestaande verwerkersovereenkomsten bekeken en waar mogelijk verlengd. Verder zijn de ontbrekende verwerkersovereenkomsten toegevoegd. Alle verwerkersovereenkomsten zijn, waar mogelijk, ook aangepast aan de richtlijnen en modelverwerkersovereenkomst van de VNG. Op verschillende punten zijn verwerkersovereenkomsten uitgebreid. Zo is er een apart hoofdstuk toegevoegd aan de verwerkersovereenkomst waarin eisen met betrekking tot informatiebeveiliging worden gesteld, zoals het kunnen voldoen aan de BIO en het uitvoeren van een penetratietest. Bij een penetratietest wordt een systeem onderzocht op kwetsbaarheden. De verwerkersovereenkomsten bevatten ook een addendum met afspraken voor het geval een organisatie hier niet aan kan voldoen.

De gemeente werkt aan het verder professionaliseren van monitoren van afspraken met derden en heeft een softwareapplicatie aangeschaft voor het ISMS, waar op termijn ook normen met betrekking tot de AVG in worden opgenomen. Dit ISMS moet eenduidigheid brengen en maakt het mogelijk om bij te houden en aantoonbaar te maken aan welke maatregelen wel of niet voldaan wordt. Ten tijde van het onderzoek was dit in ontwikkeling en was het niet duidelijk wanneer dit zou zijn afgerond. Er is geen systeem dat de monitoring van alle verwerkersovereenkomsten op een centrale plek monitort.

De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. Hierin is aandacht voor mogelijke (ongewenste) knelpunten.	+
Er is een routine voor meten en verbeteren.	+

[11] DPIA-Leidraad v. 1.2

[12] ENSIA staat voor Eenduidige Normatiek Single Information Audit.

[13] Zie hoofdstuk IV van de AVG.

Om ervoor te zorgen dat ook nieuwe werknemers bekend zijn met het privacy- en informatiebeveiligingsbeleid worden ook nieuwe medewerkers hierover geïnformeerd. Zij worden aangemeld voor een leermodule over privacy en andere modules. Zij moeten deze modules met succes afronden. Of medewerkers goed omgaan met persoonsgegevens kan ook worden besproken in functionerings- en/of beoordelingsgesprekken wanneer dit relevant is. In de organisatie wordt er daarnaast op verschillende manieren aandacht gegeven. Zo wordt er extra aandacht gegeven aan privacy op de 'Europese dag van de privacy' en wordt de jaarlijkse 'week van de veiligheid' in oktober gebruikt voor informatieveiligheid.

De gemeente informeert de inwoner op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.	+
De gemeente verschaft aan inwoners schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.	+

Op de website van de gemeente is een Privacyverklaring[14] te vinden. Hierin wordt uitgelegd hoe de gemeente omgaat met de verwerking van persoonsgegevens. Er wordt toegelicht hoe er wordt omgegaan met uitwisseling van gegevens met derden en waarom en hoe er met gegevens om wordt gegaan.[15] Ook worden de privacyrechten van inwoners toegelicht en uitgelegd en hoe zij hier een beroep op kunnen doen en wanneer ze een klacht kunnen indienen.

Het contact met inwoners over privacy vindt op verschillende plekken plaatsen. Er is een participatieplatform, 'Met Amersfoort', waarbij JDA adviseert. Bij dit platform worden inwoners betrokken en komen onderwerpen en ideeën van inwoners van buiten naar binnen. Dit gebeurt in de vorm van (online) bijeenkomsten[16]. Tevens is er los van het platform een burgerpanel, Technologisch Burgerpanel Amersfoort, dat meedenkt over ontwikkelingen rondom Amersfoort als Smart City. Zij denken mee over de inzet van technologie in de stad en geven de gemeente feedback hierover. Op deze manier kan het burgerperspectief worden betrokken bij het maken van beleid. Kwartiermaker van dit technologisch burgerpanel is POWER (Prettig Ouder Worden en Relativeren). POWER bestaat uit leden boven de leeftijd van 50. Met kennis en vaardigheden willen zij iets betekenen voor de stad. Hierbij speelt digitalisering een belangrijke rol. Het doel hierachter is dat gewone burgers beoordelen wat voor effect gemeentelijke digitaliseringsbeleid heeft op het dagelijks leven.

Klachten van inwoners over de bescherming van persoonsgegevens worden meestal gericht aan de FG, maar niet uitsluitend. Klachten kunnen ook bij andere medewerkers binnenkomen, omdat een inwoner daar al contact mee heeft. Er is door de gemeente (nog) geen representatief onderzoek of inventarisatie gedaan naar het perspectief van inwoners op de bescherming van persoonsgegevens door de gemeente. Medewerkers van de gemeente hebben de indruk dat inwoners weten hoe ze vragen kunnen stellen aan de gemeente. Er komen niet veel vragen binnen. Incidenten worden breed geregistreerd. Ook bij twijfel of iets werkelijk een schending is van privacy wordt het geregistreerd als melding. Er zijn geen klachten of meldingen van burgers die POWER doorzet naar de gemeente. Als het technologisch burgerpanel helemaal loopt zal opnieuw worden gekeken naar deze constructie.

[14] https://www.amersfoort.nl/bericht/privacyverklaring-gemeente-amersfoort.htm

[15] https://www.amersfoort.nl/bericht/digitaal-samenwerken-met-gemeente-amersfoort-of-de-wijkteams.htm

[16] https://metamersfoort.nl/met+amersfoort/default.aspx

Indien er sprake is geweest van een datalek, heeft de gemeente conform de vastgelegde procedure gehandeld.	+

In 2018 zijn er 75 meldingen gerapporteerd, waarvan 45 datalekken. Hiervan zijn er 16 gemeld bij de Autoriteit Persoonsgegevens (AP). In 2019 zijn er 67 meldingen gerapporteerd waarvan 47 datalekken. Hiervan zijn er 19 gemeld bij de AP. In 2020 zijn er 50 meldingen gerapporteerd, waarvan 46 datalekken. Hiervan zijn er 6 gemeld bij de AP. Meldingen, dit kunnen incidenten, signalen of datalekken zijn, worden opgenomen in de kwartaalrapportages. De kwartaalrapportage Informatiebeveiliging en privacy informeert de kerngroep privacy en informatieveiligheid, de directie en de portefeuillehouders. Meldingen worden intentioneel breed geregistreerd, zodat er niets over het hoofd wordt gezien. Incidenten worden behandeld volgens vastgestelde werkwijzen en een Protocol.[17] In de praktijk wordt hiernaar gehandeld. Er wordt geregistreerd welke van de meldingen datalekken betreffen. Indien er als gevolg van de inbreuk waarschijnlijk sprake is van een risico of hoog risico op de rechten en vrijheden worden deze gemeld bij respectievelijk de AP en betrokkenen.

De precieze aard van de meldingen wordt geregistreerd. Er wordt vastgelegd in welke categorie het lek valt. De meest voorkomende melding is dat er persoonsgegevens zijn verstuurd of afgegeven aan een onjuist ontvanger. Er wordt door leidinggevenden en sleutelpersonen actief gewerkt aan een werkklimaat waarbij medewerkers fouten durven te melden.

In het onderzoek zijn geen voorbeelden gevonden waarbij er een oneigenlijk beroep is gedaan op de AVG of dat informatie niet wordt gedeeld terwijl dit wel zou mogen of moeten. Er is een aantal neveneffecten van de AVG. De AVG stelt eisen aan de inrichting van systemen. Deze eisen worden echter niet als ongewenst ervaren, maar wel als iets dat de gemeente nog meer moet oppakken, zeker als het gaat om privacy-by-design[18]. Ook vraagt de AVG dat bedrijfsprocessen soms langzamer verlopen, omdat er nauwkeurig moet worden gewerkt. Ook dit wordt niet direct als ongewenst ervaren, maar wel als uitdagend.

2.3 Cultuur binnen de organisatie

Deelvraag 5 Hoe monitort/verifieert de gemeente afspraken in verwerkersovereenkomsten met derden, waar knelt de AVG, waar zitten beperkingen en risico's? Denk aan GGD, Veiligheidshuis, sociale wijkteams, werk inkomen en zorg, belastingen, afval, Geldwijzer033, BRP, personeelsadministratie, Smart City toepassingen?
Deelvraag 6 Zijn er verschillen en zo ja welke, in de bescherming van persoonsgegevens door de gemeente en door derden?
Deelvraag 9 Hoe vinden inwoners dat hun privacy (door derden) wordt beschermd? Hoe gaat de gemeente om met klachten? Wat is de aard van eventuele klachten?

Normen voor deelvragen 5, 6 en 9	**Beoordeling**
De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens en worden van aanpassingen op de hoogte gehouden.	+

[17] 'Protocol Afhandelteam Incidentenmeldingen' en 'Werkwijze Afhandelteam Incidentmeldingen'

[18] Privacy-by-design houdt in dat privacy bij het ontwerp van een technisch of organisatorisch proces al in een vroeg stadium wordt meegenomen.

In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk privacybeleid na te leven.	+

Het belang van privacy wordt onderstreept in alle lagen van de organisatie en privacy wordt regelmatig in overleggen in de verschillende bestuurslagen besproken. Dit blijkt onder andere doordat het onderwerp standaard op de agenda staat bij het sleutelpersonenoverleg, maar ook in overleggen van het Management Team van de gemeentelijke organisatie. Ook is er een specifieke Kerngroep Privacy en Informatiebeveiliging (PIB) opgericht die kijkt naar privacy en informatiebeveiliging. In elke bestuurslaag zijn er personen die zich direct met het onderwerp bezighouden. Werknemers uit de verschillende lagen van de organisatie zijn bekend met het privacybeleid en weten hier uitvoering aan te geven in hun dagelijkse handelingen. Per domein zijn er werkprocessen die indien relevant ingaan op de omgang met persoonsgegevens.[19]

In de gemeente wordt er veel aandacht besteed aan het bewustzijn over privacy bij dagelijkse handelingen. Bij onduidelijkheden over hoe met iets moet worden omgegaan kan er advies worden gevraagd bij de afdeling Juridische Dienstverlening en Advies (JDA) en IT Dienstverlening en Advies (ITDA). Bij nieuwe ontwikkelingen in wetgeving of beleid wordt er gekeken naar mogelijke privacyrisico's en hoe deze kunnen worden gemitigeerd.

