Jaarverslag 2020

Functionaris Gegevensbescherming Gemeente Groningen

Auteur: Menno van Heumen
Datum: 8 oktober 2021
Status: definitief

Inhoud

Samenvatting

Als onafhankelijk toezichthouder van de gemeente constateert de Functionaris Gegevensbescherming (FG) dat de Gemeente Groningen ten opzichte van 2018, het jaar dat de Algemene Verordening Gegevensbescherming (AVG) van toepassing is geworden, geringe vorderingen heeft gemaakt als het gaat om de compliance-eisen die de wet met zich meebrengt .

Op vijf aspecten scoort de gemeente naar het oordeel van de FG nog niet voldoende: het op orde hebben van het register van de verwerkingen, het uitvoeren van gegevenseffectbeoordelingen (PIA's worden niet zelfstandig uitgevoerd), het toepassen van privacy-by-design en -by-default (komt nauwelijks voor), de invulling van de FG-taak (te weinig capaciteit), en het nemen van preventieve maatregelen ter voorkoming van datalekken (onvoldoende). Het informeren van betrokkenen, de aantoonbaarheid van toestemming van betrokkenen en de verwerkersovereenkomsten scoren een magere voldoende. De borging van de rechten van betrokkenen en de aandacht voor bewustwording van medewerkers zijn van voldoende niveau.

In een maatschappij die in toenemende mate gegevens van burgers gebruikt is het de vraag of de gemeente op deze wijze haar verantwoordelijkheid voldoende kan waarmaken.

De volgende kerncijfers over 2020 zijn beschikbaar:

Verwerkingen	196	Cijfer uit 2018
Datalekken	131	Gemeld bij de AP: 0
PIA's	36	
Verzoeken om inzage	<5	Via JUZA lopende verzoeken
Burgercontacten	4	
Verwerkersovereenkomsten	onbekend	

De FG adviseert, gelet op de verbeteringen die nodig zijn, de Concerndirectie een besluit te nemen aangaande het maken van afspraken met de afzonderlijke directeuren als onderdeel van de managementovereenkomst over de volgende aspecten:

- het aantal uit te voeren PIA's;
- het in afstemming met de FG publiceren van de verwerkingen op de website van de gemeente Groningen;
- welke bijdrage er geleverd wordt op het gebied van bewustwording van de eigen medewerkers.

Daarnaast zullen de prioriteiten voor de FG liggen op de volgende gebieden:

- het overdragen van de begeleidende rol bij de PIA aan Regie IA (zodat FG aandacht kan geven aan andere onderwerpen gelet op de beperkte capaciteit);
- uitdragen van informatie rondom het fenomeen datalekken (preventie);
- het bij de CD aandragen van mogelijke aanvullende afspraken die gemaakt kunnen worden met de verschillende directies.

Inleiding

Het jaarverslag 2020 van de Functionaris Gegevensbescherming (FG) van de gemeente Groningen beoogt verantwoording af te leggen van de taak van de FG zoals die is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG; art 39). In het kort omvat deze taak het informeren en adviseren van het bestuur en de werknemers van de gemeente inzake hun verplichtingen, het uitoefenen van toezicht op naleving van de AVG, advisering met betrekking tot de uitvoering van gegevenseffectbeoordelingen (privacy impact assessment ofwel PIA) en het onderhouden van contacten met de Autoriteit Persoonsgegevens (AP). De FG voert zijn dagelijkse werkzaamheden uit samen met de Privacy Officer van Juridische Zaken. De FG van de gemeente is ook de FG van de stichting WIJ en van GGD Groningen, maar dit verslag heeft geen betrekking op die twee organisaties omdat deze een zelfstandig rechtspersoon zijn.

De verantwoording zoals in dit jaarverslag is verwoord gaat in op het algemene beeld van de compliance ten aanzien van de AVG, de uitgevoerde activiteiten en opgeleverde producten, de bevindingen over het jaar 2019 en 2020 en de aandachtspunten voor 2021. Het jaar 2020 werd voor de FG gekenmerkt door de pandemie, met alle gevolgen voor de werksituatie binnen de gemeente en de aandacht die dat vergde voor het management en de medewerkers. Een groot deel van het jaar heeft de FG zonder de Privacy Officer moeten werken en de ondersteuning vanuit de organisatie is beperkt. Daarom is er in 2020 geen jaarverslag over 2019 uitgebracht.

Het jaarverslag van de FG wordt aangeboden aan het college van B&W omdat zij eindverantwoordelijk is voor de verwerking van de persoonsgegevens. Het college dient kennis te nemen van het jaarverslag en kan een uitspraak doen over de vermelde aandachtspunten voor 2021. Daarnaast kan het college het jaarverslag ter informatie aanbieden aan de gemeenteraad en het publiceren op de website van de gemeente.

