Gemeente Haarlem

Rapportage 2018-2019

Functionaris Gegevensbescherming

Cathérine Konijnenbelt

12 mei 2020

Inleiding

Meer en meer werken allerlei organisaties en ook de overheid gedigitaliseerd en met data. Het biedt vaak gemak en snelheid. Veel data leveren ook nieuwe inzichten, die kunnen worden gebruikt bij beleidsvorming of opsporing bijvoorbeeld of om de dienstverlening aan bewoners te verbeteren. Naast die voordelen, kleven er echter ook risico's aan het werken met data, zeker waar het gaat om persoonsgegevens. Het is voor mensen lastiger zelf controle te houden over wat ze wel of juist niet vrij willen geven van hun persoonlijke leven en op de juistheid van gegevens die hen betreffen die door anderen – zoals overheden – worden gebruik. En dat is wel de essentie van bescherming van de persoonlijke levenssfeer. Bovendien biedt digitalisering ook kansen aan wie misbruik wil maken van gegevens door bijvoorbeeld identiteitsfraude te plegen. Deze ontwikkelingen maakten nieuwe regels nodig om gegevens beter te kunnen beschermen. De Europese richtlijn uit 1995, in Nederland vertaald naar de Wet bescherming persoonsgegevens, was niet meer toereikend.

Op 25 mei 2018 trad de Algemene verordening gegevensbescherming (AVG) in werking. Deze Europese verordening heeft veel in beweging gebracht. Hoewel de inhoudelijke regels niet eens zo gek veel verschillen van de regels die tot dan golden via de Wet bescherming persoonsgegevens, zijn er daaromheen wel veel extra plichten ingevoerd, om de naleving van de regels te beheersen en te documenteren. Er was veel aandacht in de media voor de nieuwe wet en er ontstond onrust, soms bijna paniek, en veel onduidelijkheid over wat wel en niet mocht. Daarbij waren overigens ook veel onzinverhalen in omloop.

Ook in de eigen organisatie moest veel op touw worden gezet om in elk geval de vereiste functies, beleid en instrumenten in te richten. Er is een register van verwerkingen ingericht, een privacybeleid (intern beleid, niet de Privacynota die de raad in maart 2017 heeft vastgesteld) en privacyverklaring vastgesteld, een functionaris voor de gegevensbescherming (FG) aangewezen en een proces voor AVG-verzoeken ingericht. Dit liep samen met veranderingen in de organisatiestructuur in 2018 en de samenvoeging met de Zandvoortse ambtelijke organisatie.

In de hectiek van deze veranderingen en de veelheid aan operationele vragen die in de organisatie opkwamen, is het schrijven van een jaarrapportage over 2018 niet gelukt. Daarom bestrijkt deze rapportage de periode van twee jaar, met een vooruitblik naar het jaar 2020. Vanaf dit jaar zal ik halfjaarlijks rapporteren aan de gemeenteraad. Zo mogelijk gelijktijdig met de rapportage over informatiebeveiliging.

Samenvatting

In 2018 werd de AVG van kracht en was het aanvankelijk alle hens aan dek om de verplichte instrumenten, functies en beleid in te richten. Er moest een reglement worden gemaakt, een privacyverklaring geschreven, alle verwerkingen van persoonsgegevens in alle afdelingen geïnventariseerd en geregistreerd en er werd een FG aangewezen. Er is ook veel tijd besteed aan het versterken van bewustzijn en kennis in de organisatie door presentaties en cursussen te organiseren. De bewustwordingsactiviteiten en de aandacht die de media ruimschoots besteedden aan de invoering van de AVG zorgden ervoor dat er veel adviesvragen kwamen, rijp en groen door elkaar. 2018 was op privacygebied dan ook een behoorlijk hectisch jaar. Inmiddels is er meer rust en overzicht. Er komen nog steeds veel adviesvragen uit de organisatie maar dan heeft de vraagsteller vaak zelf al zijn eerste gedachten gevormd en zoekt hij bevestiging of nader advies. Het team zelf heeft zich ook verder ontwikkeld met een duidelijker onderlinge taakverdeling.