In de relatie met inwoners zijn de medewerkers proactief en transparant over de wijze waarop de gemeente omgaat met hun gegevens	-/+

Op de website van de gemeente is een Privacyverklaring[20] te vinden. Hierin wordt uitgelegd hoe de gemeente omgaat met de verwerking van persoonsgegevens. Er wordt toegelicht hoe er wordt omgegaan met uitwisseling van gegevens met derden en waarom en hoe er met gegevens om wordt gegaan.[21] Ook worden de privacyrechten van inwoners toegelicht en uitgelegd en hoe zij hier een beroep op kunnen doen en wanneer ze een klacht kunnen indienen.

Het contact met inwoners over privacy vindt op verschillende plekken plaatsen. Er is een participatieplatform, 'Met Amersfoort', waarbij JDA adviseert. Bij dit platform worden inwoners betrokken en komen onderwerpen en ideeën van inwoners van buiten naar binnen. Er is ook een panel van inwoners, het technologisch burgerpanel Amersfoort, dat meedenkt over ontwikkelingen rondom Amersfoort als Smart City. Zij denken mee over de inzet van technologie in de stad en geven de gemeente feedback hierover. Op deze manier kan het burgerperspectief worden betrokken bij het maken van beleid. [22]

In de Privacyverklaring van de gemeente die op de website staat, wordt uitgelegd waar inwoners heen kunnen met klachten. Hier wordt verwezen naar de FG en naar de gewone klachtenprocedure.[23] Klachten van inwoners over de bescherming van persoonsgegevens worden meestal gericht aan de FG, maar niet uitsluitend. Klachten kunnen ook bij andere medewerkers binnenkomen, omdat een inwoner daar al contact mee heeft. Er is door de gemeente (nog) geen onderzoek of inventarisatie gedaan naar het perspectief van inwoners op de bescherming van persoonsgegevens door de gemeente. Medewerkers van de gemeente hebben de indruk dat inwoners weten hoe ze vragen kunnen stellen aan de gemeente. Er komen niet veel vragen binnen. Incidenten worden breed

[19] Zoals de EU Aanbestedingsleidraad openbare procedures.

[20] https://www.amersfoort.nl/bericht/privacyverklaring-gemeente-amersfoort.htm

[21] https://www.amersfoort.nl/bericht/digitaal-samenwerken-met-gemeente-amersfoort-of-de-wijkteams.htm

[22] https://metamersfoort.nl/met+amersfoort/default.aspx

[23] https://www.amersfoort.nl/bericht/privacyverklaring-gemeente-amersfoort.htm

geregistreerd. Ook bij twijfel of iets werkelijk een schending is van privacy wordt het geregistreerd als melding.

Binnengekomen vragen/klachten/verzoeken via de FG-mail worden in behandeling genomen door of via de FG. De gemeente Amersfoort kent ook een klachtenverordening. De afhandeling wordt afgestemd met de afdeling die de betreffende verwerking onder zich heeft en indien nodig met de klachtcoördinator.

Voor de behandeling van verzoeken in het kader van rechten van betrokkenen wordt een afgesproken proces gevolgd dat staat beschreven in de privacyverklaring. Klachten worden geregistreerd bij wie de klacht is gedaan. Voor centrale registratie van verzoeken in het kader van de rechten van betrokkenen wordt momenteel een ander proces ingericht. De aard van de klachten is op dit moment niet inzichtelijk opgeslagen. De indruk van medewerkers is dat het aantal klachten laag is.

Er is geen inzicht in het aantal of het bestaan van klachten bij samenwerkingspartners. Samenwerkingspartners hoeven deze klachten niet met de gemeente te delen als de klacht over iets gaat waar geen gedelegeerde of gedeelde verantwoordelijkheid voor is. Er zijn aan de onderzoekers geen klachten uitgelicht over zaken waar er een gelegeerde of gedeelde verantwoordelijkheid was.

In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente.	+

Met verwerkers worden er verwerkersovereenkomsten afgesloten. Er gelden voor contractpartners dezelfde eisen ten opzichte van de bescherming van persoonsgegevens als de eisen die de gemeente zichzelf stelt. Wanneer er sprake is van een zelfstandige of gezamenlijke verwerkingsverantwoordelijkheid wordt er een dataleveringsovereenkomst afgesloten en/of worden er bijvoorbeeld convenanten afgesloten. Met een aantal samenwerkingspartners is daarnaast regelmatig overleg en wordt waar nodig ook de bescherming van persoonsgegevens met partners besproken.

Het kan wel het geval zijn dat er verschillen zijn met de omgang van persoonsgegevens door derden op de terreinen waar de gemeente geen (verwerkings)verantwoordelijkheid heeft. De gemeente kan hier slechts beperkt invloed op uitoefenen. Er ligt geen juridische verplichting bij de gemeente om dit na te gaan en vaak is dit niet mogelijk.

HOOFDSTUK 3 CONCLUSIES

De hoofdvraag van dit onderzoek was:

Hoe wordt de privacy van de Amersfoortse inwoners beschermd en wordt er adequaat gebruik gemaakt van de AVG, toegespitst op derden aan wie de uitvoering van beleid is uitbesteed, of met wie anderszins persoonsgegevens worden gedeeld?

Het privacybeleid voldoet in hoofdlijnen aan de AVG en hier wordt in de praktijk naar gehandeld. De verschillende eisen en principes van de AVG zijn adequaat uitgewerkt in beleid en werkprocessen. Dit geldt ook voor de afspraken die worden gemaakt met derden.

Wat opvalt is de sterke ontwikkeling van het privacybeleid binnen de organisatie. Deze is de afgelopen jaren op verschillende punten sterk verbeterd. Hierbij is allereerst de aandacht gegaan naar de uitwerking van uitgangspunten. Het beleid dat nu wordt gehanteerd, is een concretere uitwerking die richting geeft aan hoe mogelijke knelpunten moeten worden opgelost. Bij het opstellen van beleid zijn de relevante organen, zoals het college en de raad, meegenomen. Dat het beleid vervolgens in verschillende overleggen terug is gekomen, heeft ertoe geleid dat het brede bekendheid geniet.

De raad wordt omtrent privacy op de hoogte gehouden door raadsinformatiebrieven en presentaties. Daarnaast is de raad actief betrokken bij de uitgangspunten waarop het huidige privacybeleid nog steeds is gestoeld en wordt de raad direct geïnformeerd bij ernstige datalekken. Minder ernstige datalekken worden binnen reguliere bijeenkomsten besproken. Omtrent informatiebeveiliging is de raad nog beperkt betrokken. De raad wordt daarover geïnformeerd via de jaarrekening en het jaarverslag.

Er is veel aandacht geweest voor de invloed van de cultuur in de organisatie voor de omgang met persoonsgegevens. Dit is te zien aan kleine zaken, zoals dat er actief wordt gewerkt aan een prettig werkklimaat waar medewerkers mogelijke fouten durven toe te geven, zoals het versturen van een mail naar een verkeerd adres. Het is ook terug te zien in structurele aanpassingen, zoals het aanstellen van sleutelpersonen om ervoor te zorgen dat het makkelijk is om iemand in elke afdeling te vinden waarbij vragen over privacy kunnen worden gesteld. Aanvullend zijn er in de organisatie professionals die lastige, technische of juridische vragen kunnen beantwoorden.

Met derden worden consistente afspraken gemaakt in de vorm van overeenkomsten of convenanten. Aan derden waar gegevens mee worden gedeeld, worden dezelfde eisen gesteld als de eisen waar de gemeente zichzelf aan houdt op het gebied van privacy en informatiebeveiliging. Er kunnen nog stappen worden gemaakt bij de monitoring van de gemaakte afspraken. De eerste stappen in de vorm van een nieuw systeem zijn hiervoor al gezet.

De AVG wordt over het algemeen niet als knellend of belemmerend ervaren. Dit hangt samen met de constructieve houding tegenover privacy. Er zijn geen signalen verkregen op basis waarvan kan worden geconcludeerd dat er een oneigenlijk beroep wordt gedaan op de AVG. Wel doen er zich soms lastige situaties voor waarbij het niet helemaal duidelijk is hoe de AVG samengaat met andere wetgeving. Ook vraagt de AVG een nieuwe manier van werken die vraagt dat bestaande IT-systemen worden aangepast of anders worden ingericht. De organisatie werkt aan dit laatste en hoopt in de toekomst meer stappen te kunnen zetten met privacy en security by design.

De gemeente heeft beperkt inzicht in de houding van inwoners ten aanzien van privacy. Er wordt via de gangbare wegen, zoals de website en aan de balie, gecommuniceerd over privacy aan inwoners. Het is voor inwoners lastig om te beoordelen wanneer hun rechten in het gedrang zijn. Privacy is al snel een lastig onderwerp voor veel inwoners. Klachten worden afgehandeld. Op basis van de klachten

is het niet mogelijk een algemeen beeld vast te stellen over het perspectief van inwoners. Hoewel de communicatie naar inwoners op dit moment voldoende is, zou de gemeente hier een proactievere rol in kunnen nemen die past bij de houding die intern in de afgelopen jaren is bevorderd.

HOOFDSTUK 4 AANBEVELINGEN

De beantwoording van de deelvragen uit hoofdstuk 2 en de conclusies uit hoofdstuk 3 laten zien dat de gemeente Amersfoort goed op weg is op het gebied van bescherming van persoonsgegevens. Op enkele onderdelen ziet de rekenkamer aanleiding om een aanbeveling te doen:

Inventarisatie inwoners

Het huidige inzicht in de houding van inwoners omtrent de bescherming van persoonsgegevens door de gemeente is niet erg groot. Er komen af en toe klachten en vragen bij de FG terecht. Medewerkers van de gemeente Amersfoort constateren ook dat er weinig vragen binnenkomen. Inwoners weten vaak weinig over de bescherming van persoonsgegevens. Tegelijkertijd worden er veel gegevens verwerkt met vaak steeds complexere technologieën.
Om als gemeente een beter zicht te krijgen op het perspectief van de inwoners van Amersfoort op de bescherming van persoonsgegevens is een inventarisatie hiernaar nodig. Dit inzicht kan de gemeente helpen om voor inwoners ongelukkige of nadelige uitwerkingen van beleid op het gebied van persoonsgegevens proactief te signaleren en na te gaan of de huidige wijze van communiceren kan worden verbeterd. Dat kan bijvoorbeeld door aan verschillende inwoners de over hen beschikbare informatie bij de gemeente voor te leggen, uit te leggen wat de gemeente met die informatie doet en daarover het gesprek aan te gaan.