Algemeen beeld compliance AVG

2020 Is twee jaar na de invoering van de Algemene Verordening Gegevensbescherming (AVG). De gemeente was in 2018 klaar voor de AVG, maar nog niet in staat om volledig te voldoen aan de AVG. De organisatie heeft meer ervaring kunnen opdoen in het werken met de AVG en maakt daardoor stapjes in de goede richting ten opzichte van het beeld over 2018.

In 2019 was er sprake van enige uitbouw van wat in 2018 is begonnen: investeren in voorlichten van de organisatie door het houden van workshops, berichten op intranet in de speciale nieuwsgroep over privacy en de campagne 'zet jezelf op scherp'. Deze campagne werd gebouwd rond een periodieke kennisquiz met een competitie-element voor alle afdelingen. Al deze activiteiten werden uitgevoerd in nauwe samenwerking met het team Informatiebeveiliging bij het SSC I&S.
Daarnaast werden in 2019 de eerste stappen gezet bij het gebruik van de PIA (privacy impact assessment), een middel om risico's op te sporen en maatregelen te nemen. Een PIA is een verplicht instrument wanneer het risicobeeld onbekend is. Het jaar was ook vooral bedoeld om ervaring op te doen 'op de werkvloer'; zien hoe de regelgeving uitpakt en of de gemeente in de praktijk kan omgaan met hetgeen in 2018 is ontwikkeld en geïmplementeerd.

2020 is voor de Functionaris Gegevensbescherming (FG) een jaar geworden van aandacht voor de noodzakelijke dingen: afhandeling datalekken, voorlichting en begeleiding van PIA's daar waar er om gevraagd werd. Deze enigszins reactieve benadering vloeit voort uit de aandacht van het management, die begrijpelijk sterk gericht is op continuïteit van hun primaire proces in de Corona periode. Daarnaast bestond het privacyteam het grootste gedeelte van het jaar uit 1 persoon in plaats van de 3 medewerkers in de jaren daarvoor.

De FG hanteert tien aspecten voor het beoordelen van de mate van het voldoen aan de AVG, gebaseerd op art.24 over de plichten van de verwerkingsverantwoordelijke. De beoordeling door de FG van deze compliance-eisen laten ultimo 2020 zien dat het nog te vroeg is om te spreken van het volledig voldoen aan deze eisen.

Korte karakterisering van de tien eisen, welke in meer detail terugkomen bij de uitgevoerde activiteiten, opgeleverde producten en de bevindingen geeft het volgende beeld:

aspect	toelichting
Bewustwording	In samenwerking met Juridische Zaken (JUZA) en het Informatiebeveiligingsteam (onderdeel van SSC I&S Regie) is er binnen de organisatie veel aandacht voor bewustwording. Dit is vooral gericht op de medewerker en minder op het management. Bewustwording is het begin van bewustzijn.
Register verwerkingen	De FG heeft met hulp van de directies een register opgebouwd. De kwaliteit daarvan is nog onvoldoende om dit in- en extern te publiceren. Dit was in 2018 zo, en is niet veranderd.
Rechten van betrokkenen	Kenbaar gemaakt op de website van de gemeente, procedureel geborgd door het onderbrengen van dit proces bij JUZA in analogie van WOB-verzoeken. Uitoefening van de rechten komt sporadisch voor.
Toestemming betrokkenen	Voor de meest voorkomende, primaire diensten die de gemeente levert bestaat de grondslag veelal uit de uitvoering van een wettelijke verplichting of het algemeen belang. Toch zijn er situaties waarbij toestemming expliciet gevraagd moet worden. Denk daarbij aan toestemming voor doeleinden zoals nieuwsbrieven, het doen van tevredenheidsonderzoeken en enquêtes, het doorbreken van geheimhoudingsplicht, etc. Bij het inventariseren van