Ook in de stad is het bewustzijn en de kennis gegroeid. Dat is onder meer te merken aan het groeiende aantal inzageverzoeken en vragen om informatie. Datalekken worden nog niet vaak gemeld van buiten de organisatie. In 2020 zal zowel binnen als buiten de organisatie meer aandacht worden gevraagd voor het melden van datalekken en een duidelijke meldknop worden gemaakt.

Er zit duidelijk groei in kennis en bewustzijn van de organisatie, al zijn er nog wel verschillen tussen de afdelingen. Grosso modo lijkt Haarlem op ongeveer hetzelfde niveau te staan als de meeste gemeenten. Er wordt veel kennis gedeeld tussen gemeenten, rechtstreeks en via de VNG. Daaruit blijkt vaak dat veel gemeenten tegen dezelfde vragen oplopen en met ongeveer dezelfde ontwikkelingen bezig zijn. Dat we min of meer gelijklopen, wil echter niet zeggen dat er nu minder aandacht nodig is of dat we al op het gewenst niveau zijn. Feitelijk is er in alle gemeenten en ook in Haarlem nog een behoorlijke groei nodig naar een hoger niveau van volwassenheid. In 2019 is voor zowel op het niveau van de organisatie als geheel als voor de afdeling SMSR een self assessment gedaan. Op een schaal van 1 tot en met 5, werd in beide gevallen een score van ongeveer 2 behaald. Het zou goed zijn voor alle afdelingen een self assessment te doen. Dat biedt enerzijds een mooie nulmeting en anderzijds levert het concrete adviezen op over mogelijke verbeteringen.

Het privacyreglement

In mei 2018 heeft het college het (interne) gegevensbeschermingsbeleid vastgesteld, in de vorm van een privacyreglement. Het is een vertaling van de regels uit de AVG naar de Haarlemse praktijk en een verdere invulling van de Privacynota die de raad in 2017 heeft vastgesteld. In het reglement worden begrippen uit de AVG uitgelegd en zijn de uitgangspunten en eigen regels vastgesteld voor het verwerken van persoonsgegevens. Het gaat in op de rechten van betrokkenen, bijvoorbeeld de verplichting betrokkenen te informeren als hun persoonsgegevens worden verwerkt en de rechten die betrokkenen hebben op inzage, correctie of gegevenswissing. Anderzijds benoemt het reglement verplichtingen van de gemeente als verantwoordelijke, zoals het hebben van een register van verwerkingen, het aanstellen van een FG, het uitvoeren van Data Protection Imapct Assessments (DPIA, privacyrisicoanalyse) en de verplichting datalekken te melden en goed af te handelen.

Inmiddels hebben we twee jaar ervaring met de AVG. In 2020 wordt het reglement geactualiseerd. Bovendien is het de bedoeling uiteindelijk voor elke afdeling een concretere invulling te beschrijven, toegespitst op de verschillende werkprocessen. Zie ook de doorkijk naar 2020 op pagina 8.

Het privacyteam

Op 27 maart 2018 heeft het college de strategisch adviseur privacy benoemd als functionaris voor de gegevensbescherming. Dit is een verplichting die volgt uit de AVG. De FG heeft tot taak zowel te adviseren en te informeren over als toezicht te houden op de naleving van de AVG en is de contactpersoon voor de Autoriteit Persoonsgegevens (de nationale toezichthouder). College, burgemeester en raad zijn er elk zelf verantwoordelijk voor dat de AVG wordt nageleefd en dat de privacy van bewoners, medewerkers en andere betrokkenen goed wordt beschermd. De FG kan daarover onafhankelijk adviseren en zo nodig rechtstreeks contact zoeken met directie of college.

