Nota

Privacybeleid Haarlem

Haarlem
januari 2017

Privacy in Haarlem

1. Inleiding

Privacy is een onderwerp dat de laatste jaren veel in de belangstelling staat. Data zijn hot en worden het nieuwe goud genoemd. De mogelijkheden om gegevens en dus ook persoonsgegevens digitaal op te slaan, te bewerken en te delen hebben de afgelopen jaren een enorme vlucht genomen. Het gebruik van smartphones, laptops, tablets in het dagelijks leven is vanzelfsprekend geworden en een organisatie als de gemeente verwerkt enorm veel gegevens digitaal. De digitalisering brengt veel mogelijkheden met zich mee. Het kan bijvoorbeeld dienstverlening aan bewoners en organisaties vergemakkelijken en ook het maken en uitvoeren van beleid ondersteunen.

Zoveel gegevens die digitaal zijn vastgelegd, brengen echter ook risico's met zich mee, zeker daar waar het om persoonsgegevens gaat. Voorkomen moet worden bijvoorbeeld dat – welwillend of kwaadwillend – meer mensen dan nodig en wenselijk toegang hebben of zichzelf toegang verschaffen tot de opgeslagen gegevens. Mensen van wie de gemeente gegevens verwerkt, hebben er recht op dat hun persoonlijke levenssfeer wordt beschermd tegen onnodige pottenkijkers of nog erger tegen manipulatie van gegevens, zowel binnen als buiten de organisatie. Nieuwe gemeentelijke taken in het sociaal domein hebben geleid tot veel aandacht voor het belang van privacy. In bredere zin heeft ook de affaire die Edward Snowden heeft ontketend ertoe bijgedragen dat velen zich meer bewust zijn geworden van hoeveel gegevens er in systemen zijn opgeslagen en hoe gemakkelijk het is met de huidige digitale middelen om die op te zoeken en door te geven. Je kunt niet zomaar uitgaan van ieders goede wil. Mensen willen bovendien niet alleen gegevens afschermen als het om slechte bedoelingen of illegale activiteiten gaat maar ook omdat men gewoon niet alles over zichzelf bloot wil geven. Dat sommigen zelf veel informatie over zichzelf online zetten wil nog niet zeggen dat ze het dan ook goed vinden dat anderen informatie over hen verzamelen of verspreiden en neemt ook niet de eigen verantwoordelijkheid van de gemeente weg.

Gemeenten bezitten heel veel persoonsgegevens. Denk bijvoorbeeld aan de Basisregistratie persoonsgegevens, gegevens van cliënten van de sociale dienst, de salarisadministratie of de registratie van houders van parkeervergunningen. Met de nieuwe gemeentelijke taken in het sociaal domein is het aantal gegevens dat de gemeente zelf bezit en dat anderen bezitten die in opdracht van de gemeente werken alleen maar toegenomen. Die gegevens zijn nodig voor het uitvoeren van wettelijke taken. Het is van belang daar zorgvuldig mee om te gaan en ze goed te beschermen.

Wat deed Haarlem tot nu toe aan privacy?
Privacy is natuurlijk niet een volledig nieuw thema. Van 1988 tot 2006 kende Haarlem een zogeheten Registratiecommissie, die tot taak had te adviseren over de bescherming van persoonsgegevens. In 2006 werd deze commissie opgeheven en werd ook de Privacyverordening ingetrokken, omdat de zorg voor privacy onderdeel werd van de algemene interne kwaliteitszorg. Door voortschrijdende digitalisering en ook nieuwe wetgeving volstaat dat niet meer en is extra aandacht nodig en een expliciet privacykader.

Doelen van de nota en raakvlakken met ander beleid
Deze nota heeft drie hoofddoelen. Ten eerste wordt beschreven welke uitgangspunten Haarlem hanteert op het gebied van privacybescherming. Ten tweede wordt een concreet kader vastgesteld. Ten derde wordt besloten vooruitlopend op de wettelijke verplichting een Functionaris Gegevensbescherming aan te stellen.