Aanbeveling: Inventariseer hoe inwoners aankijken tegen het verzamelen en gebruik van persoonsgegevens en de bescherming daarvan door de gemeente om zo ongelukkige of nadelige uitwerkingen van beleid op het gebied van persoonsgegevens proactief te signaleren en na te gaan of de huidige wijze van communiceren hierover kan worden verbeterd.

Monitoring nakoming afspraken met derden

Met derden worden consistente afspraken gemaakt in de vorm van overeenkomsten of convenanten. Aan derden waar gegevens mee worden gedeeld, worden dezelfde eisen gesteld als de eisen waar de gemeente zichzelf aan houdt op het gebied van privacy en informatiebeveiliging. Wel is gebleken dat er nog stappen kunnen worden gemaakt bij de monitoring van de gemaakte afspraken en specifiek de monitoring van de verwerkersovereenkomsten. De eerste stappen in de vorm van een nieuw systeem zijn hiervoor al gezet.

Aanbeveling: Richt jaarlijkse monitoring in van de afspraken die met derden zijn gemaakt over bescherming van persoonsgegevens en neem de resultaten hiervan op in het jaarverslag van de FG.

Naast het opvolgen van deze twee aanbevelingen, zijn er nog mogelijkheden om verdere verbeteringen in te zetten op het gebied van bescherming van persoonsgegevens. Zowel het onderzoek van de rekenkamer als ook de gemeente zelf geven aan dat één van de grootste uitdagingen voor de toekomst is, de aandacht voor privacy vast te houden. Om de komende jaren de bescherming van persoonsgegevens nog verder te verbeteren zijn de volgende extra aanbevelingen geformuleerd:

Privacy by design en security by design

Privacy en security by design dienen nog verder ontwikkeld te worden. Simpele aanpassingen zijn al door de organisatie opgepakt, zoals hoe medewerkers de mailinstellingen in Outlook moeten instellen. Om systemen met privacy als uitgangspunt in te richten, moet er kritisch worden gekeken naar de hele levenscyclus van verwerkingen en systemen. De aandacht voor privacy dient dan ook in de toekomst sterk aanwezig te zijn bij het aankopen en inrichten van nieuwe systemen en werkprocessen. Daarnaast, aangezien er altijd weer nieuwe wetgeving en nieuwe technische mogelijkheden komen die

weer nieuwe werkprocessen met zich mee brengen, zal er ook bij huidige verwerkingssystemen moeten worden gekeken of en hoe deze kunnen worden aangepast.

Aanbeveling: Neem bescherming van persoonsgegevens en privacy als vast onderdeel mee bij de aankoop en inrichting van nieuwe systemen en werkprocessen. Controleer bij het inwerkingtreden van nieuwe of gewijzigde wetgeving of bij het beschikbaar komen van nieuwe technologieën standaard of bestaande systemen en werkprocessen als gevolg hiervan moeten worden aangepast.

De raad

Uit het onderzoek is gebleken dat de raad is geïnformeerd over de ontwikkelingen met betrekking tot privacybeleid. Echter wordt de raad over het onderwerp informatiebeveiliging vooral geïnformeerd via de jaarrekening en het jaarverslag. Onze aanbeveling is dan ook om het informeren van de raad over informatiebeveiliging te intensiveren. Hierbij zou de aandacht moeten liggen op ontwikkelingen die relevant zijn voor de gehele gemeentelijke organisatie.

Aanbeveling: Informeer de raad minimaal éénmaal per jaar integraal over relevante ontwikkelingen op het gebied van informatiebeveiliging.

Bijlage 1 Deelvragen

1. Hoe biedt de gemeente Amersfoort bescherming aan inwoners als het gaat om privacy?
2. Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid betrokken geweest?
3. Waar knelt de AVG, waar zitten beperkingen en risico's?
4. Wat heeft de FG (functionaris gegevensbescherming) nodig van de gemeente om haar werk te kunnen doen? In hoeverre is dit in Amersfoort geregeld?
5. Hoe monitort/verifieert de gemeente afspraken in verwerkersovereenkomsten met derden, waar knelt de AVG, waar zitten beperkingen en risico's? Denk aan GGD, Veiligheidshuis, sociale wijkteams, werk inkomen en zorg, belastingen, afval, Geldwijzer033, BRP, personeelsadministratie, Smart City toepassingen.
6. Zijn er verschillen en zo ja welke, in de bescherming van persoonsgegevens door de gemeente en door derden?
7. Wat zijn ongewenste neveneffecten van de AVG: gebeurt het bijvoorbeeld dat informatie niet wordt gedeeld met een (oneigenlijk) beroep op de AVG?
8. Welke privacyschendingen zijn er bij de gemeente en de samenwerkingspartners sinds de invoering van de AVG geweest/gemeld? Hoe is de gemeente daarmee omgegaan?
9. Hoe vinden inwoners dat hun privacy (door derden) wordt beschermd? Hoe gaat de gemeente om met klachten? Wat is de aard van eventuele klachten?
10. Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?

BIJLAGE 2 ONDERZOEKSOPZET EN VERANTWOORDING

Het rekenkameronderzoek kent vier fasen: de aankondiging, de deskresearch, de verdieping en tot slot de analyse en rapportage.

Fase 1: Aankondiging

Het onderzoek begon met een aankondigingsgesprek, waarin het onderzoek werd gepresenteerd aan de betrokken ambtenaren[24] en er werkafspraken zijn gemaakt.
De presentatie van het onderzoek betrof een toelichting op de uitgangspunten van het onderzoek en de werkafspraken gingen over het verkrijgen van de relevante informatie, planning van interviews en groepsbijeenkomsten, de keuze voor de beleidsdomeinen en/of casussen, en overige zaken.

Fase 2: Deskresearch

Tijdens de tweede fase is er door middel van documentenstudie en interviews inzicht verkregen in de uitgangspunten van het gemeentelijk beleid met betrekking tot de bescherming van persoonsgegevens. Een overzicht van de bestudeerde documenten staat in bijlage A. Er hebben verschillende interviews plaats gevonden. De interviewlijst staat in bijlage B. Conform gebruikelijke werkwijzen is er van elk interview een conceptverslag opgesteld. Deze is ter verificatie voorgelegd aan de geïnterviewde persoon. Na verwerking van diens opmerkingen en aanvulling werd het verslag definitief een onderdeel van het onderzoeksdossier.

Fase 3: Verdieping

In de derde verdiepende fase is gekeken in hoeverre het vastgelegde beleid in de praktijk wordt ingevuld en nageleefd, zowel binnen de gemeentelijke organisatie zelf als in de relatie met inwoners en ketenpartners. De verdiepende fase kent daarmee verschillende activiteiten:

- Er zijn twee workshops georganiseerd op (informatie-intensieve) beleidsdomeinen en gesprekken gevoerd met de bij de informatieverwerking betrokken ambtenaren om te doorgronden hoe zij in de praktijk en in het contact met inwoners omgaan met privacyvraagstukken. Dit was op het terrein van Smart City, waar in het bijzonder is gekeken naar de rol van algoritmen en naar de uitvoering van de Wet verplichte geestelijke gezondheidszorg;
- Er is gekeken naar beleidstukken en communicatie van de gemeente met betrekking tot de bescherming van persoonsgegevens geanalyseerd.
- Er heeft een inventarisatie plaats gevonden met betrekking tot welke afspraken er door de gemeente worden gemaakt met ketenpartners over de wijze waarop de ketenpartners de privacy waarborgen.
- Er is getoetst op welke wijze de gemeente de naleving van deze afspraken door ketenpartners bewaakt, zowel in de interviews bij medewerkers van de gemeente als door middel van gesprekken bij enkele belangrijke (informatie-intensieve) ketenpartners.
- Er is een sessie met medewerkers van de organisatie georganiseerd om de voorlopige bevindingen van het onderzoek te bespreken en in de juiste context te plaatsen. Onder meer is er ingegaan op mogelijke knelpunten in de praktijk die het gevolg zijn van de regelgeving (of de interpretatie daarvan) en de mogelijke oplossingen daarvoor. Een dergelijke sessie versterkt inzicht en samenhang in het rapport en ons onderzoek, en bevordert het draagvlak en de acceptatie.

[24] Dat betrof de burgemeester van Amersfoort, secretaris van de rekenkamer, privacy jurist teammanager Juridische Dienstverlening en Advies.

- Aan de hand van een aantal stellingen in een sessie met raadsleden is de rol van de raad (controlerend, sturend, kaderstellend) ten aanzien van de bescherming van persoonsgegevens besproken.

Fase 4: Analyse en rapportage

In deze fase zijn de uitkomsten van het onderzoeken geanalyseerd om te komen tot de beantwoording van de deelvragen en onderzoeksvraag. De resultaten van het onderzoek zijn beschreven in een conceptrapport. Deze is door de rekenkamer voor technisch wederhoor bij de betrokkenen neergelegd. Vervolgens zijn, na eventuele aanpassingen uit het technisch wederhoor, de conclusies en aanbevelingen toegevoegd aan het rapport.

Bijlage 3 Normenkader

Normenkader

Normen met betrekking tot het gemeentelijk beleid

- De gemeente heeft AVG-conforme beleidskaders, regels en richtlijnen met betrekking tot de (juridische) borging van de privacy van inwoners.
  Voor specifieke (meer risicovolle) domeinen heeft de gemeente aanvullende regels opgesteld.
- De algemene uitgangspunten en kaders zijn besproken in en vastgesteld door de gemeenteraad.
- In de verschillende beleidskaders wordt ingegaan op:
  - Juridische aspecten op basis van de AVG en de materie wetten
  - Vertaling naar de beleidskaders privacy.
  - Organisatie, taken en verantwoordelijkheden.
- Het toezicht op gebruik van persoonsgegevens is vastgelegd in een controleplan.
- In bestuursrapportages, programmabegroting en programmarekening wordt expliciet aandacht besteed aan de wijze waarop een correcte omgang met persoonsgegevens is gewaarborgd. Daaraan worden conclusies en maatregelen verbonden op basis van uitgevoerde controles.
- Er is een procedure vastgelegd hoe de gemeente handelt in het geval van geconstateerde ‘datalekken’.
- Er is vastgelegd hoe de raad wordt geïnformeerd over (de ontwikkelingen in) het privacybeleid.