Behalve de FG, die onderdeel uitmaakt van de afdeling Concerncontrol, zijn er binnen de afdeling Interne Dienstverlening een privacy-adviseur en een privacy en security officer. De FG en privacy-adviseur zijn beiden aangesteld voor 32 uur, de privacy en security officer is voltijds aangesteld en besteedt ongeveer de helft van haar tijd aan privacykwesties. In 2018 is er ook werk uitbesteed aan

externen. Dat betrof met name meewerken aan het invullen van het register van verwerkingen en het uitvoeren van twee DPIA's.

In 2018 en ook nog voor een groot deel van 2019 is het hele privacyteam vooral heel operationeel in touw geweest. Er moesten processen en instrumenten worden ingericht en er kwamen uit de organisatie heel veel vragen om hulp bij het opstellen van verwerkersovereenkomsten, informatie en advies, rijp en groen door elkaar. De privacy-adviseur was bovendien weliswaar een ervaren jurist en bekend met de organisatie maar privacy was voor haar een nieuw onderwerp, waar ze zich nog in moest inwerken. In de loop van 2019 is er een duidelijker taakverdeling gekomen. De privacyadviseur is de eerste adviseur, met name op tactisch niveau, de privacy officer werkt met name op operationeel niveau. Dat geeft ruimte voor de FG om meer naar de toezichthoudende rol te verschuiven en advisering op strategisch niveau. Uiteraard blijft het zo dat er een goede afstemming is en vervanging onderling.

Bewustwordingsactiviteiten en versterking kennis

De inwerkingtreding van de AVG vroeg om veel investering in de bewustwording en kennis van de organisatie hierover. In 2018 zijn in vrijwel alle afdelingen presentaties gehouden over de betekenis van de AVG voor het werk van de gemeentelijke organisatie, die vaak tot levendige discussies leidden. Ook in 2019 zijn nog geregeld presentaties gehouden. In dat jaar zijn ook cursussen gegeven, verzorgd door een extern bureau, deels basiscursussen en deels uitgebreidere cursussen met een dagdeel speciaal voor het sociaal domein.

Naast deze kennisgerichte activiteiten is op Insite een pagina over privacy gemaakt. Behalve basisinformatie en verwijzing naar regelgeving, veel gestelde vragen en reglement zijn hier ook standaarden voor verwerkersovereenkomsten en andere hulpmiddelen te vinden, zoals beslisbomen en afwegingskaders.

Inmiddels is aan het type adviesvragen te merken dat men meer bekend is met de regels rond privacy. Vaak is er zelf al wel nagedacht over hoe en wat en zoekt men bevestiging of preciezer advies.

Register van verwerkingen

Waar onder de Wet bescherming persoonsgegevens steeds bij de voorloper van de AP melding moest worden gedaan van verwerkingen van persoonsgegevens, werkt de AVG anders, namelijk met een documentatieplicht. Het register van verwerkingen is daarvoor het belangrijkste instrument. Hierin wordt per proces vermeld welke categorie van persoonsgegevens wordt verwerkt, van welke categorie betrokkenen, voor welk doeleinde, wat de bron is van de gegevens, aan wie eventueel gegevens worden verstrekt, of er een verwerkersovereenkomst is gesloten (als een andere partij voor de gemeente de gegevens verwerkt) en zo mogelijk de bewaartermijn.

Het invullen van het register heeft in 2018 veel tijd gekost, doordat met elke afdeling de relevante werkprocessen moesten worden doorgenomen. Het is de verantwoordelijkheid van de vakafdelingen om het actueel te houden maar het privacyteam zal om dat te ondersteunen jaarlijks uitvragen of de geregistreerde gegevens nog kloppen. Dat is gebeurd in het voorjaar van 2019 en zal gebeuren in 2020 in het derde kwartaal.

Op dit moment is het register alleen intern te raadplegen. Sommige gemeenten hebben op hun website ook een – iets minder uitgebreide – publieke versie. Het is te overwegen ook voor Haarlem een publieke versie op de website te plaatsen.