Daarbij wordt vooruitgekeken naar nieuwe regelgeving die recent van kracht is geworden dan wel van kracht gaat worden, zoals de plicht datalekken te melden en de nieuwe Europese verordening Gegevensbescherming. De nota heeft betrekking op de privacy van zowel extern betrokkenen, de burgers, als van intern betrokkenen, de bestuurders, raadsleden en ambtenaren.

Het privacybeleid raakt aan een aantal andere beleidsvelden. In de Nota Informatievoorziening 'Transparant en veilig' (2015/128172) en in de nota Minimaliseren aantal geheime stukken (2015/34307) is vastgelegd dat Haarlem als uitgangspunt hanteert dat het maximaal transparant werkt volgens het principe ' openbaar tenzij'. Dat blijft voorop staan. Privacy kan echter een reden zijn om gegevens toch af te schermen. Dat dient de gemeente goed te organiseren. Wie bewust andermans privacy schendt, maakt zich schuldig aan een integriteitsschending zoals bedoeld in de notitie Integriteitsmeldingen (2015/467586). Nog een relevant aandachtsgebied vormen de open data. Binnenkort verschijnt een nota over wat Haarlem wil bereiken met open data en hoe daarmee om te gaan. Er is ook een raakvlak met het beleid rond Participatie en Inspraak, waar het gaat om de beantwoording van zienswijzen. Volgens zowel het participatiebeleid als volgens de voorliggende nota Privacybeleid Haarlem worden die geanonimiseerd bij publicatie.

2. Wat is privacy en waarom is het van belang?

In juridische zin heeft privacy betrekking op het beschermen van persoonsgegevens: alle gegevens die zijn terug te leiden tot een individueel persoon en die geordend (meestal geautomatiseerd, in elk geval doorzoekbaar) worden verwerkt. Of iets een persoonsgegeven is, kan afhangen van de omstandigheden. Een kenteken sec is bijvoorbeeld geen persoonsgegeven maar in combinatie met een adres leidt het al snel tot een persoon. De Wet bescherming persoonsgegevens benoemt bovendien wat 'bijzondere persoonsgegevens' zijn. Dat zijn bijvoorbeeld gegevens over ras, over geloof, over gezondheid of strafrechtelijke gegevens. Deze genieten extra bescherming.

Het maatschappelijke begrip privacy is breder en tegelijk abstracter. Het is misschien samen te vatten als de te respecteren behoefte van mensen om een deel van hun leven af te schermen voor buitenstaanders. Daarbij zijn er gradaties in welke informatie mensen voor zichzelf willen houden of juist delen. Wat je in je dagboek schrijft, vertel je bijvoorbeeld minder gauw aan een ander dan waar je werkt. Er zijn ook gradaties in degenen voor wie mensen informatie willen afschermen. Familieleden en goede vrienden mogen meestal meer weten dan mensen met wie je een zakelijke relatie hebt. Tegelijk is het zo dat sommige vertrouwelijke gegevens juist worden gedeeld of moeten worden gedeeld met iemand vanwege diens functie, bijvoorbeeld een huisarts of een medewerker van de sociale dienst. En dan maakt het ook nog uit op wat voor manier je informatie deelt, in een persoonlijk gesprek of op je facebookpagina.

De gemeente werkt in eerste instantie met de juridische regels maar het is goed de maatschappelijke dimensie van privacy daarbij in het achterhoofd te houden.

Waarom is bescherming van privacy van belang?
Mensen over wie de gemeente gegevens bezit, moeten erop kunnen vertrouwen dat die gegevens niet in handen komen van anderen die het niets aangaat. En ook dat de gemeente of organisaties met wie de gemeente samenwerkt zelf zo min mogelijk gegevens verzamelen; alleen die gegevens die werkelijk nodig zijn. Dat geldt voor gegevens van zowel burgers als van bestuurders, raadsleden en ambtenaren. In de eerste plaats omdat dat in de wet staat. En evenzeer omdat het vervelend is voor de betrokkene – de maatschappelijke connotatie van privacy – maar ook omdat het gevolgen kan hebben. Als bijvoorbeeld de leerkracht van je kind een GGD-dossier te zien krijgt, heeft die misschien op voorhand al een gekleurd beeld van het kind en ontneemt het daarmee bepaalde kansen. Nog veel ingrijpender is het als een ander zich voor jou uitgeeft. Identiteitsfraude kan mensen grote schulden bezorgen of zorgen dat ze ten onrechte als crimineel worden gezien en ook zo worden behandeld. Het gaat erom dat je zelf controle kunt houden over je gegevens.