Normen met betrekking tot de uitvoering van het gemeentelijk beleid

- In de praktijk wordt gehandeld conform de wijze waarop de bescherming van de persoonsgegevens is geregeld in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.
- Afspraken in verwerkersovereenkomsten met derden worden door de gemeente gemonitord en geverifieerd.
- De gemeente heeft een leer- en verbetercyclus waar privacy een apart onderdeel van uitmaakt. Hierin is aandacht voor mogelijke (ongewenste) knelpunten.
- De gemeente heeft een routine voor het meten en verbeteren van de bescherming persoonsgegevens en legt vast wat de bevindingen en maatregelen zijn. Deze routine is al tenminste één keer uitgevoerd.
- Indien er sprake is geweest van een datalek, heeft de gemeente conform de vastgelegde procedure gehandeld.
- De gemeente informeert de burger op een toegankelijke en begrijpelijke wijze over hun privacy-rechten, zowel schriftelijk als mondeling.
- De gemeente verschaft aan inwoners schriftelijk en mondeling begrijpelijke informatie over het gebruik van hun persoonsgegevens, zowel in algemene zin als afgestemd op de verschillende fasen in het dienstverleningsproces. Daarbij wordt aangegeven met welk doel dit gebeurt, wie inzage heeft en wat er vervolgens met de gegevens gebeurt.
- In de praktijk wordt de raad conform de overeengekomen systematiek geïnformeerd over de ontwikkelingen in het privacybeleid.
- De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken.

Normen met betrekking tot de cultuur binnen de organisatie m.b.t. privacy
• De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid bescherming persoonsgegevens en worden van aanpassingen op de hoogte gehouden. • In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk privacybeleid na te leven. • In de relatie met inwoners zijn de medewerkers proactief en transparant over de wijze waarop de gemeente omgaat met hun gegevens. • In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente.

Bijlage 4 Uitgebreide bevindingen

Deze bijlage bevat de verdere uitwerking van de onderzoeksbevindingen uit hoofdstuk 2.

In dit hoofdstuk wordt een uitgebreidere onderbouwing van de bevindingen beschreven en uiteengezet hoe het beleid op het gebied van privacy en informatiebeveiliging zich heeft ontwikkeld. Juist omdat de ontwikkeling van het privacybeleid nadrukkelijk naar voren is gekomen in dit onderzoek, is hier extra aandacht aan gegeven in de bevindingen. Daarnaast is in het bijzonder aandacht besteed aan de wijze waarop rollen en verantwoordelijkheden zijn georganiseerd en de waarborging van privacy en informatiebeveiliging bij contact met derden.[25]

Om de leesbaarheid te bevorderen hebben we de bevindingen m.b.t. de verschillende deelvragen in vier thema's onderverdeeld:

1. *De ontwikkeling van het privacy- en informatiebeveiligingsbeleid*
   - Hoe biedt de gemeente Amersfoort bescherming aan burgers als het gaat om privacy?

2. *Rollen en verantwoordelijkheden*
   - Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid betrokken geweest?
   - Wat heeft de FG (functionaris gegevensbescherming) nodig van de gemeente om haar werk te kunnen doen? In hoeverre is dit in Amersfoort geregeld?
   - Op welke manier wordt de gemeenteraad geïnformeerd over de uitvoering van het beleid rondom de bescherming van persoonsgegevens? Welke mogelijkheden heeft de raad om te sturen en te controleren?

3. *Samenwerking met derden en AVG (neven)effecten*
   - Hoe monitort/verifieert de gemeente afspraken in verwerkersovereenkomsten met derden, waar knelt de AVG, waar zitten beperkingen, risico's? Denk aan GGD, Veiligheidshuis, sociale wijkteams, werk inkomen en zorg, belastingen, afval, Geldwijzer033, BRP, personeelsadministratie, Smart City toepassingen?
   - Zijn er verschillen en zo ja welke, in de bescherming van persoonsgegevens door de gemeente en door derden?
   - Wat zijn ongewenste neveneffecten van de AVG: gebeurt het bijvoorbeeld dat informatie niet wordt gedeeld met een (oneigenlijk) beroep op de AVG.
   - Welke privacyschendingen zijn er bij de gemeente en de samenwerkingspartners sinds de invoering van de AVG geweest/gemeld, hoe is de gemeente daarmee omgegaan?
   - Waar knelt de AVG, waar zitten beperkingen, risico's?

4. *Inwoners*
   - Hoe vinden inwoners dat hun privacy (door derden) wordt beschermd? Hoe gaat de gemeente om met klachten? Wat is de aard van eventuele klachten.

Eerst wordt een overzicht van de ontwikkelingen van het beleid en de uitvoering gedurende deze collegeperiode besproken. Vervolgens worden de rollen en verantwoordelijkheden binnen de

[25] De reikwijdte van de huidige college periode tot oplevering rapport is het uitgangspunt. Aangezien het beleid dat in deze periode een rol speelde soms al eerder was opgesteld, is die ook meegenomen.

gemeente ten aanzien van privacy besproken. Daarna komt hoe de samenwerking met derden is geregeld aan bod en hoe de omgang met inwoners plaatsvindt. Tot slot wordt aandacht besteed aan uitdagingen die voortkomen uit de AVG bij de gemeente en wordt vooruitgekeken.

1. De ontwikkeling van het privacy- en informatiebeveiligingsbeleid

1.1 Privacybeleid

De wijze waarop de gemeente vormgeeft aan de bescherming van privacy van inwoners is te vinden in het privacy- en informatiebeveiligingsbeleid. Waar vaak de komst van de AVG een van de belangrijkste redenen was voor de gemeente om het privacybeleid verder te ontwikkelen, was er bij de gemeente Amersfoort een andere directe aanleiding om nog eens goed naar het privacybeleid en de cultuur binnen de organisatie te kijken. In 2016 en 2017 hebben er verschillende datalekken plaatsgevonden die wegens de ernst en omvang ook de aandacht van de media trokken.[26] De datalekken gaven reden kritisch naar de eigen organisatie te kijken. De komst van de AVG heeft de kritische houding nog verder bevorderd.

Ontwikkeling in beleid tussen 2017 - 2019

In januari 2017 is het Privacybeleid Gemeente Amersfoort 2017-2019 opgesteld. Hierin wordt privacy breed gedefinieerd. Zowel de bescherming van persoonsgegevens, de bescherming van de persoonlijke levenssfeer en het recht op vertrouwelijk communiceren worden meegenomen. Omdat de verwerking van persoonsgegevens en informatie vaak gebeurt via geautomatiseerde systemen, wordt er in dit privacybeleid van uitgegaan dat privacy en informatiebeveiliging onlosmakelijk met elkaar zijn verbonden. Het privacybeleid is afgestemd met de raad.

Het Privacybeleid uit 2017 stelt kaders die als uitgangspunt hebben gediend voor het verder uitwerken van gedragsrichtlijnen en protocollen of om deze te actualiseren.[27] Het Privacybeleid neemt wetgeving en de menselijke maat als uitgangspunt. Hiermee wordt bedoeld dat het beleid voor de verwerking van persoonsgegevens niet dusdanig ingewikkeld of rigide is, dat het in de weg staat aan de zorg- en dienstverlening waar de inwoner iets aan heeft. De AVG die in 2018 van toepassing werd, was in eerste instantie nog niet meegenomen in het beleid maar is er wel in genoemd.

Toen de AVG in aantocht was, is er een kerngroep privacy en informatiebeveiliging gevormd. Het ontstaan van de kerngroep heeft als reden dat de directie er behoefte aan had actief betrokken te zijn bij het thema privacy en informatieveiligheid. Het was in die tijd een betrekkelijk nieuw thema en vroeg om een centrale coördinatie en sturing. De kerngroep had onder andere als doel om een strategische verbinding in stand te houden tussen privacy en informatieveiligheid. De raad is steeds meegenomen in de ontwikkelingen, onder meer via raadsinformatiebrieven.

Ontwikkeling in 2019

De gemeente Amersfoort heeft in 2019 een nieuw privacy- en informatiebeveiligingsbeleid gepubliceerd. Dit nieuwe privacybeleid sluit wel aan bij de kaders uit de AVG en is gebaseerd op een aantal bestuurlijke uitgangspunten en gemeentelijke waarden die in het beleid verder worden uitgewerkt.

Het gaat om de volgende vier uitgangspunten en kernwaarden:
Allereerst staat de mens centraal bij de verwerkingen van persoonsgegevens. Dit betekent dat de betrokkene, degene van wie de persoonsgegevens worden verwerkt, zoveel mogelijk regie heeft over

[26] Dossier Datalekken gemeente Amersfoort | AD.nl

[27] Gemeente Amersfoort, Privacybeleid Gemeente Amersfoort 2017-2019, januari 2017

de eigen gegevens. Daarnaast wordt dit begrip vertaald naar de eis dat het handelen van de gemeentelijke overheid voorspelbaar moet zijn.

Ten tweede streeft de gemeente naar een balans tussen goede privacybescherming en optimale dienstverlening en werkbaarheid. Als privacyregels onevenredige belemmeringen vormen voor de werkbaarheid is de gemeente bereid deze ter discussie te stellen.

Ten derde wordt veiligheid gezien als een randvoorwaarde voor een goede verwerking van persoonsgegevens. Onderdeel hiervan is het zicht houden op de afspraken en relaties met externe partijen. Met verwerkers van persoonsgegevens worden verwerkersovereenkomsten gesloten naar de standaard VNG overeenkomst.[28] Deze overeenkomst wordt waar nodig aangevuld met een door de gemeente Amersfoort ontwikkeld addendum.

Tot slot moet er voor elke verwerking een helder doel zijn en een wettelijke grondslag. Hierbij zijn de grondslagen wettelijke verplichting, taak van algemeen belang en/of in het kader van een taak van openbaar gezag meestal van toepassing. Binnen het sociaal domein wordt er, als het niet anders kan, gewerkt met toestemming.