Meldplicht datalekken

In 2016 werd in Nederland vooruitlopend op de AVG al een meldplicht voor datalekken geïntroduceerd. Daarvoor is dat jaar in Haarlem ook een proces ingericht. Datalekken kunnen vanuit de organisatie zelf worden gemeld op een apart mailadres: datalekmelden@haarlem.nl. Meldingen worden daar opgepakt door het privacyteam, aanvankelijk aangevuld met de information security officer. Meldingen worden geregistreerd, met de melder wordt contact opgenomen om te bespreken wat er precies aan de hand is en of er actie moet worden ondernomen om het lek te dichten en de betrokkenen te informeren. Als het nodig is, wordt het lek gemeld bij de AP. Van buiten de organisatie kunnen datalekken worden gemeld via FG@haarlem.nl.

De meeste lekken betreffen mails of brieven die naar een verkeerd mail- of postadres zijn gestuurd en verloren devices (telefoons, tablets en laptops). In 2018 zijn er 21 datalekken geregistreerd, waarvan er 5 aan de AP zijn gemeld. In 2019 zijn er 20 datalekken geregistreerd, waarvan er 6 aan de AP zijn gemeld.

Waarschijnlijk zijn er meer datalekken dan er gemeld worden. Mogelijk herkent niet iedereen een incident als datalek of men weet niet dat het gemeld moet worden. Op dit moment wordt het hele proces opnieuw beschreven, in samenhang met de meldingen van andere beveiligingsincidenten. Daar wordt één duidelijke meldknop voor gemaakt op Insite. Achter de schermen wordt vervolgens bezien om wat voor type melding het gaat. Zodra dit rond is (naar verwachting rond de zomer), wordt er weer actief aandacht voor gevraagd dat elk incident gemeld moet worden, waarom en hoe.

Rechten van betrokkenen

In de AVG zijn de rechten van betrokkenen versterkt. Een belangrijk doel van de AVG is tenslotte ervoor te zorgen dat iedereen zelf de controle houdt over zijn persoonsgegevens. Natuurlijk heeft de gemeente veel taken waarvoor persoonsgegevens moeten worden verwerkt, daarin hebben burgers vaak geen vrije keuze. Controle bestaat er dan uit in ieder geval overzicht te hebben over welke gegevens voor welk doel worden verwerkt, of dat gelegitimeerd is en of de gegevens kloppen.

Mensen kunnen een inzageverzoek doen, om te zien welke persoonsgegevens van hen voor welk doel worden verwerkt. Als gegevens niet kloppen, mogen ze rectificatie of aanvulling vragen. Als de verwerking niet legitiem is, kan men ook verwijdering vragen. Dat zijn de belangrijkste rechten van betrokkenen waar de gemeente mee te maken heeft.

Inzageverzoeken kunnen op verschillende manier worden afgedaan, afhankelijk van de aard van het verzoek. Als een verzoeker inzage vraagt in zijn eigen dossier, wordt hij of zij uitgenodigd om samen met de behandelend ambtenaar het dossier door te nemen. Op andere verzoeken wordt met een beschikking een overzicht verstrekt van welke persoonsgegevens worden verwerkt, voor welk doel, wie toegang hebben en – voor zover aan de orde – aan wie de gegevens worden verstrekt. Doorgaans zijn de verzoekers bereid en in staat hun verzoek te specificeren, zodat gericht gezocht kan worden naar hun gegevens. Het komt echter ook voor dat een verzoek over de volle breedte wordt gedaan. In 2019 zijn er ook verzoeken geweest die ‘breed gespecificeerd’ waren; deze hadden

betrekking op alle gegevens van de verzoekers die in het sociaal domein worden verwerkt. Het gaat om 7 verzoeken. De verzoeken om verwijdering hebben steeds betrekking gehad op gegevens die ten onrechte op de website zijn gepubliceerd, (in een nota, overzicht indieners zienswijze/petitie en in een ingekomen brief die bij de commissiestukken was gepubliceerd zonder te anonimiseren).

In 2018 zijn er 4 inzageverzoeken gedaan, 4 verzoeken tot verwijdering van gegevens en is éénmaal bezwaar gemaakt tegen verwerking van gegevens. Twee personen hebben tegen het besluit een bezwaarschrift ingediend, één van hen is vervolgens in beroep gegaan. Op het beroep is nog niet beslist.