	verwerkingen wordt dit aspect benoemd. Er is nog niet vastgesteld of aantoonbaar gemaakt kan worden dat de toestemming ondubbelzinnig en actief is gegeven.
Informeren van betrokkenen	Wanneer de gemeente gegevens gaat verzamelen moeten betrokkenen hierover worden geïnformeerd. Naast het ontbreken van een gepubliceerd register bestaat bij de FG het beeld dat in een aantal gevallen betrokkenen minder concreet worden geïnformeerd over het verwerken van hun gegevens.
Gegevenseffect-beoordelingen (PIA's)	Van dit middel wordt inmiddels tientallen malen per jaar gebruik gemaakt en dat is een goede ontwikkeling. Het is wel zo dat de inbreng van de FG daarbij groot is ('toetst soms wat hij zelf voorstelt'). De organisatie is nog niet in staat hier zelfstandig invulling aan te geven. Daarnaast worden genomen maatregelen zelden teruggekoppeld aan de FG.
Privacy-by-design en privacy-by-default	Waar PIA's inzicht geven in nodige maatregelen rond verwerkingen zijn deze twee aspecten vooral bedoeld om bij het procesontwerp privacyaspecten als dataminimalisatie en opslagbeperkingen (beginselen AVG art 5) standaard mee te nemen. Dit vindt nog nauwelijks aantoonbaar plaats. Wel een pluim voor het fietsmonitorproject. Deze innovatieve ontwikkeling heeft vanaf het begin oog gehad voor privacy en de FG actief betrokken.
Functionaris Gegevensbescherming	Deze is aanwezig (bij JUZA), maar heeft geen vervanger en kreeg in 2020 nog te weinig juridische en praktische ondersteuning bij de uitvoering van zijn taken.
Meldplicht datalekken	Er is een vastgestelde procedure voor het onderzoeken en registreren van meldingen van mogelijke datalekken. Informatiebeveiliging houdt hiervan een register bij. Het aantal meldingen ligt op een bescheiden niveau (ruim honderd per jaar). Het aantal dat moet worden gemeld bij de AP is gedaald tot nul, een ongeloofwaardig aantal. De oorzaak zal waarschijnlijk liggen in het massale thuiswerken waarbij de meldingsbereidheid lager ligt. Een aantal systemen bevat vanwege gebrekkige controle onnodig veel persoonsgegevens (eSuite, ServiceNow).
Verwerkersovereenkomsten	Er is een standaard ontwikkeld voor het aangaan van verwerkersovereenkomsten, gebaseerd op het format van de VNG dat in toenemende mate wordt gebruikt. Leveranciers komen nog wel eens met hun eigen 'standaard'. Er bestaat geen totaaloverzicht van de aanwezige (en afwezige) overeenkomsten.

<u>Conclusie:</u>
Samenvattend kan gesteld worden dat ten opzichte van 2018, de start van de AVG, de gemeente met kleine stapjes zet bij het voldoen aan de AVG, maar dat er nog een compliance risico bestaat.

Belangrijke verbeterpunten zijn:
- het publiceren van het verwerkingenregister;
- het zelfstandig uitvoeren van de gegevenseffectbeoordelingen (PIA's);
- het toepassen van privacy-by-design.

Daarnaast zijn er accenten te leggen op de aspecten die op zichzelf al goed gaan:
- aandacht voor de meldingsbereidheid van datalekken;
- het bespreken van de status van de verwerkersovereenkomsten.

Bij de vormgeving van deze punten is het wenselijk dit slim te organiseren opdat de capaciteit van de FG en het privacyteam nu eenmaal beperkt is.

Uitgevoerde activiteiten

In 2019 en 2020 zijn de volgende activiteiten uitgevoerd:

Bewustwording
Een belangrijke sleutel tot succes is de bewustwording van medewerkers over het verantwoord omgaan met persoonsgegevens. Belangrijkste activiteiten zijn geweest:

- Het houden van (online) bijeenkomsten met medewerkers en leidinggevenden over het werken met persoonsgegevens.
- Het mede organiseren van de game 'Zet jezelf op scherp' waarin enkele specifieke privacyvragen werden gesteld. De deelnamegraad liep gaandeweg terug zodat na vier games deze activiteit is gestopt.
- Het laten ontwikkelen van een speciale e-learning leerlijn die in 2021 beschikbaar wordt gesteld aan alle medewerkers via het Leer Management Systeem van de afdeling HRM.
- Het plaatsen van berichten op de speciale intranetgroep 'alles over privacy'.

Deze activiteiten zijn uitgevoerd in nauwe samenwerking met het team Informatiebeveiliging van het SSC I&S (Informatie en Services).

Ontwikkelen hulpmiddelen
In samenwerking met Informatiebeheer en Informatiebeveiliging zijn drie afzonderlijke hulpmiddelen samengevoegd die in sommige gevallen maken dat gesprekken met de opdrachtgever en materiedeskundigen beperkt worden in aantal en omvang. Het gaat daarbij om de risico-inventarisaties op drie verschillende gebieden: informatiebeheer, privacy en security (beschikbaarheid, integriteit, vertrouwelijkheid). Deze samenvoeging kan niet altijd gebruikt worden omdat een informatiesysteem niet altijd samenvalt met één proces.

Advisering
Het privacyteam (de FG en de PO) heeft een algemeen e-mailadres beschikbaar (privacy@groningen.nl) waar medewerkers terecht kunnen met vragen, opmerkingen en verzoeken tot ondersteuning en advies. Op dat adres komen per jaar *honderden* berichten binnen die de organisatie in staat hebben gesteld het privacy-aspect bij het oplossen van hun vraagstukken adequaat mee te nemen. Er is sprake van een grote diversiteit aan herkomst en aard van de vraagstukken. Een veel voorkomende vraag is nog steeds: 'mag dit van de AVG?'. Omdat de AVG weinig specifiek normerend is vergt het antwoord op deze vraag veelal maatwerk. Het uitgangspunt hierbij is altijd dat van de AVG veel mag maar dat dit wel vereist dat 'het huiswerk' gemaakt wordt. Daarmee wordt bedoeld dat de specifieke kenmerken van een verwerking zoals deze worden benoemd in de wet duidelijk gemaakt worden. Dit vergt kennis en kunde binnen de organisatieonderdelen en die is niet altijd aanwezig.
De FG adviseert desgevraagd de klachtenfunctionaris(sen) en de ombudsman binnen de gemeente wanneer burgers zich bij hen hebben gemeld met klachten waarbij privacy ook een steeds vaker genoemd aspect is.