Om ervoor te zorgen dat het bewustzijn over privacy en informatieveiligheid in de gehele organisatie aanwezig is zijn er sleutelpersonen privacy en informatieveiligheid aangesteld. Sleutelpersonen zijn medewerkers die worden gekozen in overleg met afdelingsmanagers/teammanagers en zijn aangewezen als eerste aanspreekpunt voor collega's rondom het thema privacy en informatieveiligheid. Sleutelpersonen zijn verspreid over alle afdelingen van de organisatie. Zij kunnen collega's op een laagdrempelige manier helpen bij vragen en overpeinzingen. Sleutelpersonen krijgen een cursus en nemen deel aan het sleutelpersonenoverleg. Sinds 2019 is ook meer aandacht voor veiligheid gekomen bij het uitvoeren van DPIA's[29]. Bij een DPIA worden, voordat een proces van start gaat, privacy- en informatieveiligheidsrisico's met betrekking tot de verwerking van persoonsgegevens in kaart gebracht.

Voor de zomer van 2019 zijn er bijeenkomsten met het college en ambtenaren georganiseerd om de uitgangspunten van het nieuwe beleid te verkennen. Hier waren stakeholders uit verschillende afdelingen, waaronder het sociaal domein, bij betrokken. Ook is er een sessie met het college gehouden onder begeleiding van een externe deskundige. Na de zomer van 2019 is het beleid afgestemd met de raad door middel van een rondetafelgesprek. Hoewel dit grotendeels ging om uitvoeringsbeleid, is de raad hierbij betrokken door middel van een workshop en een prikkelende, externe spreker. In oktober 2019 is het nieuwe beleid aangeboden aan de raad. Sindsdien gaat de rapportage via de P&C-cyclus.

De FG maakt een jaarverslag waarin wordt geëvalueerd. In maart 2021 is het verslag over 2019 en 2020 overhandigd. De raad wordt door het college geïnformeerd over het privacybeleid. De raad wordt ook geïnformeerd over datalekken. Dat gebeurt jaarlijks over het aantal datalekken, hoeveel hiervan zijn gemeld bij de Autoriteit Persoonsgegevens (AP) en tot welke categorie de datalekken behoren. Daarnaast wordt de raad actief geïnformeerd over datalekken met een hoog risico, mochten deze hebben plaatsgevonden.

[28] https://vng.nl/nieuws/standaard-verwerkersovereenkomst-gemeenten-wordt-verbindend

[29] Data Protection Impact Assessment is een door de AVG verplicht onderzoek waarin risico's op het gebied van privacy in kaart worden gebracht.

Heden

De meest recente beleidsplannen over privacy zijn te vinden in het Jaarplan Privacy 2020. In het jaarplan staan het huidige privacybeleid en de doelstellingen voor dit jaar beschreven. Het belangrijkste streven in dit plan is het bevorderen van bewustzijn over privacy op de gehele werkvloer. Dit plan heeft tot doel dat iedereen zijn rol pakt en zijn verantwoordelijkheid die past bij privacy, kent en neemt.

De vier uitgangspunten van het Privacybeleid 2017-2019 die hierboven zijn uitgelicht, staan ook hier centraal en krijgen een concrete invulling. In het jaarplan staat verder per thema aangegeven welke stappen worden gezet en wanneer deze een succes zijn. Dit helpt de ontwikkelingen meetbaar te maken. Er worden acht thema's onderscheiden; privacybeleid, privacygovernance, stelselhouder privacy, DPIA's, datalekken, rechten van betrokken, samenwerking(sverbanden) en verantwoording.

Uit het jaarplan blijkt dat er vorderingen te zien zijn op de verschillende thema's. Het beleid is breed bekend bij de organisatie. Dit komt onder andere door de inzet van sleutelpersonen. De governance is in kaart gebracht in het document Privacy Governance 2020. Hierin zijn de verschillende rollen, taken en verantwoordelijkheden beschreven. De afdeling Juridische Dienstverlening en Advies (JDA) treedt op als stelselhouder met betrekking tot privacy.[30]

Het projectmatig vaststellen en inrichten van een systematiek voor de DPIA's heeft de afgelopen drie jaar veel aandacht gekregen. Ten tijde van dit onderzoek zijn er 46 DPIA's uitgevoerd, waarvan ongeveer de helft is vastgesteld door de afdelingsmanager. Er zijn verschillende hulpmiddelen ontwikkeld om medewerkers te helpen bij DPIA's. Zo is er een Quickscan ontwikkeld die helpt bij het bepalen of er een DPIA moet worden uitgevoerd. Er zijn mensen aangesteld en opgeleid als DPIA-begeleider. Ook kunnen medewerkers bij de sleutelpersonen en medewerkers van JDA vragen stellen. Het regelmatig uitvoeren van DPIA's behoort tot de standaardpraktijk van de organisatie.

Het aantal ernstige datalekken is sinds 2017 afgenomen. Het aantal datalekken wordt in de gaten gehouden door JDA en ITDA.[31] Bij dalingen en stijgingen wordt er gekeken of dit kan worden verklaard. Zo werd er tijdens het begin van de pandemie een daling in het aantal gemelde datalekken geconstateerd. Dit vond men opvallend, omdat het plotseling thuiswerken juist voor meer lekken zou kunnen zorgen. Inmiddels is het aantal datalekken weer op het niveau van voor maart 2020. De precieze reden is niet bekend, maar de gemeente vermoed dat door de overschakeling naar het thuiswerken medewerkers misschien tijdelijk minder datalekken melden.

De kerngroep privacy en informatiebeveiliging bestaat nog steeds. Recent is in de kerngroep intensief gesproken over nut en noodzaak van de kerngroep, en zijn deze bevestigd. Het overleg wordt op strategisch niveau gevoerd en is risicogericht. Concreet gaat het om de volgende thema's: ontwikkelingen, bestuurlijke zaken en borging. In de kerngroep worden ook de kwartaalrapportages met betrekking tot privacy en informatiebeveiliging besproken.

De afdeling JDA is gegroeid. Op dit moment zijn er vier privacyjuristen die de organisatie bedienen, maar ook proactief opereren en de organisatie opzoeken. Ze reageren op adviesvragen, maar halen ook adviezen op. Op de afdeling ITDA werken nu twee adviseurs informatiebeveiliging. Eén houdt zich meer bezig met technische zaken en maatregelen, één meer met het beleid (zoals de implementatie

[30] In thema II van deze bijlage wordt er verder op de governancestructuur ingegaan.

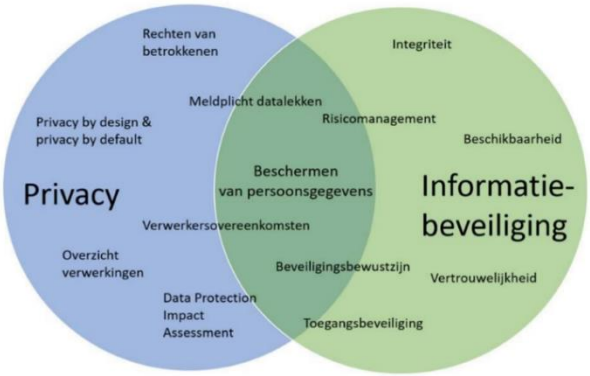
[31] In 2018 zijn er 78 meldingen gerapporteerd waarvan 48 datalekken. 18 hiervan zijn gemeld bij de AP. In 2019 zijn er 67 meldingen gerapporteerd waarvan 47 datalekken. 19 hiervan zijn gemeld bij de AP. In 2020 zijn er 49 meldingen gerapporteerd waarvan 46 een datalek. Hiervan zijn er 7 gemeld bij de AP. Een tabel met het overzicht staat in Bijlage 7.

van de BIO). Daarnaast is er een Chief Information Officer (CIO) en een Concern Information Security Officer (CISO).

Om ervoor te zorgen dat ook nieuwe werknemers bekend zijn met het privacy- en informatiebeveiligingsbeleid worden zij hierover geïnformeerd. Nieuwe medewerkers worden aangemeld voor een leermodule over privacy en andere modules. Zij moeten deze modules met succes afronden. Of medewerkers goed omgaan met persoonsgegevens kan ook worden besproken in functionerings- en/of beoordelingsgesprekken wanneer dit relevant is. In de organisatie wordt er daarnaast op verschillende manieren aandacht gegeven. Zo wordt er extra aandacht gegeven aan privacy op de 'Europese dag van de privacy' en wordt de jaarlijkse 'week van de veiligheid' in oktober gebruikt voor informatieveiligheid.

1.2 Informatiebeveiliging

In het Privacybeleid 2019 beschrijft de gemeente Amersfoort al de samenhang tussen de beleidsonderwerpen informatiebeveiliging en privacy. Deze onderwerpen overlappen elkaar: informatiebeveiliging wordt als een belangrijk onderdeel van privacy gezien, maar omvat ook de beveiliging van gegevens die geen persoonsgegevens betreffen. De relatie tussen privacy en informatiebeveiliging wordt in het privacybeleid als volgt weergegeven:



Figuur 1 Samenhang tussen privacy en informatiebeveiliging zoals beschreven in het privacybeleid

De gemeente Amersfoort heeft in 2019 een nieuw informatiebeveiligingsbeleid gepubliceerd voor de jaren 2019 tot en met 2022. Een belangrijke verandering ten opzichte van het Informatiebeveiligingsbeleid 2016-2019 is het gebruik van het nieuwe normenkader Baseline Informatiebeveiliging Overheid (BIO). Een belangrijk verschil met de oude Baseline Informatiebeveiliging Gemeenten (BIG) is de nadruk op risicomanagement. Het verschil zit in het maken van keuzes en afwegingen over de beveiliging van processen en informatiesystemen op basis van de risico's die er bestaan voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

In het informatiebeveiligingsbeleid zijn ook de verantwoordelijkheden, taken en rollen op het gebied van informatiebeveiliging (de beveiligingsorganisatie) omschreven, waaronder:

- De CISO heeft een toezichthoudende rol en is verantwoordelijk voor het opstellen en implementeren van het informatiebeveiligingsbeleid en -plan.
- Afdelingsmanagers zijn verantwoordelijk voor de integrale beveiliging van de afdeling (waaronder de processen en systemen van de afdeling).
- Zij worden daarbij ondersteund en geadviseerd door de adviseur informatiebeveiliging.
- De sleutelpersonen zijn de eerste aanspreekpunten voor medewerkers van een afdeling (op de onderwerpen privacy en informatiebeveiliging).