Als de gemeente slordig omgaat met persoonsgegevens of ten onrechte vraagt om bepaalde gegevens, kan dat ook voor de gemeente zelf schadelijk zijn. Er wordt nu al in de media geregeld heel wantrouwend gekeken naar welke gegevens gemeenten al dan niet menen nodig te hebben om jeugdzorg te betalen. Als er in concrete gevallen iets mis gaat, is dat in eerste instantie voor de betrokken persoon vervelend maar het kan ook voor de gemeente vervelende gevolgen hebben. Het schaadt het imago van betrouwbare partner en kan leiden tot juridische procedures. Die kunnen uiteindelijk nog verdere imagoschade en bovendien bij een veroordeling kosten opleveren. Ook kan de Autoriteit Persoonsgegevens (AP, voorheen bekend als het College Bescherming Persoonsgegevens) boetes opleggen als het constateert dat een organisatie zich niet aan de wet houdt. De maximale hoogte van die boete is per 1 januari 2016 verhoogd naar € 810.000,- of 10 % van de jaaromzet. Met de nieuwe Europese verordening wordt dit verhoogd tot 20 miljoen euro of 4 % van de jaaromzet.

Waardoor kan er iets mis gaan?
Als er iets misgaat op het gebied van privacybescherming, kan dat liggen aan zowel menselijk als technisch falen.

Van technisch falen is sprake als informatie naar buiten komt door een hack of door een virus. Dat kan gebeuren door inbraak in dat deel van de gemeentelijke systemen waarin de gegevens zijn geregistreerd maar ook doordat mailverkeer wordt onderschept. De Wet bescherming persoonsgegevens vereist dat hiertegen ‘passende’ technische en organisatorische maatregelen worden genomen.

Een groot risico zit daarnaast in de organisatorische en menselijke kant. In het niet goed organiseren van welke informatie mag worden geraadpleegd of opgevraagd door wie. In onoplettendheid doordat een scherm blijft openstaan, het laten slingeren van een usb-stick of uitwisselen van meer gegevens dan noodzakelijk dan wel op een onveilige manier.

Veel taken laat de gemeente inmiddels uitvoeren door partners. Ook in het werkproces van een partner kan iets mis gaan. Om dat te voorkomen worden afspraken gemaakt in de vorm van

bijvoorbeeld een privacyprotocol zoals dat met de deelnemende organisaties in de sociale wijkteams is gesloten en met zogenaamde bewerkersovereenkomsten, waarin wordt vastgelegd hoe de partner met persoonsgegevens om moet gaan. De gemeente is ervoor verantwoordelijk dat afspraken worden gemaakt en dat die worden nageleefd, zij is aansprakelijk als dat niet gebeurt. De uitvoerende partij is aansprakelijk voor schade die ontstaat door zijn werkzaamheden. Waarschijnlijk zullen de uitvoerders – de daadwerkelijke bewerkers – zelf ook meer verantwoordelijkheden krijgen, als de nieuwe Europese privacyverordening in werking treedt. Die wordt verderop in deze nota besproken.

3. Regelgeving

Er zijn verschillende wetten waarin bepalingen staan met betrekking tot privacybescherming. De Wet bescherming persoonsgegevens (Wbp) is de belangrijkste en meest algemene nationale wet op het gebied van privacybescherming, de basis van de Nederlandse privacyregels. Deze wet is gebaseerd op een Europese richtlijn uit 1995. Die richtlijn wordt vervangen door een Europese verordening die in 2018 in werking treedt. De Wbp en de nieuwe Europese Algemene verordening gegevensbescherming worden hieronder beschreven.