Opgeleverde producten

In 2019 en 2020 zijn er geen noemenswaardige producten rond het thema privacy opgeleverd. Wel is een start gemaakt met de noodzakelijke herziening van het 'reglement e-mail en internetgebruik' voor medewerkers. Deze regeling is sterk verouderd en nodig aan herziening toe; de geldigheidstermijn is al enkele jaren overschreden.

Conclusie:
De uitgevoerde activiteiten en opgeleverde producten voorzien in beantwoording van vragen die leven bij de medewerkers van de gemeente, en dragen bij aan een verdere toename van de mate van AVG-compliance.

Jurisdictie

De gemeente Groningen is bij diverse organisaties en instellingen direct of zijdelings betrokken. Van belang is altijd in hoeverre de gemeente verantwoordelijkheid draagt bij het verwerken van persoonsgegevens. Dat is nodig voor het kunnen bepalen welke activiteiten uitgevoerd moeten worden vanuit de AVG gezien, wie er moet handelen bij een optredend datalek en waar bijvoorbeeld de aansprakelijkheid ligt bij het niet nakomen van verplichtingen. Het bepaalt ook of de FG van de gemeente toezichthouder is, of juist niet. De gemeente maakt dit zichtbaar voor het publiek middels een groot aantal websites (tussen de 50 en de 100) waar feitelijk juiste informatie hoort te staan over de omgang met persoonsgegevens. Dat is niet altijd het geval.

Er zijn diverse verschijningsvormen van de rollen die de gemeente heeft:

Volledig eindverantwoordelijk:
Er sprake van directe betrokkenheid bij De Oosterpoort/Stadsschouwburg (Spot Groningen), het Centrum voor Beeldende Kunst en Sport050 die zich op hun eigen wijze naar de buitenwereld presenteren.

Voor de FG zijn deze organisatie-onderdelen gelijk aan iedere afzonderlijke directie binnen de gemeente en dat is prima werkbaar.

Gemeenschappelijke regelingen:
De gemeente participeert in een negental Gemeenschappelijke Regelingen (GR) waarbij initieel sprake zal zijn van gedeelde verantwoordelijkheid. Voorbeeld is de RIGG als onderdeel van de GR Publieke Gezondheid. Hoewel de gemeente de uitvoering voor haar rekening neemt zijn de deelnemende gemeenten allen verantwoordelijk. De GGD Groningen heeft overigens op grond van diezelfde GR een zelfstandige status gekregen waarmee deze gezondheidsdienst volledig eindverantwoordelijk is voor de verwerking van de persoonsgegevens.

Als FG van de RIGG en de GGD bestaat er goed zicht op de verantwoordelijkheidsverdeling, maar de FG heeft dat niet van de andere acht Gemeenschappelijke Regelingen.

Zijdelingse betrokkenheid:
Deze categorie kent diverse verschijningsvormen:

(i). Met betrekking tot de stichting WIJ kan gesteld worden dat vanuit de criteria opdrachtbepaling en inzet van middelen de gemeente ook eindverantwoordelijk lijkt voor de verwerking. In de praktijk acteert de stichting als zelfstandig rechtspersoon en neemt haar verantwoordelijkheid bij het verwerken van persoonsgegevens.

De FG van de gemeente is ook de FG van WIJ waardoor de grens van verantwoordelijkheid goed bewaakt kan worden; het toezicht functioneert wat dat betreft goed.

(ii). Met betrekking tot de Arbeidsmarktregio en het RMC (Regionaal Meld- en Coördinatiepunt; leerlingenzaken) heeft de stad een centrale rol in de provincie of regio welke is afgedwongen door de landelijke overheid. Dat brengt met zich mee dat de FG van de gemeente betrokken kan worden bij activiteiten die deze samenwerkingen uitvoeren. Dat gebeurt niet consequent of structureel waardoor het compliance beeld van deze samenwerkingen onvolledig is. Dat geldt zeker wanneer de regio zelf ook weer samenwerkingsverbanden aangaat. Dit speelt ondermeer bij de aandacht die er moet zijn voor schoolgaande jeugd (tot de leeftijd van 27 jaar (..)). Dit brengt veel juridisch getint maatwerk met zich mee en zou gepaard moeten gaan met duidelijke informatievoorziening naar de betrokken burger.

Het is voor de FG niet duidelijk of zijn beeld van de regionale organisaties volledig en juist is.