In 2019 zijn er 13 inzageverzoeken gedaan en 1 verzoek tot verwijdering. Twee personen hebben een bezwaarschrift ingediend.

Ook op grond van de Wet Basisregistratie Personen kunnen inzageverzoeken worden gedaan. Die werden tot nu toe niet bijgehouden, vanaf 2020 gebeurt dat wel. Naar schatting zijn er in 2018 en 2019 vijf verzoeken per jaar ingediend.

Data Protection Impact Assessments

Als een proces of systeem wordt ingericht of aangeschaft waarin persoonsgegevens worden verwerkt en daarbij waarschijnlijk hoge privacyrisico's ontstaan, moet tevoren een zogeheten gegevensbeschermingseffectbeoordeling (gebruikelijke term: DPIA) worden gemaakt. Daarbij wordt aan de hand van een vragenlijst beoordeeld wat de privacyrisico's zijn en welke maatregelen nodig zijn om die risico's weg te nemen of te beperken. Als er dan nog steeds een hoog risico bestaat, moet het oordeel van de AP worden gevraagd. Dat is nog niet aan de orde geweest.

Om te beoordelen of een DPIA nodig is, is een 'basiskader en DPIA-check' ontwikkeld.

De verantwoordelijke afdeling voert de DPIA in principe zelf uit, met ondersteuning door de afdeling Interne Dienstverlening. Het verslag wordt aan de FG gestuurd, die er een advies over geeft. Vervolgens is het aan de afdeling om te beslissen of een besluit voor te leggen aan college of raad.

In 2018 zijn 3 DPIA's uitgevoerd, in 2019 zijn er 6 uitgevoerd.

Dit instrument kan beter en vooral vaker worden benut. Het is de bedoeling dat de DPIA in een vroeg stadium wordt uitgevoerd, zodat er tijd is om maatregelen te nemen en de uitkomst goed kan worden meegewogen bij de verdere besluitvorming en inrichting van systeem of proces. Het gebeurt nu nog wel dat eerst besloten wordt om een systeem aan te schaffen of in gebruik te nemen en dan pas een DPIA te doen. Dan zijn de mogelijkheden om risico's weg te nemen vaak al minder en hebben mogelijke privacyrisico's niet mee kunnen wegen in de keuze tussen systemen.
Een ander punt is dat DPIA's nu nog niet standaard aan de FG worden toegestuurd. Dat moet wel gebeuren, zodat er de mogelijkheid is een advies mee te geven.

Bijzonderheden

Klacht over bezoekersparkeren en onderzoek AP
In het najaar van 2018 meldde de AP het college dat het een klacht had ontvangen over de wijze waarop het bezoekersparkeren is geregeld. Hierover heeft een gesprek plaatsgevonden met de AP, om toe te lichten hoe het systeem werkt en hoe de DPIA was uitgevoerd. De AP had kritische vragen,

waarop ter plekke en ook in vervolg op het gesprek is er informatie uitgewisseld. Het leidde ertoe dat een opdracht is verstrekt aan PI-Lab (een samenwerking van TNO, de universiteiten van Nijmegen en Tilburg en de stichting Internet Domeinregistratie Nederland) om te adviseren hoe het kentekenparkeren zo kan worden ingericht dat de privacy maximaal wordt gewaarborgd. Dit onderzoek is nog niet afgerond. De AP heeft eind 2019 wel besloten een onderzoek in te stellen naar het bezoekersparkeren. Na de aankondiging van het onderzoek is de gevraagde informatie verstrekt. Daarop is tot nu toe nog geen antwoord ontvangen.