Toezicht door de Autoriteit Persoonsgegevens

De instantie die in Nederland toezicht houdt op de naleving van de Wbp is de Autoriteit Persoonsgegevens (AP), voorheen genaamd College Bescherming Persoonsgegevens. Alle registraties van persoonsgegevens moeten onder de huidige wet in principe worden gemeld bij de AP, tenzij er een vrijstelling geldt. De AP kan dwangsommen en boetes opleggen aan wie zich niet aan de regels houdt.

Wet bescherming persoonsgegevens

Hierin is vastgelegd wat persoonsgegevens zijn en onder welke voorwaarden die mogen worden bewerkt. Bewerken is elke handeling met betrekking tot persoonsgegevens, zoals vastleggen, ordenen, wijzigen, opvragen en doorsturen.

Gronden voor verwerking

Er moet een grond zijn om persoonsgegevens te mogen verwerken. Naast ondubbelzinnige toestemming van betrokkene is er een beperkt aantal gronden voor verwerken van persoonsgegevens. Een belangrijke grond voor de gemeente is dat de verwerking nodig is voor ‘ de uitvoering van een wettelijke plicht’ of ‘voor een goede vervulling van een publiekrechtelijke taak’. Soms wordt in een wet duidelijk omschreven dat bepaalde gegevens nodig zijn voor de uitvoering van een wettelijke taak maar dat is niet altijd zo. Dan kan het dus toch gerechtvaardigd zijn persoonsgegevens te verwerken, als dat nodig is voor een publiekrechtelijke taak of om een wettelijke verplichting uit te voeren.

Doelbinding

Een basisprincipe op het gebied van privacyrecht is de zogenaamde doelbinding. Als persoonsgegevens worden verwerkt, gebeurt dat voor een duidelijk omschreven en gerechtvaardigd doel. De gegevens mogen vervolgens niet voor een ander doel worden gebruikt. Dat is voor een organisatie als de gemeente, waar veel gegevens worden verzameld voor diverse doeleinden, heel belangrijk. Als bijvoorbeeld gegevens bekend zijn van personen doordat zij een

uitkering aanvragen, kunnen die niet zomaar gebruikt worden om hen uit te nodigen als Gast van de raad. Of om te zoeken of zij toevallig ook een bouwvergunning aanvragen. Als je gegevens wilt gebruiken voor een ander doel dan waarvoor ze zijn verzameld, is ondubbelzinnige toestemming van de betrokkene nodig. Bovendien moeten de gegevens worden verwijderd op het moment dat ze niet meer nodig zijn voor het specifieke doel.

Meldplicht datalekken
Met ingang van 2016 is in de Wbp de zogenaamde meldplicht datalekken opgenomen. Die houdt in dat een datalek met ernstige nadelige gevolgen voor de bescherming van persoonsgegevens onmiddellijk moet worden gemeld aan de AP. Een datalek is bijvoorbeeld het kwijtraken van een laptop met daarop persoonsgegevens, per ongeluk versturen van een mail aan een verkeerd adres of een inbraak in een bestand met persoonsgegevens.

Een andere belangrijke verandering is dat de maximale boete die het CBP (vanaf dan: Autoriteit persoonsgegevens) kan opleggen verhoogd wordt van 4.500 tot 810.000 euro.

Europese Verordening Gegevensbescherming
De Wbp is de implementatie van een Europese richtlijn uit 1995. In april 2016 is de Algemene Verordening Gegevensbescherming (AGV) aangenomen door het Europese Parlement. Deze verordening vervangt de richtlijn en ook de Wbp, doordat een verordening rechtstreeks werkt in alle lidstaten. De verordening treedt in werking op 25 mei 2018.

De werkingssfeer - de regels omtrent wat persoonsgegevens zijn en wie ze wanneer mag verwerken - blijft min of meer dezelfde. Daaromheen verandert wel het nodige, op het gebied van handhaving en transparantie. Bovendien worden veel particuliere bedrijven en organisaties en alle overheden verplicht een zogeheten Functionaris Gegevensbescherming aan te stellen.