(iii). Daarnaast kent de gemeente samenwerkingen die zijn vastgelegd in convenantvorm zoals het Zorg- en Veiligheids Huis, en waarbij ieders verantwoordelijkheid op het gebied van de verwerking van persoonsgegevens is vastgelegd. Vaak is ook hier een centrale rol voor de gemeente bij onderlinge uitwisseling van gegevens waardoor de FG in de gelegenheid is zijn rol te spelen. Gelet op vele betrokkenen is het vaststellen van de samenwerking en invulling geven aan privacyaspecten een langdurige kwestie. In de tussentijd is er wel een operationele situatie die nog niet volledig concreet in beeld is gebracht.

Er zijn meer vormen van samenwerking. Bijvoorbeeld op het gebied van de mobiliteit: ‘Groningen Bereikbaar’ waarbij de gemeente samenwerkt met de provincies Groningen en Drenthe. Door gebruikmaking van moderne technologie komen daar privacyvraagstukken naar voren die niet altijd leiden tot heldere verantwoordelijkheidsverdelingen.

<u>De gemeente als verwerker</u>
De ICT infrastructuur van de gemeente wordt ook gebruikt door GGD Groningen, het Noordelijk Belastingkantoor en de stichting WIJ. De gemeente handelt dan vanuit het AVG perspectief als een verwerker en heeft daarom met die organisaties een verwerkersovereenkomst. Dat stelt vervolgens eisen aan de gemeente op het punt van het aantoonbaar kunnen leveren van een adequaat beveiligingsniveau dat passend is bij de gegevens die worden verwerkt. In hoeverre de gemeente voldoet aan de NEN-normen op het gebied van het verwerken van gezondheidsgegevens is niet helder in kaart gebracht.
De gemeente heeft voor het onderhoud van de infrastructuur een contract gesloten met Fujitsu. De mate waarin deze organisatie in staat is te voldoen aan de beveiligingseisen conform de Baseline Informatiebeveiliging Overheid (BIO) staat binnen de I&S organisatie consequent op de agenda.

<u>Conclusie:</u>
Het verwerven van meer inzicht in de verwerkingsverantwoordelijkheden die de gemeente met al haar samenwerkingen heeft, en de bijbehorende privacyrisico’s die daardoor worden gelopen, is een aandachtspunt.

Bevindingen

De kerncijfers van 2020 zijn:

Verwerkingen	196	Cijfer uit 2018
Datalekken	131	Gemeld bij de AP: 0
PIA's	36	
Verzoeken om inzage	<5	Via JUZA lopende verzoeken
Burgercontacten	4	
Verwerkersovereenkomsten	onbekend	

Verwerkingen

De verwachting is dat nog niet alle binnen de gemeente voorkomende verwerkingen van persoonsgegevens geregistreerd zijn. Naar schatting ontbreekt er nog ca 20% , ongeveer 40 verwerkingen. Deze constatering is in 2018 reeds gedaan en sindsdien is hierin geen verandering gekomen.
Het opnemen van een verwerking in het register vereist duidelijkheid over diverse aspecten zoals ondermeer doelstelling, grondslag en bewaartermijn. Deze aspecten zijn bij de verantwoordelijke directeur niet altijd bekend. Dat betekent dat de kwaliteit van de opgegeven informatie onvoldoende is om het register te publiceren en dat is sinds 2018 dan ook niet gebeurd. Publicatie van het register is gewenst vanuit de plicht om de burgers te informeren over wat de gemeente aan persoonsgegevens verwerkt.

Datalekken

Het aantal meldingen is ten opzichte van 2019 (149) licht gedaald en dat heeft ongetwijfeld te maken met het thuiswerken. Het vertrek van de GGD als onderdeel van de gemeente zorgt maar gedeeltelijk voor de daling van het aantal.

Er bestaat geen norm voor het aantal gemelde datalekken om te kunnen beoordelen of de gemeente op dit punt goed of slecht presteert. Gelet op de omvang van de gemeente (qua medewerkers en inwoners) beoordeelt de FG het aantal bij hem gemelde lekken als blijkbaar passend bij de organisatie. Aan de andere kant is een aantal van 2 tot 3 meldingen per week laag te noemen. Er is slechts één melding doorgezet naar de Autoriteit Persoonsgegevens (AP) en dat is wel uitzonderlijk laag. Het betrof overigens een voorval bij de GGD waarbij onbevoegden gebruik konden maken van een WhatsApp account. De gemeente heeft hierbij de rol van verwerker. Dit betekent dat er van de gemeentelijke datalekken er geen enkele melding naar de AP is gegaan en dat oogt onwaarschijnlijk. In 2019 zijn 7 meldingen doorgezet naar de AP omdat er sprake was van een risico voor de betrokkene. De FG ziet dit als signaal dat er meer aandacht geschonken moet worden aan het verschijnsel datalekken.

De meest voorkomende datalekken zijn: onbevoegd gebruik (ca 40%), onjuiste adressering (25%) en verloren apparatuur (20%). Opvallend datalek omdat dat niet meer verwacht mag worden anno 2020: het versturen van een mail naar 500 externe contacten zonder gebruikmaking van de 'BCC: mogelijkheid'.