De gemeente Amersfoort wil een solide en betrouwbare partner zijn naar haar inwoners, bedrijven, keten- en regiepartners en derden vanuit haar verantwoordelijkheid voor gegevens en informatie. Hierbij zijn een viertal doelstellingen geformuleerd met betrekking tot veiligheid, betrouwbaarheid, privacy- en beveiligingsbewustzijn en bestuurbaarheid[32]. Naast de geformuleerde doelstellingen zet de gemeente Amersfoort in op drie speerpunten voor informatiebeveiliging voor de periode 2019 - 2022:

- Speerpunt 1: Het belang voor informatiebeveiliging is duidelijk voor iedereen
- Speerpunt 2: Technische maatregelen groeien mee met het cyberdreigingsbeeld
- Speerpunt 3: Planning en Control cyclus (P&C) voor informatiebeveiliging is ingericht voor alle afdelingen[33]

Deze speerpunten krijgen een specifieke invulling in een jaarlijks informatiebeveiligingsbeleidsplan. In kwartaalrapportages wordt gerapporteerd over de speerpunten en de voortgang van de activiteiten uit het plan.

De jaarlijkse ENSIA-audit[34] is een belangrijk instrument voor de verantwoording over informatiebeveiliging. Deze audit, een self-assessment, wordt onder verantwoordelijkheid van een afdelingsmanager per afdeling die specifiek binnen de BIO een plek inneemt, uitgevoerd door een beveiligingsbeheerder (een aangewezen contactpersoon per afdeling). In 2019 heeft de gemeente geconcludeerd dat de self-assessment te pragmatisch werd ingevuld met te weinig aandacht voor het kunnen aantonen van de werking van beveiligingsmaatregelen.

Dit is aanleiding geweest voor een professionaliseringsslag waarbij onder andere een softwareapplicatie is aangeschaft om het Information Security Management System (ISMS) te ondersteunen. Het ISMS is het managementsysteem dat gebruikt wordt als beheersings- en verbetercyclus voor informatiebeveiliging. In de ISMS-tooling kunnen beveiligingsbeheerders informatie gerelateerd aan beveiligingsnormen en maatregelen (bijvoorbeeld met betrekking tot ENSIA, de BIO of de AVG) vastleggen. De tooling moet bijdragen aan de eenduidigheid in de genomen maatregelen en het aantoonbaar maken of er aan een norm wordt voldaan. Ook is het eenvoudiger om bepaalde maatregelen (zoals een uitwijkprocedure) te hergebruiken tussen afdelingen.

Per relevante afdeling (afdelingen die een specifieke plek in de BIO hebben) en voor een aantal specifieke processen is een GAP-analyse uitgevoerd om vast te stellen aan welke ENSIA-normen (aantoonbaar) wel of niet wordt voldaan. Deze analyse is de basis voor een verbeterplan voor de betreffende afdeling of proces. In dit verbeterplan worden de (geprioriteerde) maatregelen opgenomen gerelateerd aan de ENSIA-normen waar nog niet aan wordt voldaan. De verbeterplannen komen in overleg tussen de afdelingsmanager, beveiligingsbeheerder, adviseur informatiebeveiliging en CISO tot stand.

De self-assessments van de afdelingen leiden tot twee rapportages: een detailrapportage voor de afdelingsmanager en een algemene rapportage voor de directie.

[32] Volledige formulering van de doelstellingen is te vinden in het Informatiebeveiligingsbeleid 2019-2022, p.2

[33] Informatiebeveiligingsbeleid 2019-2022, p. 3 - 4

[34] ENSIA staat voor Eenduidige Normatiek Single Information Audit. Bij een ENSIA audit legt een gemeente in één keer verantwoording af over informatieveiligheid gebaseerd op de normen die gelden voor de Nederlandse overheid, de BIO.

2. Rollen en verantwoordelijkheden

2.1 Governance structuur

De rollen en verantwoordelijkheden ten opzichte van privacy zijn vastgelegd in verschillende documenten.[35] Iedereen die werkzaam is bij de gemeente heeft een verantwoordelijkheid om op een verantwoorde manier om te gaan met het verwerken van (persoons)gegevens. Tegelijkertijd kan men niet verwachten dat iedereen een expert is op het gebied van privacy en informatiebeveiliging en moet er een aantal rollen uit de AVG aan specifieke personen worden toegewezen.

Het college en (voor de wettelijke veiligheidstaken) de burgemeester zijn bestuurlijk verantwoordelijk; zij zijn verwerkingsverantwoordelijk in de zin van de AVG. Zij verantwoorden zich ten opzichte van de gemeenteraad en stellen de kaders vast. Er is een portefeuillehouder met het onderwerp privacy en informatiebeveiliging. De portefeuillehouder wordt stelselmatig geïnformeerd over mogelijke incidenten en datalekken. Het staat de raad vrij om het thema te agenderen en/of om te verzoeken over het thema bijgepraat te worden. Maar hiervan is in de huidige raadsperiode geen sprake geweest.

De directie is verantwoordelijk, binnen door het college gestelde kaders, voor de uitvoering van het Privacybeleid. De eerstelijns verantwoordelijkheid voor privacy ligt bij de afdelingsmanagers en hun sleutelpersonen. De afdeling Juridische zaken (JDA) is, als stelselhouder privacy, verantwoordelijk voor de centrale sturing en regie. JDA werkt nauw samen met de afdeling IT Dienstverlening en Advies (ITDA) die zich bezighouden met informatiemanagement, functioneel en technisch beheer en informatiebeveiliging in de brede zin.

Met betrekking tot informatiebeveiliging stelt het college de kaders vast in een informatiebeveiligingsbeleid, die gebaseerd is op landelijke en Europese wet- en regelgeving en landelijke normenkaders. De directie is verantwoordelijk voor de uitvoering van het informatiebeveiligingsbeleid en stuurt op de risico's. Zij evalueert periodiek de beleidskaders en stelt deze waar nodig bij.

Afdelingsmanagers zijn verantwoordelijk voor het maken van afspraken met externe partijen, waaronder de partijen waarbij taken in mandaat zijn neergelegd, inclusief het vastleggen van deze afspraken. Er geldt een brede managementverantwoording. Bij de verantwoording moeten managers, naast de financiële, ook over andere onderwerpen verantwoording afleggen waaronder privacy en informatiebeveiliging. Elke afdeling vult een verantwoordingsdocument in, sommige afdeling hebben ook al zo'n formulier voor privacy en informatiebeveiliging. Zo kunnen ze ook het college een goed en breed beeld geven.

Sleutelpersonen zijn werknemers die op de werkvloer het eerste aanspreekpunt zijn voor vragen over privacy en informatiebeveiliging. Om de kennis van sleutelpersonen op peil te houden en te reflecteren op hoe het gaat in de organisatie, is er regelmatig een sleutelpersonenoverleg. Deze overleggen zijn gemeentebreed en zijn vaak informerend van aard. Er worden vooral aandachtspunten gedeeld en presentaties gegeven. Eerst werden deze overleggen voorgezeten door de FG of een medewerker vanuit JDA, maar inmiddels zitten sleutelpersonen dit overleg zelf voor. Daarnaast zijn er bij sommige domeinen, zoals het sociaal domein, ook nog werkgroepen specifiek over privacy en informatiebeveiliging.

[35] Waaronder Gemeente Amersfoort, Privacy Governance 2020 v. 1.0 en Privacybeleid Gemeente Amersfoort 2019

2.2 Rol en positie van de raad

De gemeenteraad is de toezichthouder van het college van B&W en verwerkingsverantwoordelijk voor de gegevensverwerkingen van de gemeenteraad. De gemeenteraad is ook door het grote datalek uit 2016 erg alert op de ontwikkeling van privacy in de organisatie. Daarom wordt er met regelmaat gecommuniceerd met de raad over situaties die spelen rondom privacy. Op het moment dat een significant datalek speelt, wordt dit direct gecommuniceerd aan de raad.

De raad wordt verder geïnformeerd via de jaarrekening, het jaarverslag en het FG-verslag. Hele technische of juridische vraagstukken worden niet in de raad besproken. Bij de totstandkoming van de beginselen van beleid in 2019 is de raad intensiever op de hoogte gehouden. De gemeenteraad is nog beperkt betrokken bij het onderwerp informatiebeveiliging.

Tijdens de sessie met de raad werd duidelijk dat de raadsleden bewust en actief bezig zijn met privacy. Raadsleden zijn over het algemeen goed op de hoogte van de basisuitgangspunten van het beleid en hebben in het algemeen het vertrouwen dat Amersfoort de basis op orde heeft. Weliswaar verwijzen ze naar datalekken, maar ze zien een datalek eerder als een aanleiding dat hen het bredere belang van het onderwerp duidelijk heeft gemaakt. Nu de basis op orde is, denkt de raad na over de verdere uitdagingen. De raad ziet goede privacybescherming als een onderdeel van de gemeentelijke dienstverlening en rekent erop dat de gemeente ook in dat aspect de dienstverlening op orde heeft. Daarop wil de raad ook sturen en daarover willen ze geïnformeerd worden. Enkele raadsleden hebben belangstelling voor de beveiliging van de informatiesystemen en willen de zekerheid krijgen dat de gemeente ook wat dat betreft aandacht heeft voor de steeds geraffineerder wordende dreigingen. Immers, als de systemen worden gekraakt, kan dat ook consequenties hebben voor de privacy van de personen die in de systemen zijn opgenomen.

2.3 Toezichthouders

Er zijn verschillende betrokkenen met een toezichthoudende rol bij de gemeente die te maken hebben met privacy en informatiebeveiliging. De belangrijkste zijn de FG, CISO, concerncontroller en de archivaris.