Versterking rechten van de betrokkene
De rechten van de betrokkene worden versterkt. Er worden hogere eisen gesteld aan transparantie. Het moet voor betrokkenen duidelijk zijn welke gegevens over hen worden verwerkt en met welk doel. Zij worden hierover geïnformeerd in duidelijke, eenvoudige taal. Als toestemming nodig is voor het verwerken van persoonsgegevens wordt dat expliciet gevraagd. De betrokkene moet er daarbij op worden gewezen dat hij de toestemming ook weer kan intrekken maar dat dat eventueel wel consequenties kan hebben voor de dienstverlening. Twee andere belangrijke rechten zijn het recht op rectificatie en het zogenaamde recht op vergetelheid. Het eerste houdt in dat betrokkene een verzoek kan doen om onjuiste gegevens te corrigeren. Dit moet vervolgens zonder onredelijke vertraging gebeuren. Het recht op vergetelheid houdt in dat de betrokkene er recht op heeft dat zijn gegevens helemaal worden gewist, bijvoorbeeld als de gegevens niet meer nodig zijn voor het doel waarvoor ze waren verzameld of als hij zijn toestemming intrekt en er geen andere grond is voor het verwerken van de gegevens. Tot slot krijgt de betrokkene het recht van inzage.

Documentatieplicht in plaats van meldplicht
Nu moeten gegevensverwerkingen nog worden gemeld bij de AP. Daarvoor in de plaats komt straks een documentatieplicht. De gemeente moet kunnen laten zien hoe haar privacybeleid eruit ziet, welke gegevens waar vastliggen, wat de bronnen zijn, wie bewerkers zijn en hoe de informatiebeveiliging is georganiseerd en voorafgaand aan het verzamelen van gegevens een

zogenaamd privacy impact assessment (PIA) doen, om te beoordelen welke impact de voorgenomen gegevensverzameling heeft voor de betrokkenen. Er zullen criteria worden ontwikkeld om te beoordelen wanneer een PIA nodig is. Betrokkene wordt geïnformeerd over welke gegevens van hem worden vastgelegd, met welk doel en voor hoelang. Hij wordt daarbij geïnformeerd dat hij een verzoek kan indienen om zijn eigen gegevens in te zien en te verzoeken deze te corrigeren of te wissen. In het geval van wettelijke taken zal het niet altijd mogelijk zijn om gegevens te laten wissen, bijvoorbeeld als het om strafrechtelijke gegevens gaat. Ook voor verwerking van persoonsgegevens met als grondslag toestemming gelden onder de nieuwe Verordening aangescherpte eisen. Als organisatie moet je kunnen bewijzen dat een betrokkene toestemming heeft gegeven. Ook moet voor de betrokkene in begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal worden gepresenteerd op zodanige wijze dat voor de betrokkene duidelijk is waarvoor hij toestemming verleent. Toestemming kan te allen tijde door de betrokkene worden ingetrokken.

Er komen meer verantwoordelijkheden te liggen bij de bewerker die in opdracht werkt. Dat betekent dat duidelijk moet worden afgesproken wie in een ketensamenwerking de eerstverantwoordelijke is en dat die afspraken worden vastgelegd.

Overheden worden verplicht een Functionaris Gegevensbescherming (FG) te benoemen, die zijn taken onafhankelijk uitvoert. In artikel 37 tot en 39 met van de Algemene Verordening Gegevensbescherming wordt een omschrijving gegeven van de positie en taken van de FG. De FG informeert en adviseert over regelgeving met betrekking tot privacy en ziet erop toe dat die regels worden nageleefd. Hij zorgt dat de organisatie privacybewust wordt, geeft advies over en ziet toe op de uitvoering van de zogeheten gegevensbeschermingseffect-beoordeling (ook vaak PIA genoemd: privacy impact assessment) en is de contactpersoon voor de Autoriteit Persoonsgegevens.

De nationale toezichthouders krijgen sterkere handhavingsmogelijkheden. Onder andere wordt de maximale boete verhoogd, in de meest vergaande tekstvariant zelfs tot een maximum van twintig miljoen euro of 4% van de wereldwijde jaaromzet van een organisatie per overtreding. Ze mogen ook de verantwoordelijke opdragen gegevens te rectificeren of vernietigen of om de verwerking van gegevens al dan niet tijdelijk te beperken.

4. Wat zijn de Haarlemse principes?

Binnen de ruimte van de wet, hanteert Haarlem een aantal principes op het gebied van privacy.