Interessant is het aandeel onjuiste adressering, dat in 2018 nog meer dan 50% bedroeg. Het toenemende gebruik van systemen (zoals de eSuite) waar burgers zelf de informatie kunnen inzien heeft ongetwijfeld tot gevolg dat er minder post wordt gestuurd (fysiek of per e-mail). De toename van datalekken 'ongeoorloofd gebruik' (door gegevens in het verkeerde dossier te plaatsen) laat echter zien dat it-oplossingen nieuwe problematiek met zich meebrengen. De impact voor burgers is

echter groter; meer mensen, ook van buiten de gemeente, zien onbedoeld gegevens van anderen. Een brief die verkeerd wordt bezorgd zal niet altijd geopend worden. De gemeente zou hier alerter op moeten zijn. Het is de vraag of er voldoende controle is bij binnenkomst van gegevens op noodzaak tot opname in het juiste (!) dossier. Ook bij afsluiten van een dossier zou een controle op aanwezigheid onjuist opgenomen gegevens uitgevoerd moeten worden. Niet zelden komt het bij beroep- en bezwaarprocedures voor dat er allerlei gegevens verwijderd moeten worden omdat deze niet opgenomen hadden mogen worden. Het betreft dan vooral gegevens van derden.

Door het beheer op afstand zijn de gevolgen van datalekken na verlies van apparatuur beperkt en dat is heuglijk. Het verlies van bedrijfsmiddelen is natuurlijk wel een kostenpost.

PIA's (privacy impact assessments)

Gegevenseffectbeoordelingen zijn een uiterst probaat hulpmiddel bij het beoordelen of er sprake is van risico's en voor het bepalen van daartoe te nemen maatregelen. Een PIA is verplicht wanneer er 'waarschijnlijk sprake is van een hoog risico voor de rechten en vrijheden van natuurlijke personen' (AVG art 35). Om dat te kunnen bepalen is er een richtsnoer uitgegeven door het onafhankelijke Europese adviesorgaan WP29. Deze stelt dat 'In gevallen waarin het niet duidelijk is of een PIA vereist is, deze toch uit te voeren omdat het de verwerkingsverantwoordelijke helpt om aan de wetgeving te voldoen.' De FG stelt zich dan ook op het standpunt dat omdat de gemeente tot 2018 geen PIA's heeft uitgevoerd het (meer dan) wenselijk is dat er PIA's uitgevoerd worden van alle bestaande verwerkingen. Daarnaast zullen er PIA's uitgevoerd moeten worden bij het opzetten van nieuwe processen of bij invoering van nieuwe informatiesystemen omdat de gemeente nagenoeg altijd persoonsgegevens verwerkt. Een risicobeoordeling is dan op zijn plaats.
Het uitvoeren van een PIA is de verantwoordelijkheid van de proceseigenaar. De FG brengt over de uitgevoerde PIA een advies uit.

In 2018 heeft de FG de I-adviseurs van het team Regie IA (onderdeel SSC I&S) geïnformeerd over het toepassen van de PIA en het gebruik van het model. De I-adviseurs zijn bij uitstek geschikt qua kennis en positie om PIA's uit te voeren. De FG is vanaf 2018 dus betrokken als procesbegeleider van te houden PIA's om de I-adviseurs in de gelegenheid te stellen ervaring op te doen. Dit is nog niet succesvol gebleken. De uitvoering van de PIA leunt teveel op de kennis en ervaring van de FG.

Er zijn in 2020 36 PIA's uitgevoerd: 21 in het sociaal domein, 10 ruimtelijk/economisch en 5 overig. De PIA's bevat een advies van de FG aan de verantwoordelijke directeur. Er wordt door de FG zelden een (formele) terugkoppeling ontvangen van de geadviseerde maatregelen.
Het aantal uitgevoerde PIA's is bovendien te laag. Van de bestaande processen zou jaarlijks een kwart bekeken moeten worden op mogelijke privacyrisico's; circa 50 extra dus. Daarmee zijn voor de verantwoordelijke directeuren de risico's onvoldoende bekend.

Verzoeken om inzage

De verzoeken op basis van de AVG waarmee burgers hun rechten kunnen uitoefenen kunnen betrekking hebben op inzage, wijziging of verwijdering van hun persoonsgegevens. Hierbij is de werkwijze dat de burger dit verzoek doet met het algemene contactformulier. Het klantcontactcentrum routeert deze verzoeken naar Juridische Zaken (JUZA) ter afhandeling. JUZA haalt mogelijk aanwezige informatie op bij de betreffende directies en bewaakt de afhandelingstermijn. Ook in 2020 hebben enkele burgers de weg naar de gemeente gevonden via het algemene contactformulier. De organisatie wordt dus niet overstelpt met verzoeken.
Overigens kunnen burgers op grond van de al langer bestaande wetgeving rond het BRP bij Publiekszaken ook verzoeken om informatie indienen. Ook zullen er in het dagelijkse contact met

burgers door de afdelingen gegevens worden getoond uit bijvoorbeeld het informatiesysteem dat bij het proces wordt gebruikt. Daarover heeft de FG geen verdere informatie.