Testen met persoonsgegevens
Bij de behandeling op 28 maart 2019 van het Rekenkamerrapport over informatiebeveiliging heeft de raad motie 14.2 aangenomen: Testen doen we met geanonimiseerde persoonsgegevens. Daarin wordt het college verzocht ervoor te zorgen dat er niet meer met persoonsgegevens wordt getest en de raad voor de Kadernota te informeren over de genomen stappen. Naar aanleiding van deze motie hebben Haarlem, de Drechtsteden en de VNG gezamenlijk contact gezocht met de AP om de problematiek te bespreken. De AP onderkende in dat gesprek dat het probleem ingewikkeld is, doordat veel systemen gebruik maken van persoonsgegevens uit andere, vaak externe, systemen. Het probleem kan dan alleen worden opgelost door gelijktijdig in alle betrokken systemen de nodige aanpassingen te doen. Daarbij komt voor veel gevallen de afhankelijkheid van de leverancier. De oplossingsrichting wordt langs twee lijnen gekozen. Enerzijds is de VNG in gesprek met een aantal leveranciers die aan veel gemeenten leveren. Anderzijds worden samen met de VNG de systemen die wat overzichtelijker zijn aan de hand van de DPIA doorlopen om tot een oplossing te komen.

Vooruitblik 2020

In 2020 krijgt het Sociaal Domein in den brede prioriteit. Op dat gebied zijn er veel privacyrisico's, doordat er met veel, vaak gevoelige gegevens wordt gewerkt. Bovendien zijn er veel samenwerkingspartners met wie gegevens worden uitgewisseld. Met alle afdelingen in het Sociaal Domein wordt een self assessment gedaan. Dat levert een beeld van de stand van zaken met daarbij adviezen voor mogelijke verbeteringen. Een tweede inhoudelijke prioriteit is de verdere implementatie van de Wet Politiegegevens, die mede in het Sociaal Domein zijn beslag krijgt.

Daarnaast zijn er drie punten die organisatiebreed spelen:
1. Verdere aanpak Anonimiseren van testdata.
2. Risico-analyse van het e-mailverkeer met de partners met wie geregeld gevoelige informatie wordt gewisseld en implementeren van maatregelen om die risico's te beperken.
3. Risico-analyse van het documentmanagementsysteem Verseon en implementeren van maatregelen om de risico's te beperken.

Tot slot worden instrumenten verbeterd en procesbeschrijvingen gemaakt voor de melding van datalekken en voor het behandelen van inzage- en andere AVG-verzoeken.

Begrippen en afkortingen

- *AVG*
  Algemene verordening gegevensbescherming. Europese verordening omtrent gegevensbescherming, bevat het privacyrecht zoals dat rechtstreeks van toepassing is in alle EU-lidstaten.

- *AP*
  Autoriteit Persoonsgegevens. De nationale privacyautoriteit, die toezicht houdt op de naleving van de AVG.

- *FG*
  Functionaris voor de gegevensbescherming. Onafhankelijk adviseur en intern toezichthouder op het naleven van de AVG, contactpersoon voor de AP.

- *DPIA*
  Data Protection Impact Assessment of Gegevensbeschermingseffectbeoordeling. Risicoanalyse van een (voorgenomen) verwerking van persoonsgegevens die waarschijnlijk grote risico's kent voor de rechten en vrijheden van betrokkenen.

- *Persoonsgegeven*
  Elk gegeven dat zonder al te veel inspanning te herleiden is naar een natuurlijk persoon.

- *Verwerking van persoonsgegevens*
  Elke handeling met persoonsgegevens, zoals bijvoorbeeld registreren, kopiëren, raadplegen, verstrekken aan een ander of vernietigen.

- *Verwerkersverantwoordelijke*
  De persoon of organisatie die formeel verantwoordelijk is voor een verwerking van persoonsgegevens. In de gemeente gaat het doorgaans om het college, de raad of de burgemeester.

- *Verwerker*
  De persoon of organisatie die in opdracht van de verwerkersverantwoordelijke persoonsgegevens verwerkt.

  Verwerkersovereenkomst
  Overeenkomst tussen verwerkersverantwoordelijke en verwerker waarin afspraken worden gemaakt over de gegevensverwerking over onder meer doel, welke gegevens, beveiligingsmaatregelen en duur van de verwerking.