Werk met het minimum aan persoonsgegevens
Voor bepaalde taken is het onontkoombaar of zelfs verplicht dat er persoonsgegevens worden verwerkt. Dat gebeurt met het minimum aan gegevens dat daarvoor nodig is. Vrijelijk raadplegen of combineren van gegevens is niet toegestaan.

Voor het verwerken van persoonsgegevens wordt altijd een afweging gemaakt tussen het doel waarvoor de gegevens worden verwerkt en de impact die dat heeft op de privacy van betrokkenen. Die moeten in verhouding staan tot elkaar. Daarbij wegen de bijzondere

persoonsgegevens dan weer zwaarder dan bijvoorbeeld adresgegevens. Er wordt in principe gekozen voor de voor betrokkene minst belastende aanpak. Een voorbeeld van een afweging is de vraag of je in een onderzoek naar het gebruik van sociale voorzieningen maximaal nauwkeurig bent en gegevens over het gebruik in kaart brengt tot op het niveau van individuele adressen of kun je ook toe met iets minder nauwkeurige gegevens op postcodeniveau.

Dit principe kan betekenen dat de service minder wordt. Als je bijvoorbeeld mensen wilt attenderen op mogelijke financiële ondersteuning in het kader van het armoedebeleid maar je mag daarvoor niet de adressen gebruiken van degenen die een uitkering ontvangen. Dat zou betekenen dat je die ondersteuningsmogelijkheden alleen via algemene aankondigingen bekend kunt maken. In dergelijke gevallen is soms een tussenweg mogelijk door toestemming te vragen. Het moet dan wel gaan om een zogenaamd 'informed consent': degene die toestemming geeft, moet goed begrijpen waarvoor hij precies toestemming geeft en hoe hij de toestemming weer kan intrekken. Werken met persoonsgegevens op basis van toestemming gebeurt alleen in situaties waarin de betrokkene zich vrij voelt de toestemming al dan niet te geven. Dat is niet snel het geval, omdat de verhouding tussen overheid en burger nu eenmaal een ongelijke is. Het zal dus alleen gebeuren als daarmee een eenvoudige service kan worden verleend. Uitgangspunt is dat het de betrokkene geen daadwerkelijk nadeel mag opleveren als de toestemming niet wordt gegeven. In het beschreven voorbeeld betekent het dat je dan alleen via algemene aankondigingen en niet rechtstreeks geattendeerd wordt op de mogelijkheid van financiële ondersteuning. Het mag echter niet betekenen niet dat je daar geen recht meer op zou hebben.

> Zo is de gemeente weliswaar verantwoordelijk voor hulpverlening aan kinderen in het kader van de Jeugdwet, maar beschikken we niet over de inhoudelijke dossiers. De aanbieder vermeldt op de factuur wel het BSN van het kind, zodat de gemeente kan zien dat het gaat om een kind dat in Haarlem woont. Daarnaast wordt ook een productcode genoemd, die aangeeft welk type zorg is verleend. In het geval van Jeugd GGZ betreft dit DiagnoseBehandelCombinaties die het medisch beroepsgeheim raken. Er kan binnen de Jeugdwet gebruik worden gemaakt van de zogenaamde opt-out-regeling: als ouders bezwaar maken tegen het delen van deze informatie, mag de zorgaanbieder de zorg declareren zonder de code. Er loopt een pilot om op een andere manier, op hoofdlijnen, te factureren.

Ook bij de publicatie van zienswijzen wordt de afweging gemaakt tussen het doel waarvoor de gegevens worden verwerkt en de impact die dat heeft op de privacy van betrokkenen. Bij de publicatie van zienswijzen wordt als beleidslijn gekozen om ten behoeve van het besluitvormingsproces de namen van diegenen die een zienswijze ingediend hebben wel bekend te maken en te publiceren op internet. Uit het antwoord van de minister van binnenlandse zaken op kamervragen over deze kwestie[1] blijkt dat "het aankomt op een afweging van belangen door gemeenten in het specifieke geval". De post- en mailadressen worden niet vermeld.