Burgercontacten

De FG heeft op het mailadres fg@groningen.nl in 2020 vier vragen van burgers ontvangen. Deze vragen betreffen het specifieke handelen van de gemeente in hun persoonlijke situatie. Omdat het vragen zijn en niet direct klachten kan de FG dit beantwoorden en hoeft er niet verwezen te worden naar bijvoorbeeld de ombudsman of de klachtenfunctionaris. De FG is als interne toezichthouder gericht op het toepassen van de wet- en regelgeving rond de privacy door de organisatie. Dat is een andere rol dan de ombudsman of de klachtenfunctionaris die gericht is op klachten van burgers over de uitvoering van de werkzaamheden door de gemeente.
Wat opvalt is dat de vragen over de privacy wel een relatie hebben met de wijze waarop de burger door de gemeente is bejegend of vanwege een genomen besluit of uitgevoerde handeling.

Verwerkersovereenkomsten

De gemeente hanteert sinds 2020 het VNG-model voor de verwerkersovereenkomst. Hoewel de privacy-organisatie vrijwillig aangeboden overeenkomsten juridisch toetst, wordt er door hen geen administratie bijgehouden van afgesloten overeenkomsten. Dat is een verantwoordelijkheid van de organisatie zelf. Het blijkt dat er binnen de gemeente geen overzicht bestaat van afgesloten overeenkomsten. Dit wordt veroorzaakt door het op verschillende plaatsen aanwezig zijn van contracten: bij contractbeheer I&S Regie, bij de directies zelf en bij Inkoop (waarschijnlijk in beperkte mate). Dat brengt twee risico's met zich mee. Ten eerste is het de vraag of het aantal af te sluiten overeenkomsten aansluit bij de verwerkingen waarvoor de gemeente verantwoordelijk is. Ten tweede bestaat er geen zekerheid dat afgesloten overeenkomsten kwalitatief in orde zijn. Of er sprake is van periodieke toetsing van bijvoorbeeld het afgesproken beveiligingsniveau is onbekend.

Interventies

De FG kan interveniëren wanneer er sprake is van een zodanig groot risico dat aanvullende maatregelen dringend gewenst zijn. Een interventie zal via de gebruikelijke lijn kenbaar gemaakt worden (via het project, afdeling, directie of het GMT/secretaris). In 2020 is er één interventie geweest.

In 2019 is een start gemaakt met de beoordeling van de risico's rond de invoering van de iVRI's. Dat zijn intelligente stoplichten die op enkele locaties binnen de gemeente zijn geplaatst. Dit vloeit voort uit een door het ministerie van Infrastructuur & Waterstaat gesponsorde ontwikkeling van technologische oplossingen in het kader van het mobiliteitsbeleid. Via Groningen Bereikbaar trekt de gemeente als wegbeheerder samen op met de provincies Groningen en Drenthe. De respectievelijke FG's zijn van mening dat nader extern juridisch onderzoek uitgevoerd moet worden naar de positie van de wegbeheerder en de uitwerking daarvan in de contractuele afspraken. Er worden immers persoonsgegevens verwerkt waarvoor er wel verantwoordelijkheid lijkt te zijn maar geen bevoegdheid. Met dit voorbehoud is omwille van het onderhoud wel een contract getekend met de leverancier en staat de verwerking van de persoonsgegevens nog 'on-hold'. Deze situatie lijkt in een impasse te geraken.

Ontwikkelingen in de datagedreven maatschappij

De maatschappij maakt in toenemende mate gebruik van nieuwe technologie die gekenmerkt wordt door een grote datagedrevenheid. Maatwerk voor mensen, interessant voor commerciële doeleinden maar ook voor overheden, verlangt beschikbaarheid van gegevens over mensen. Dat is op zichzelf een goede ontwikkeling. Maar data wordt 'handel' en kan ook meer en meer gebruikt worden voor ongewenste beïnvloeding en buitensporige controle. Hier heeft een overheid, dus ook de gemeente, een verantwoordelijkheid. Niet om dingen te verbieden of tegen te houden. Wel om alert te zijn bij het verzamelen van gegevens over de burger: hebben we deze gegevens echt nodig? Ook moeten er bij het samenwerken met andere overheden of het inschakelen van externe private partijen goede afspraken gemaakt worden over het gebruik van de gegevens. Vanuit de zorgplicht die er is voor de burger.

