Jaarverslag 2018 Functionaris Gegevensbescherming Gemeente Groningen

Inhoudsopgave

BIJLAGE I. Indicatie gewenste capaciteit Privacyteam

Auteur: Menno van Heumen, Functionaris Gegevensbescherming

Datum: 16 april 2019
Status: definitief

Samenvatting

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing geworden. Vanaf 25 mei 2018 houdt de Functionaris Gegevensbescherming (FG) toezicht op deze toepassing door de Gemeente Groningen. Met het jaarverslag 2018 legt de FG verantwoording af over het gevoerde toezicht.

Het algemene beeld van de mate waarin de gemeente voldoet aan de AVG is dat de gemeente wel klaar is voor de AVG, maar dat er nog geen sprake is van het volledig voldoen aan de AVG. Op vier aspecten scoort de gemeente naar het oordeel van de FG nog een onvoldoende: het uitvoeren van gegevenseffectbeoordelingen, het toepassen van privacy-by-design en -by-default, het omgaan met verwerkersovereenkomsten en de aantoonbaarheid van toestemming van betrokkenen (indien van toepassing). Het register van de verwerkingen en de meldplicht datalekken scoren een magere voldoende. De rechten van betrokkenen zijn redelijk geborgd. Bewustwording van medewerkers scoort het hoogst, daar is dan ook veel in geïnvesteerd.

De producten die door het privacyteam van Juridische Zaken (JUZA; FG en privacy officer) zijn opgeleverd maken dat de gemeente wel adequate (randvoorwaardelijke) maatregelen heeft genomen om te kunnen gaan voldoen aan de AVG.

De volgende kerncijfers zijn beschikbaar:

Verwerkingen	196	
Datalekken	34	Gemeld bij de AP: 6
PIA's	4	
Verzoeken om inzage	6	Via JUZA lopende verzoeken
Burgercontacten	3	
Verwerkersovereenkomsten	onbekend	
Interventies	1	Blockchain GKB

Voor 2019 adviseert de FG de gemeente aandacht te besteden aan de volgende punten:

1. Verbetering van de als onvoldoende beoordeelde aspecten: uitvoering PIA's, privacy-by-design en -by-default, verwerkersovereenkomsten en toestemming betrokkenen;
2. Verhoging kwaliteit register verwerkingen en informatievoorziening rond meldplicht datalekken;
3. Borging/besturing afspraken GMT met directies;
4. Formatie van het privacyteam herbezien en regelen vervanger van de FG.

De FG zal naast deze punten in 2019 ook de volgende onderwerpen actief volgen: autorisaties en logging, de aan de gemeente gelieerde websites, de relatie met audit/control en nieuwe Europese regelgeving (ePrivacy verordening).

Inleiding

Het jaarverslag 2018 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 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 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 2018 en de aandachtspunten voor 2019.

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 niet alleen kennis te nemen van het jaarverslag maar ook besluiten te nemen over de aandachtspunten voor 2019. 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

In mei 2018 werd de AVG van toepassing. De gemeente heeft zich hierop voorbereid door de uitvoering van het traject 'Implementatie AVG' dat in 2017 is gestart op basis van een plan van aanpak dat is gemaakt door een team bestaande uit een kwartiermaker, afdelingshoofd JUZA, afdelingshoofd Regie I&A, de CISO, senior juridisch adviseur en de privacyofficer. De FG heeft in mei 2018 uitgesproken dat de gemeente per 25 mei 2018 klaar is voor AVG, maar dat de uitvoering van de tijdens de implementatie ontwikkelde producten pas zichtbaar zal gaan maken in hoeverre de gemeente daadwerkelijk aan de AVG voldoet (compliance). De beoordeling van de tien door de AP samengevatte compliance-eisen geven ultimo 2018 te zien dat het nog te vroeg is om te spreken van het volledig voldoen aan deze eisen.
Het voldoen aan de eisen vanuit de AVG is een op risicoanalyse gebaseerde doelstelling, ingebed binnen de gebruikelijke control-cyclus (plan-do-check-act). Korte karakterisering van de tien eisen, welke in meer detail terugkomen bij de uitgevoerde activiteiten en opgeleverde producten geeft het volgende beeld:

aspect	toelichting
Bewustwording	In samenwerking met Juridische Zaken (JUZA) en Informatiebeveiligingsteam (onderdeel van I&A Regie) is er binnen de organisatie veel aandacht aan bewustwording. Onderdeel daarvan is de vaststelling van het privacy beleid, privacy statements en diverse protocollen. Bewustwording is het begin van bewustzijn.
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.
Register verwerkingen	De FG heeft met hulp van de directies een register opgebouwd. De kwaliteit daarvan is nog niet voldoende om dit in- en extern te publiceren.
Gegevenseffect-beoordelingen (PIA's)	Er is weliswaar een methode beschikbaar om deze uit te kunnen voeren maar gelet op het schamele aantal van vier uitgevoerde PIA's in 2018 moet de gemeente nog een substantiële inspanning verrichten om dit te verbeteren.
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.
Functionaris Gegevensbescherming	Deze is aanwezig (bij JUZA), maar heeft geen backup en krijgt onvoldoende 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. De FG houdt daarvan een register bij. Gelet op het relatief lage aantal meldingen in 2018 (34 waarvan 6 bij de AP) verdient dit onderwerp meer aandacht.
Verwerkersovereenkomsten	Er is een standaard ontwikkeld voor het aangaan van verwerkersovereenkomsten. Het is niet duidelijk in hoeverre deze wordt toegepast en er bestaat geen totaaloverzicht van de aanwezige (en afwezige !) overeenkomsten.
Leidend toezichthouder bij vestigingen in EU landen	Niet van toepassing voor de gemeente.

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 en aantoonbaar gemaakt moet worden. Denk daarbij aan toestemming voor doeleinden zoals nieuwsbrieven, andere voorzieningen of producten (bijvoorbeeld de Stadjerspas), het doen van tevredenheidsonderzoeken en enquêtes, het doorbreken van geheimhoudingsplicht, etc. Bij het inventariseren van de verwerkingen wordt dit aspect wel benoemd, maar daarmee is nog niet vastgesteld dat dit daadwerkelijk aan de orde is, of dat aantoonbaar gemaakt kan worden dat deze toestemming ondubbelzinnig en actief is gegeven.

Samenvattend kan gesteld worden dat ten opzichte van 2017, de start van de voorbereiding op de AVG, de gemeente inderdaad klaar is voor de naleving van de AVG. In de uitvoering zal nog aandacht gegeven moeten worden aan het register van de verwerkingen, de gegevenseffectbeoordelingen, privacy-by-design en -by-default en de verwerkersovereenkomsten. Richting de burgers zal nagegaan moeten worden of een eventuele toestemming aantoonbaar is.

Uitgevoerde activiteiten

In 2018 zijn de volgende activiteiten uitgevoerd:

Bewustwording
Een belangrijke sleutel tot succes is de bewustwording van medewerkers over het verantwoord omgaan met persoonsgegevens. In het jaar dat de AVG van toepassing werd is er veel aandacht hieraan besteed op de volgende wijze:

- Het houden van tientallen, bijeenkomsten met medewerkers en leidinggevenden over de betekenis van de AVG voor de bestaande werkwijzen;
- In het bijzonder zijn alle WIJ-teams bezocht en alle JGZ-medewerkers van de GGD voorgelicht;
- Het mede organiseren van de game 'Zet jezelf op scherp' waarin enkele specifieke privacyvragen werden gesteld. De deelnamegraad bedroeg 46%.
- De 'cursus Privacy en de AVG' is tweemaal verzorgd in de algemene opleidingsweek in oktober;
- Tweemaal is er een College Tour programma verzorgd;
- Het aanwezig zijn met een stand in het kader van de jaarlijkse introductie van nieuwe medewerkers (Ontmoet en Groet);
- Het aanpassen van de opzet en de inhoud van de speciale privacy 'tegel' op het intranet van de gemeente;
- 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
Om invulling te geven aan de verplichtingen die voortvloeien uit de AVG zijn de volgende hulpmiddelen zelfstandig ontwikkeld:

- De inventarisatie de verwerkingen van persoonsgegevens;
- Een methode voor de uitvoering van de verplichte gegevenseffectbeoordelingen (PIA; privacy impact assessment);
- De opzet voor de registratie van datalekken;
- Het ontwikkelen van een format voor de verwerkersovereenkomst waarbij het VNG-model als basis heeft gediend. De Groningse versie is compacter en gericht op praktische toepasbaarheid;
- Standaardteksten voor privacyverklaringen en gegevensuitwisselingsconvenanten.

Advisering
Het privacyteam (de FG en de PO) heeft een algemeen e-mailadres beschikbaar gesteld (privacy@groningen.nl) waar medewerkers terecht kunnen met vragen, opmerkingen en verzoeken tot ondersteuning en advies. Op dat adres zijn in 2018 honderden berichten binnengekomen 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 'mag dit van de AVG?'. Omdat de AVG weinig specifiek normerend is vergt het antwoord op deze vraag veelal maatwerk.
De FG adviseert desgevraagd ook de ombudsman binnen de gemeente (zowel de gemeentelijke ombudsman als de binnen de verschillende domeinen voorkomende ombudsman).

Opgeleverde producten

In 2018 zijn er de volgende producten opgeleverd:

- Register verwerkingen. Het register bevat een overzicht van de verwerkingen waar de Gemeente Groningen eindverantwoordelijk is. Per verwerking wordt het volgende vastgelegd: het doel, de wettelijke grondslag, de categorie van persoonsgegevens, de categorie betrokkenen, de bewaartermijn, de eventuele verwerker, de bewaartermijn, de eventuele doorgifte aan landen buiten de EER, het beveiligingskader.
- Datalekkenregister. Dit bevat een overzicht van gemelde datalekken die door de FG zijn onderzocht. Daarbij wordt onder andere een opgaaf gedaan van waar het lek zich heeft voorgedaan, wat de aard is van het lek, welke maatregelen er zijn getroffen, het eventuele informeren van betrokkenen en het al dan niet melden bij de Autoriteit Persoonsgegevens.
- Datalekkenprocedure. Er is een gewijzigde versie opgeleverd van de datalekkenprocedure met als kernpunt dat medewerkers nu zelf een melding kunnen doen bij het centrale meldpunt (ict-servicedesk) in plaats van door de leidinggevende.
- Beleid. Op 29 mei 2018 heeft het college van B&W het privacybeleid van de gemeente Groningen vastgesteld. Dit is gepubliceerd op de website van de gemeente en op overheid.nl (gemeenteblad 2018/118888).
- Privacystatements. De gemeente Groningen communiceert met de burgers onder andere via de gemeentelijke website: gemeente.groningen.nl. Op de site moet duidelijk gemaakt worden hoe de gemeente omgaat met de privacy bij het bezoeken van de site. Dat gebeurt door het plaatsen van een privacystatement (hoe gaat de gemeente om met uw privacy) aangevuld met een proclaimer (over het gebruik van cookies en statistische gegevens). Afgeleid daarvan zijn er privacystatements of protocollen verschenen voor websites waar de gemeente Groningen ook verantwoordelijkheid draagt, zoals bijvoorbeeld bij de GGD of WIJ.
- Model voor PIA (Privacy Impact Assessment). Een PIA of een gegevenseffectbeoordeling is een middel om te onderzoeken of er bij het verwerken van persoonsgegevens risico's zijn die voorzien moeten worden van aanvullende maatregelen. Om PIA's te kunnen uitvoeren is er een model ontwikkeld. In dat model worden de risico's bepaald op een zevental aspecten die samenhangen met de te verwerken persoonsgegevens. Dit model kan in combinatie met de zogenaamde BIA (Business Impact Assessment) worden gebruikt. De BIA besteed namelijk aandacht aan een classificatie van gegevens in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid. De BIA levert daarmee een set van informatiebeveiligingsmaatregelen die als input voor de PIA gebruikt kunnen worden. In sommige situaties is de PIA verplicht, de criteria hiervoor zijn te vinden in de Europese richtlijn van de zogenaamde werkgroep29.
- Format verwerkersovereenkomst. Wanner bij het verwerken van de persoonsgegevens een derde partij, buiten de gemeente, wordt ingeschakeld dient er een separate verwerkersovereenkomst afgesloten te worden. Omdat het door de VNG voorgestane model door de FG/PO als juridisch omslachtig werd beoordeeld is er voor de gemeente een compacte variant opgesteld die op het intranet is gepubliceerd.