De FG ziet toe op naleving van de privacywetgeving en adviseert over de bescherming en borging van een juiste verwerking van persoonsgegevens in werkprocessen conform de wetgeving. De FG houdt toezicht, adviseert over kaders en kan audits (laten) uitvoeren. De FG werkt zowel voor het college als de raad. De FG mag ook ongevraagd advies geven en doet dit ook af en toe. Hier wordt positief op gereageerd. De FG sluit aan bij verschillende overleggen, zoals bij de kerngroep en het sleutelpersonenoverleg. De functie van FG is functioneel belegd bij de afdeling JDA, maar in praktijk opereert de FG geheel onafhankelijk.

De CISO is verantwoordelijk voor het opstellen en implementeren van het informatiebeveiligingsbeleid en -plan. Hij is ook coördinator voor ENSIA en wordt ondersteund door adviseurs met verschillende achtergronden. De FG en de CISO spreken elkaar wekelijks.

De archivaris gaat na of overheidsinformatie behoorlijk wordt gearchiveerd en houdt hier toezicht op binnen de gemeente. Het kan daarbij ook gaan om persoonsgegevens.

De concerncontroller gaat na of het beleid van de gemeente conform de geldende afspraken wordt uitgevoerd. Hij bewaakt onder andere of de afspraken over privacybescherming en informatiebeveiliging in de praktijk ook worden nageleefd.

Deze vier toezichthouders spreken elkaar regelmatig in het zogenaamde ‘vierhoeksoverleg’. Hierin wordt gekeken waar overlap ligt tussen de deelgebieden waar zij toezicht op houden en of zij risico’s

hebben geconstateerd die de thema's van de andere toezichthouders ook raken. Ze letten ook op of er opvolging is van eerder gestelde maatregelen, bijvoorbeeld maatregelen die uit DPIA's naar voren zijn gekomen. Ze kwamen tot de conclusie dat er tooling nodig is om de risico's en maatregelen in de gaten te kunnen houden. De gemeente heeft deze tooling aangeschaft. Hierin willen de toezichthouders normenkaders, risico's, audits en ENSIA-controles bij elkaar brengen zodat zij een gezamenlijk zicht hebben op risico's, maatregelen en verbeterplannen.

Ieder kwartaal wordt er een rapportage opgesteld over privacy en informatiebeveiliging. Ieder kwartaal is er ook een bijeenkomst van de kerngroep privacy en informatiebeveiliging waar de kwartaalrapportages besproken worden.

3. Samenwerking met derden en (neven)effecten AVG

3.1 Afspraken en overeenkomsten

Bij de uitwisseling van persoonsgegevens met derden vereist de AVG dat hier duidelijke afspraken over moeten worden gemaakt.[36] Om hier een goed overzicht over te krijgen is er in 2019 een project over verwerkersovereenkomsten afgerond. Dit project had als doel een goed overzicht te krijgen van alle verwerkersovereenkomsten in de organisatie of waar verwerkersovereenkomsten afgesloten hadden moeten zijn. Daarin zijn bestaande verwerkersovereenkomsten bekeken en waar mogelijk verlengd. Verder zijn de ontbrekende verwerkersovereenkomsten toegevoegd. Alle verwerkersovereenkomsten zijn aangepast volgens de richtlijnen en de modelverwerkersovereenkomst van de VNG, maar zijn op verschillende punten ook uitgebreid. Er is een apart hoofdstuk toegevoegd in de verwerkersovereenkomsten waarin eisen met betrekking tot informatiebeveiliging worden gesteld, zoals het kunnen voldoen aan de BIO en het uitvoeren van een penetratietest. Indien nodig is de verwerkersovereenkomst aangevuld met een addendum met daarin aanvullende voorwaarden.

Uit gesprekken met derden blijkt dat de gemeente Amersfoort wordt gezien als een prettige samenwerkingspartner. De gemeente heeft met sommige partners veelvuldig contact. In overleggen waar dit relevant is wordt ook de omgang met persoonsgegevens besproken.

Derden met een eigen verwerkingsverantwoordelijkheid hebben ook een eigen verantwoordelijkheid en een eigen beleid ten aanzien van de wijze waarop zij omgaan met persoonsgegevens. In dat geval heeft de gemeente geen juridische basis om eisen te stellen (bijvoorbeeld via een overeenkomst) over de verwerking. Ook kan het zijn dat de gemeente samen met een andere partij verwerkingsverantwoordelijke is. Er kan dan gesproken worden van gezamenlijke verantwoordelijkheid. Wanneer er sprake is van een zelfstandige of gezamenlijke verwerkingsverantwoordelijkheid wordt er een dataleveringsovereenkomst gesloten en/of worden er bijvoorbeeld convenanten gesloten.

Op de wijze zoals hiervoor omschreven vereist Amersfoort dat een contractpartner waarmee Amersfoort persoonsgegevens deelt, hetzelfde beveiligingsniveau als die de gemeente zelf toepast. Er is op dit momenteel geen systeem dat het totaaloverzicht op de verwerkersovereenkomsten ondersteund.

[36] Zie hoofdstuk IV van de AVG

3.2 Toezicht

Het toezicht op de samenwerkingspartners op het vlak van informatiebeveiliging wordt nu ingericht met behulp van specifieke GRC-tooling[37], gekoppeld aan de ISMS-tooling[38]. Alle incidenten, PIA's, maatregelen en acties kunnen hierin worden geregistreerd én gemonitord. Ook kunnen de verantwoordelijken en actiehouders erin worden bijgehouden. De tooling kan ook notificaties sturen, bijvoorbeeld bij het bewaken van uit te voeren acties. In de huidige situatie is een dergelijke monitoring en strakke sturing op acties nog niet aanwezig. Dit gebeurt nog te ad hoc met het risico dat acties niet of te laat worden uitgevoerd, omdat er geen integraal overzicht is.

De gemeente heeft overigens niet gemerkt of geconstateerd dat er grote risico's spelen bij partners. Wat wel opgevallen is, is dat er oude overeenkomsten zijn waar eisen met betrekking tot informatiebeveiliging niet in staan.[39] Het hoofdstuk over informatiebeveiliging is pas in 2019 toegevoegd aan de overeenkomst. Het is zaak om elke drie jaar de overeenkomst te evalueren, zodat dit op termijn wordt opgelost.

Bij het goed regelen van samenwerking met derden zijn verschillende adviseurs betrokken. In de samenwerking met bijvoorbeeld de veiligheidsregio en de GGD is ook de bestuurlijke verantwoordelijkheid en borging geregeld. Werknemers van de gemeente zorgen dat dit conform de AVG plaatsvindt. Welke afspraken er met een partner worden gemaakt, hangt af van de aard van de samenwerking en de juridische verhouding tussen de gemeente en de samenwerkingspartner, bijvoorbeeld of deze een eigen zelfstandige verwerkingsverantwoordelijkheid heeft of niet. De afdelingsmanager legt verantwoording af over de (rechtmatigheid van) de processen die onder zijn afdeling vallen. De FG en CISO houden daar toezicht op.

De samenwerkingen verlopen in het algemeen goed, hoewel er verschillen zijn per samenwerkingspartner. Het is belangrijk om alert te blijven op wat er gebeurt en hoe het gebeurt. De gemeente gaat na of gemaakte afspraken met samenwerkingspartners op de juiste manier conform de AVG worden uitgevoerd door dit regelmatig te checken en hierover in gesprek te blijven met de samenwerkingspartners.

3.3 Informatiebeveiliging

Voor tijdelijke technische ondersteuning of als een deel van de dienstverlening door externen wordt uitgevoerd, kan toegang tot systemen van de gemeente door externe partijen nodig zijn. In het Beleid Logische toegangsbeveiliging[40] staat beschreven op welke manier externe partijen toegang krijgen tot gegevens vanuit de gemeente Amersfoort. In dit beleid is ook opgenomen dat alle externe partijen die werkzaamheden uitvoeren, gebruik maken van een account waarmee de uitgevoerde handelingen te herleiden zijn tot een specifiek persoon.

In het Beleid Logische toegangsbeveiliging wordt beschreven dat het de bedoeling is dat externe partijen die op afstand ondersteuning leveren, een beveiligde verbinding onder controle van Amersfoort gebruiken en alleen toegang krijgen na goedkeuring van Amersfoort. Deze toegang is altijd tijdelijk. Externe partijen die permanente toegang nodig hebben, maken gebruik van een externe

---

[37] GRC-tooling staat voor Governance, Risk en Compliance tooling en is gericht op het beheren van de algehele governance van een organisatie.

[38] ISMS- tooling staat voor Information Security Management System (SIMS). Deze tooling ondersteunt bij het nemen van informatiebeveiligingsmaatregelen.

[39] In het onderzoek is niet vastgesteld wat het actuele aandeel is van dergelijke 'verouderde' overeenkomsten.

[40] Beleid Logische toegangbeveiliging, gemeente Amersfoort

koppeling. In het beleid staat verder benoemd dat de handelingen van externe partijen worden gelogd en beveiligd.

3.4 AVG knelpunten, beperkingen en risico's

Binnen de gemeente is oneigenlijk gebruik van de AVG niet bekend. Over het algemeen geven medewerkers aan dat bij beperkingen ten gevolge van de AVG of misvatting over privacyregelgeving advies gevraagd wordt en wordt overlegd met JDA. Er wordt steeds een praktische vertaalslag gemaakt. Privacy moet onderdeel worden van ieders reguliere werkzaamheden. Echte misstanden, zoals dat mensen bewust de AVG niet handhaven of de AVG wordt gebruikt om informatie niet te delen, terwijl hiervoor wel de ruimte is, zijn niet bekend. Er is altijd ruimte om knelpunten te bespreken. Hierbij spelen de sleutelpersonen een belangrijke rol. Ze signaleren problemen en kunnen advies van de privacyjurist vragen. Dit heeft geleid tot een actieve betrokkenheid van de juristen.