In dat kader zou er aandacht moeten zijn voor het volgende:

(i). Ethische vraagstukken. In toenemende mate komen er vraagstukken op tafel die een politiek/ethische afweging vergen: 'willen wij dit als gemeente wel?' Willen wij dat de burger ervaart dat de gemeente zich ook verantwoordelijk voelt, en daar naar handelt, voor de persoonlijke levenssfeer? Voorbeelden zijn:

- Het plaatsen van intelligente stoplichten waarbij voor de gemeente niet bekend is wat er met de data gebeurt.
- Het verlenen van vergunningen aan een scooter-verhuur-bedrijf dat overweegt om de scooters uit te rusten met camera's zodat de route van de huurder nog beter bekend is. Overigens heeft de gemeente daar geen opdracht voor gegeven.
- Het gebruik van wifi-tracking techniek om drukte te meten (is terecht niet doorgegaan).
- het gebruik van gegevens van burgers bij het testen van informatiesystemen.

Inmiddels is er vanuit het programma Virtueel Groningen een opdracht opgehaald bij het college om na te denken over het gebruik van technologie en algoritmes en om daarbij handreikingen, hulpmiddelen en vormen van ondersteuning te ontwikkelen.
De FG is van mening dat er een hoogste adviescollege zou moeten zijn waarin de politiek/bestuurlijke, de uitvoerende en de toezichthoudende component zich gerepresenteerd voelen. Zo'n 'ethische commissie' zou ter zake het college kunnen adviseren.

(ii). Registers voor aanwezige sensoren. Het gebruik van sensoren (gericht op registreren van persoonsgegevens) neemt toe. De gemeente kent het gebruik van camera's, maar in toenemende mate worden er diensten aangeboden op basis van andere technologie (wifitracking, warmtesensoren). Voor de gemeente ligt er een taak als het gaat om de openbare ruimte (veiligheid). Maar het is bij de gemeente niet bekend welke sensoren er allemaal in de gemeente aanwezig zijn. Burgers mogen zich onbespied wanen, of ze moeten er over worden geïnformeerd. Er zijn gemeentes actief op dit gebied waarbij een meldingsplicht aan de orde kan zijn en de plaatsing gewoon op de website gepubliceerd wordt.

(iii). Algoritmes. Een andere verantwoordelijkheid betreft het al dan niet gebruiken van algoritmes. In 2020 heeft de VNG een heldere handleiding hierover gepubliceerd en het zou heel goed zijn wanneer de gemeente werk maakt van een inventarisatie en ook hiervan de resultaten publiceert. Maak helder wat de gemeente doet.

Invulling rol FG en privacyteam

De uitvoering van de werkzaamheden van de FG en het privacyteam worden bepaald door de hoeveelheid tijd die beschikbaar is. Binnen de gemeente is er 0,9 fte FG (functionaris gegevensbescherming) en 0,8 fte PO (privacy officer) beschikbaar. Dat is aan de bescheiden kant en

dat betekent dat sommige aspecten minder aandacht krijgen, zoals bijvoorbeeld de rol van de gemeente in samenwerkingsverbanden. Het kan ook tot gevolg hebben dat zaken langer op zich laten wachten, denk aan het publiceren van het verwerkingenregister.

Om dit aspect te verbeteren is het naast het stellen van prioriteiten ook goed om te kijken of sommige zaken slimmer georganiseerd kunnen worden. Een voorbeeld daarvan is het vergroten van de rol van de I-adviseurs bij het tot stand komen van de risicobeoordelingen (PIA's).

Aandachtspunten 2021/2022

Gelet op het algemene beeld van de compliance (blz. 5) en de bevindingen (blz. 10 t/m 14) is de FG van oordeel dat de gemeente *meer sturing* moet geven aan de opgaven die er zijn om beter te voldoen aan de wetgeving rond persoonsgegevens. Hierbij is een cruciale rol weggelegd voor de Concerndirectie, in samenspraak met de directeuren van de verschillende afdelingen.

Specifiek zijn er voor 2021/2022 de volgende aandachtspunten voor de gemeente:

Voor de Concerndirectie:

1. het maken van afspraken met de afzonderlijke directeuren als onderdeel van de managementovereenkomst over de volgende aspecten:
   - het aantal uit te voeren PIA's
   - het in afstemming met de FG publiceren van de verwerkingen op de website van de gemeente Groningen;
   - welke bijdrage er geleverd wordt op het gebied van bewustwording van de eigen medewerkers

Voor de Functionaris Gegevensbescherming:

2. het initiatief nemen voor het op orde brengen van het verwerkingenregister
3. het overdragen van de begeleidende rol bij de PIA aan Regie IA
4. uitdragen van informatie rondom het fenomeen datalekken (preventie)
5. het bij de CD aandragen van mogelijke aanvullende afspraken die gemaakt kunnen worden met de verschillende directies.

Publicatie Jaarverslag

Dit jaarverslag wordt na bespreking in de Concerndirectie ter vaststelling aangeboden aan het college en ter informatie aan de gemeenteraad, de ondernemingsraad (OR), verspreid onder de directeuren en gepubliceerd op de website en het intranet van de gemeente.