Jurisdictie

De gemeente Groningen is bij diverse organisaties en instellingen direct of zijdelings betrokken. Zo is er sprake van een directe betrokkenheid bij De Oosterpoort/Stadsschouwburg en het Centrum voor Beeldende Kunst waardoor de gemeente eindverantwoordelijk is voor de verwerking van persoonsgegevens. Daarnaast participeert de gemeente in een negental Gemeenschappelijke Regelingen (GR) waar ook sprake kan zijn van deze eindverantwoordelijkheid. Voorbeelden zijn de GGD en de RIGG als onderdeel van de GR Publieke Gezondheid. Met betrekking tot de stichting WIJ kan gesteld worden dat vanuit de criteria opdrachtbepaling en inzet van middelen de gemeente ook eindverantwoordelijk is voor de verwerking. Verder is de gemeente de spil in de Arbeidsmarktregio. Het vaststellen van de jurisdictie is van belang voor de noodzakelijke duidelijkheid wie eindverantwoordelijk is voor het verwerken van persoonsgegevens. Dat wordt niet altijd expliciet benoemd in de GR. De FG zal dit bij de betreffende GR kenbaar maken.

Bevindingen

De kerncijfers van 2018 zijn:

Verwerkingen	196	
Datalekken	34	Gemeld bij de AP: 6
PIA's	4	
Verzoeken om inzage	6	Via JUZA lopende verzoeken
Burgercontacten	3	
Verwerkersovereenkomsten	onbekend	
Interventies	1	Blockchain GKB

Toelichting op de kerncijfers

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. Zo is er geen opgave ontvangen van de directies OPSB, CB en zijn er een aantal directies met maar één verwerking.
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 in 2018 dan ook niet gebeurd. Publicatie van het register is gewenst vanuit de plicht om de burgers te informeren over wat de gemeente zoal aan persoonsgegevens verwerkt.

Datalekken
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 vrij laag. Gemiddeld één melding per week is niet veel. In 2018 zijn 6 meldingen doorgezet naar de AP omdat er sprake was van een risico voor de betrokkene.
Meer dan de helft van de meldingen gaat over het versturen van berichten en/of documenten naar anderen dan de beoogde ontvangers, of dat nu per post of via de mail plaatsvindt. Het is een goede zaak dat de gemeente het gebruik van Zivver aanbiedt om het risico van mail gerelateerde datalekken te verkleinen.
In 2018 is de procedure voor het melden van datalekken door de FG aangepast en aangeboden aan het college ter vaststelling [noot: deze is begin 2019 vastgesteld]. Belangrijkste wijziging is dat medewerkers zelf een melding kunnen doen bij het centrale meldpunt (ict-servicedesk) in plaats van dat de leidinggevende dat moet doen.
Op verzoek van de AP heeft de gemeente meegewerkt aan een verkennend onderzoek naar het melden van datalekken. De FG heeft de gewenste documentatie opgeleverd, het ging daarbij om het overzicht van de meldingen, de meldingsprocedure en de managementinformatie.