Soms worden er bij de gemeente tegenstrijdigheden vastgesteld tussen privacywetgeving en voorschriften voor archivering. Het wegnemen van deze tegenstrijdigheden valt vaak niet in de invloedsfeer van de gemeente, omdat de tegenstrijdigheden niet voortkomen uit gemeentelijke regelgeving of gemeentelijk beleid. De bedoelde tegenstrijdigheden betreffen met name de bewaartermijnen. Binnen de mogelijkheden van de gemeente wordt in individuele situaties een afweging gemaakt. In het veiligheidsdomein wordt de AVG wel soms als beperkend ervaren, bijvoorbeeld bij het delen of ontvangen van informatie in de samenwerking met derden (zie deelvraag 7). Dit kan bijvoorbeeld het geval zijn bij samenwerkingen met veiligheidspartijen waarmee niet altijd gegevens mogen worden uitgewisseld of waarbij onduidelijkheid is wanneer welke gegevens mogen worden uitgewisseld. Ook vraagt de AVG soms dat (bestaande) systemen anders moeten worden ingericht. Dit is niet zozeer een beperking of een probleem, maar de AVG vraagt de organisatie wel dat aan de voorkant systemen zo zijn ingericht dat hier ook conform AVG mee te werken is. Soms blijkt iets dan toch mogelijk, maar duurt het iets langer om het goed te regelen.

Binnen de gemeente Amersfoort zijn medewerkers zich over het algemeen bewust van privacyrisico's. Bij twijfel zullen medewerkers eerder iets niet delen en om advies vragen, dan het 'maar gewoon doen' en achteraf kijken of dat wel goed is.

De gemeente heeft een proces voor het melden en registreren van datalekken. Medewerkers melden (mogelijke) datalekken ook daadwerkelijk: door incidenten in het verleden is hier veel aandacht voor. Werknemers worden geïnformeerd over privacy om datalekken te voorkomen, maar tegelijkertijd wordt er erkend dat menselijke fouten zullen blijven bestaan en dat als dit gebeurt, hier adequaat mee moet worden omgesprongen. Er heerst geen afrekencultuur waardoor mensen lekken durven te melden. Mensen zeggen elkaar aan te spreken wanneer er kleine en grote fouten worden gemaakt. Daarnaast helpt het dat er regelmatig DPIA's worden uitgevoerd.

Privacyrisico's worden systematisch door middel van DPIA's voor een verwerking start in kaart gebracht. Deze DPIA's worden regelmatig uitgevoerd en wanneer nodig geëvalueerd. Om te bepalen of een DPIA moet worden uitgevoerd is er een Quickscan opgesteld. Bij het uitvoeren van de DPIA zelf kan er een leidraad worden gevolgd.[41]

Meldingen, dit kunnen incidenten, signalen of datalekken zijn, worden opgenomen in de kwartaalrapportages. Deze meldingen worden intentioneel breed geregistreerd, zodat er niets over het hoofd wordt gezien. Incidenten worden behandeld volgens vastgestelde Werkwijzen en een Protocol.[42] In de praktijk wordt hiernaar gehandeld. Er wordt geregistreerd welke van de meldingen

[41] DPIA-Leidraad v. 1.2

[42] 'Protocol Afhandelteam Incidentenmeldingen' en 'Werkwijze Afhandelteam Incidentenmeldingen'

datalekken betreffen. Indien er als gevolg van de inbreuk waarschijnlijk sprake is van een risico of hoog risico op de rechten en vrijheden worden deze gemeld bij respectievelijk de AP en betrokkenen.

De meest voorkomende melding is dat er persoonsgegevens zijn verstuurd of afgegeven aan een onjuist ontvanger. Er wordt door leidinggevenden en de sleutelpersonen actief gewerkt aan een werkklimaat waarbij medewerkers fouten durven te melden.

In 2018 zijn er 75 meldingen gerapporteerd, waarvan 45 datalekken. Hiervan zijn er 16 gemeld bij de Autoriteit Persoonsgegevens (AP). In 2019 zijn er 67 meldingen gerapporteerd waarvan 47 datalekken. Hiervan zijn er 19 gemeld bij de AP. In 2020 zijn er 50 meldingen gerapporteerd, waarvan 46 datalekken. Hiervan zijn er 6 gemeld bij de AP.

4. Inwoners

Op de website van de gemeente is een Privacyverklaring[43] te vinden. Hierin wordt uitgelegd hoe de gemeente omgaat met de verwerking van persoonsgegevens. Er wordt toegelicht hoe er wordt omgegaan met uitwisseling van gegevens met derden en waarom en hoe er met gegevens om wordt gegaan.[44] Ook worden de privacyrechten van inwoners toegelicht en uitgelegd en hoe zij hier een beroep op kunnen doen en wanneer ze een klacht kunnen indienen.

Het contact met inwoners over privacy vindt op verschillende plekken plaatsen. Er is een participatieplatform, ‘Met Amersfoort’, waarbij JDA adviseert. Bij dit platform worden inwoners betrokken en komen onderwerpen en ideeën van inwoners van buiten naar binnen. Dit gebeurt in de vorm van (online) bijeenkomsten[45]. Tevens is er los van het platform een burgerpanel, Technologisch Burgerpanel Amersfoort, dat meedenkt over ontwikkelingen rondom Amersfoort als Smart City. Zij denken mee over de inzet van technologie in de stad en geven de gemeente feedback hierover. Op deze manier kan het burgerperspectief worden betrokken bij het maken van beleid. Kwartiermaker van dit technologisch burgerpanel is POWER (Prettig Ouder Worden en Relativeren). POWER bestaat uit leden boven de leeftijd van 50. Met kennis en vaardigheden willen zij iets betekenen voor de stad. Hierbij speelt digitalisering een belangrijke rol. Het doel hierachter is dat gewone burgers beoordelen wat voor effect gemeentelijke digitaliseringsbeleid heeft op het dagelijks leven.

Klachten van inwoners over de bescherming van persoonsgegevens worden meestal gericht aan de FG, maar niet uitsluitend. Klachten kunnen ook bij andere medewerkers binnenkomen, omdat een inwoner daar al contact mee heeft. Er is door de gemeente (nog) geen onderzoek of inventarisatie gedaan naar het perspectief van inwoners op de bescherming van persoonsgegevens door de gemeente. Medewerkers van de gemeente hebben de indruk dat inwoners weten hoe ze vragen kunnen stellen aan de gemeente. Er komen niet veel vragen binnen. Incidenten worden breed geregistreerd. Ook bij twijfel of iets werkelijk een schending is van privacy wordt het geregistreerd als melding.

[43] https://www.amersfoort.nl/bericht/privacyverklaring-gemeente-amersfoort.htm

[44] https://www.amersfoort.nl/bericht/digitaal-samenwerken-met-gemeente-amersfoort-of-de-wijkteams.htm

[45] https://metamersfoort.nl/met+amersfoort/default.aspx

BIJLAGE 5 OVERZICHT MELDINGEN EN DATALEKKEN

		totaal aantal (incident-) meldingen	waarvan een datalek	waarvan melding bij AP
2018	Q1	20	9	2
	Q2	26	13	5
	Q3	21	16	6
	Q4	8	7	3
2019	Q1	14	7	4
	Q2	18	14	2
	Q3	13	11	6
	Q4	22	15	7
2020	Q1	20	18	1
	Q2	6	6	1
	Q3	11	10	3
	Q4	13	12	1

BIJLAGE 6 GEÏNTERVIEWDE PERSONEN

#	datum	functie
1	29 oktober 2020	CISO
2	30 oktober 2020	Functionaris Gegevensbescherming (tijdelijk gedeelde functie)
3	30 oktober 2020	Functionaris Gegevensbescherming (tijdelijk gedeelde functie)
4	9 november 2020	Teammanager Privacy
5	10 november 2020	Procesbegeleider
6	10 november 2020	Sleutelpersoon Privacy
7	11 november 2020	Adviseur Concerncontrol
8	11 november 2020	Concerncontroller
9	13 november 2020	Burgemeester
10	13 november 2020	Adviseur Informatiebeveiliging
11	13 november 2020	Senior Juridisch Adviseur Privacy
12	13 november 2020	Voorzitter Kerngroep Privacy
13	18 november 2020	Wethouder & Portefeuillehouder Privacy en Informatiebeveiliging
14	18 november 2020	CIO
15	4 januari 2021	Secretaris Cliëntenraad Werk & Inkomen
16	5 januari 2021	Vertegenwoordiger POWER
17	11 februari 2021	Solutions Factory (samenwerkingspartner)
18	12 februari 2021	Reclassering Amersfoort

Bijlage 7 Overzicht gebruikte documenten

Landelijke bronnen

#	documentnaam	versie	datum
1	Standaard Verwerkersovereenkomst Gemeenten	2.1	11 november 2019
2	Gegevensverwerking en privacy		

Bronnen gemeente Amersfoort

#	documentnaam	versie	datum
1	Stadsberichten: Nieuws van de gemeente Amersfoort	-	26 augustus 2020
2	Privacyverklaring gemeente Amersfoort	-	7 oktober 2020
3	Procesplan Privacy Governance	1.3	juli 2020
4	Beantwoording Feitelijke vragen Jaarstukken 2019		9 juni 2020
5	Dataleveringsovereenkomst		2020
6	Aanbestedingsleidraad	1.0	
7	Informatiebeveiligingsbeleid 2019-2022		25 juni 2019
8	Integriteits- en geheimhoudingsverklaring Externe Medewerkers		
9	Jaarplan Privacy 2020	1.2	2020
10	Jaarstukken 2019		9 juni 2020
11	Meldingen 2018-2020		
12	Privacy Governance 2020	1.0	
13	Privacybeleid Gemeente Amersfoort 2019	1.0	
14	Rapport IV Governance Gemeente Amersfoort	1.0	23 april 2020
15	Register van verwerkingen december 2019		
16	Eindrapportage DPIA project juli		8 juni 2020
17	Beleid logische toegangsbeveiliging		Januari 2019
18	Beleid Mobile Device Management		Maart 2020
19	Bewustwordingsprogramma PIV Amersfoort	1.0	
20	DPIA-leidraad	1.2	
21	Format Brief aanstelling sleutelpersoon (functie-inhoud)		
22	Format DPIA-quickscan	1.1	
23	Format verslag melding datalekken		
24	Pre-Audit Informatiehuishouding Gemeente Amersfoort		
25	Governance DPIA	1.0	Juli 2020
26	Handboek werken met persoonsgegevens		27 oktober 2020
27	Opzet E-learningprogramma Bewustwording IB & Privacy		
28	Protocol Afhandelteam Incidentmeldingen	1.0	November 2019
29	Protocol Veilig delen van informatie		Oktober 2018
30	Rapportage Programma Standaard VWO	1.1	20 december 2019
31	Werkwijze Afhandelteam Incidentmeldingen		November 2019