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 adequate 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 in 2018 tijdelijk betrokken als procesbegeleider van te houden PIA's om de I-adviseurs in de gelegenheid te stellen ervaring op te doen. Gelet op de rol van de FG moet dit in 2019 afgebouwd worden. Er zijn 4 PIA's uitgevoerd:

onderwerp	toelichting	afdeling/directie
RIGG Dashboard	Managementinformatie met Power BI.	RIGG
Roosteren	Product Ortec. Gebruik door diverse directies.	SSC MOC
HR Vierkant	Managementinformatie uit fin en hrm.	SSC MO&C en SSC FI&J
GKB Blockchain	Inzicht in vorderingen van en door schuldeisers.	Inkomensdienstverlening

Het aantal van vier PIA's is te zien als een eerste begin. Maar gelet op het totaal aantal verwerkingen en de hoeveelheid nieuwe ontwikkelingen is dit aantal schrikbarend laag.

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. In 2018 hebben zes 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. Daarover heeft de FG geen informatie.

Burgercontacten
De FG heeft op het mailadres fg@groningen.nl in 2018 drie 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. 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 die gericht is op klachten van burgers over de uitvoering van de werkzaamheden door de gemeente.

Verwerkersovereenkomsten
Hoewel de privacy-organisatie wel het format heeft ontwikkeld voor de verwerkersovereenkomst, én vrijwillig aangeboden overeenkomsten juridisch toetst, wordt er geen administratie bijgehouden van afgesloten overeenkomsten. Dat is een verantwoordelijkheid van de organisatie zelf. Het blijkt echter dat er gemeente breed geen overzicht bestaat van afgesloten overeenkomsten. 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.

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 2018 is er één interventie geweest. Bij het Blockchain project van de GKB (Inkomensdienstverlening) is aangedrongen op het uitvoeren van een PIA. Deze heeft inmiddels plaatsgevonden.

Overige waarnemingen
Door de vele contacten die de FG inmiddels heeft zijn er ook een aantal waarnemingen die hier gemeld moeten worden:

(i). autorisaties en logging. Met uitzondering van Suwinet en het BRP was het in 2018 voor de FG onduidelijk hoe dit is ingeregeld voor de informatiesystemen van de gemeente. Wijzigt een medewerker van functie of afdeling dan zouden de autorisaties aangepast moeten worden. Dat schijnt niet altijd te gebeuren. Inmiddels (april 2019) is duidelijk dat van minimaal 68 applicaties autorisatiematrices aanwezig zijn die nog wel periodieke aandacht vergen (van de directies op aangeven van het informatiebeveiligingsteam).
(ii). toestemming betrokkenen. Wordt dat altijd aantoonbaar vastgelegd?
(iii). websites gelieerd aan de gemeente. Deze lijst van tussen de 50 en 100 sites moet periodiek getoetst worden op actualiteit: bestaat de site nog, is de privacy-informatie nog correct?
(iv). relatie met audit/control. Deze relatie is nog niet structureel vormgegeven en ligt vanwege de sturing op afspraken wel voor de hand. Directies worden dan vanuit één punt ondersteund.
(v). verdergaande Europese regelgeving (ePrivacy verordening). Wetgeving staat niet stil en moet beoordeeld worden op consequenties voor de gemeentelijke processen. Dat geldt overigens in algemene zin voor alle wijzigingen in wetgeving omdat daar veelal de grondslag ligt voor het verwerken van persoonsgegevens door de gemeente.
(vi). Overzicht verwerkersovereenkomsten. Deze overeenkomsten liggen verspreid over de organisatie: bij het SSC I&S, bij SSC FI&J en bij de directies zelf. Bij gebrek aan totaaloverzicht loopt de gemeente meer risico bij de naleving van de overeenkomsten.

Aandachtspunten 2019

Grofweg zijn er voor 2019 drie aandachtspunten voor de organisatie, gezien vanuit het perspectief van de FG:
(i). Vervolg op de bevindingen zoals beschreven in de vorige paragraaf. Specifiek gaat het om:

- verhogen inhoudelijke kwaliteit register van verwerkingen en het publiceren daarvan op de website van de gemeente.
- informatievoorziening rond de meldingen van datalekken verbeteren door periodieke rapportage aan het GMT;
- het doen uitvoeren van substantieel meer PIA's;
- het procesmatig beter borgen van inzageverzoeken van burgers;
- het binnen de organisatie aandacht vragen voor de overige waarnemingen.

(ii). Besturing en borging afspraken met management.
De onder (i) genoemde aandachtspunten kunnen alleen effectief geborgd worden wanneer het management (GMT en directies) daarover specifieke afspraken maakt. De FG kan daartoe een specifiek voorstel per directie doen. De FG kan de voortgang daarvan monitoren.

(iii). Formatie
De uitvoering van de werkzaamheden van de FG en het privacyteam worden bepaald door de hoeveelheid tijd die beschikbaar is. Medio 2018 is reeds aangegeven dat de beschikbare formatie niet toereikend is, en dat de FG als toezichthouder formeel gesproken geen vervanger heeft. Een organisatie met de omvang van de gemeente Groningen moet in staat geacht worden invulling te geven aan functiescheiding. Omdat de FG ook als contactpersoon fungeert tussen de organisatie en de AP is er duidelijk sprake van een ongewenste situatie. De AVG stelt in dit verband dat de verwerkingsverantwoordelijke middelen beschikbaar moet stellen voor het uitvoeren van de FG taken (AVG, art 38 lid 2). In Bijlage I staat een indicatie voor de gewenste formatie verwoord. Het betreft een uitbreiding van 1,8 naar 3,9 fte.

Publicatie Jaarverslag

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

BIJLAGE I. Indicatie gewenste capaciteit Privacyteam

Grondslag:
De komst van de AVG (Algemene Verordening Gegevensbescherming) brengt een aantal wettelijke verplichtingen met zich mee. Art.38 geeft aan dat de FG voor zijn taken voldoende middelen tot zijn beschikking moet hebben.

Huidige bezetting:
1,8 fte (1,0 voor Functionaris Gegevensbescherming (FG) en 0,8 voor de privacyofficer (PO).
Deze capaciteit wordt nu gebruikt voor:

- Toezicht (algemeen en datalekken);
- Advisering organisatie;
- Voorlichting en communicatie;
- Beheer (register, onderhoud beleid/statements/formats).

Ontwikkeling
De volgende ontwikkelingen maken structurele uitbreiding van capaciteit noodzakelijk:

- Advisering rond gebruik Privacy Impact Analyses (PIA's);
- Juridische advisering rond af te sluiten verwerkersovereenkomsten;
- FG voor derden (GGD, RIGG, gemeenschappelijke regelingen);
- Backup van bestaande FG (nu niet aanwezig; noodzakelijk vanwege wettelijk bepaalde reactietermijn van 3 dagen ingeval van datalekken);
- Autonome groei vanwege herindeling (Ten Boer en Haren).

De omvang van deze ontwikkeling wordt geschat op +0,5 FG +0,8 PO en 0,8 uitvoering/ondersteuning.

Benodigde bezetting:
Huidige bezetting en uitbreiding vanwege de verdere ontwikkelingen geeft het volgende beeld:
FG 1,5 fte
PO 1,6 fte
Uitvoering juridisch/administratief 0,8 fte

Totaal 3,9 fte. Structureel.

Bronfinanciering: Een deel van de financiering kan gevonden worden door afspraken hieromtrent met de derde partijen zoals de GGD, RIGG, Groninger Archieven en mogelijk de andere Gemeenschappelijke regelingen. Schatting: 0,5-1,0 fte.

Niet invullen van deze capaciteit geeft grote risico's op het gebied van compliance, imagoschade en boetes van de Autoriteit Persoonsgegevens (4% van de gemeentebegroting; max. 20 miljoen).