Maximale transparantie

De overheid en dus ook de gemeente werkt maximaal transparant. Persoonsgegevens zelf lenen

[1] Beantwoording-kamervragen-over-verwarring-omtrent-het-publiceren-van-namen-door-gemeenten Kenmerk 2014-0000288486

zich uit hun aard niet voor openbaarmaking maar de manier waarop je met persoonsgegevens omgaat wel. Dat betekent een goede documentatie. Het moet zichtbaar en controleerbaar zijn welke persoonsgegevens worden verwerkt, om wat voor persoonsgegevens het gaat en wat het doel is van de verwerking. Het werk wordt zo ingericht dat alleen die medewerkers die de informatie werkelijk nodig hebben voor hun werk toegang hebben. Dat geldt voor verwerking van gegevens in eigen huis maar ook voor verwerkingen door anderen als dat onder verantwoordelijkheid van de gemeente gebeurt. Er worden standaarden ontwikkeld voor deze documentatie, op zo'n manier dat daarmee ook wordt voldaan aan de eisen van de AGV.

Privacy by design
Privacy by design betekent dat als nieuwe werkprocessen worden ingericht die direct zo worden ontworpen dat de privacy gewaarborgd is. Dat is efficiënter en goedkoper dan achteraf aanpassen. Door vooraf goed na te denken over hoe je systemen en processen inricht, wordt de kans dat je iemands privacy schendt kleiner. En daarmee ook het risico op boetes, claims en imagoschade.

Het begint met de vraag wat het doel is dat je wilt bereiken, of je daarvoor werkelijk persoonsgegevens nodig hebt en of dat mag op grond van de wet. Als dat zo is, wordt bezien hoe je dat met zo min mogelijk persoonsgegevens kunt organiseren. Daarbij komt de proportionaliteit aan de orde: staat de mate waarin privacy wordt 'geschonden' in verhouding tot het doel waarvoor je de gegevens verwerkt? Daarbij komt de vraag welke maatregelen nodig zijn om maximaal zorgvuldig te zijn. Wie moet toegang hebben tot de gegevens? Wie bepaalt dat en wie beheert deze autorisaties? Hoe scherm je de gegevens af voor anderen? Hoe informeer je de betrokkenen? Tot wanneer blijven de gegevens bewaard en hoe zorg je dat ze na die termijn daadwerkelijk worden verwijderd?

Het beantwoorden van dit type vragen gebeurt in een zogeheten PIA: privacy impact assessment. Afhankelijk van het proces dat wordt ingericht en de ingrijpendheid en complexiteit worden daar meer of minder collega's bij betrokken. Het betekent ook dat er eisen worden gesteld aan de leveranciers van systemen. Dat alles betekent een extra stap in het inrichten van systemen en processen, die tijd kost. Er wordt op dit moment een standaard vragenlijst ontwikkeld voor PIA's. PIA's worden overigens onder de AVG verplicht zodra gegevens worden verwerkt waarbij er een hoog risico is voor het recht op privacybescherming.

Mensen kunnen hun eigen gegevens zien
Iedereen kan opvragen welke gegevens over hem of haar de gemeente verwerkt, met welk doel dit gebeurt en met wie deze gegevens worden gedeeld. Op dit moment worden op zo'n vraag de gegevens nog 'handmatig' bij elkaar gezocht. Naar verwachting kunnen gemeenten op termijn deze informatie geautomatiseerd aanbieden op MijnOverheid Persoonlijke Gegevens[2]. Op dit moment kunnen gemeenten nog niet aansluiten op die landelijke voorziening. Wel kunnen voorbereidingen worden getroffen op deze ontsluiting door de eigen processen te stroomlijnen en te zorgen dat genoemde gegevens op uniforme wijze worden vastgelegd, zodat eenvoudig kan worden aangesloten op het centrale platform zodra dit mogelijk is.

[2] Zie https://mijn.overheid.nl/info/persoonlijkegegevens

Op grond van jurisprudentie van het Europese Hof van Justitie moeten mensen geïnformeerd worden als overheden persoonsgegevens van hen uitwisselen, ook als dat twee overheden binnen één lidstaat zijn. Dit betekent dus dat wij mensen in die gevallen actief moeten informeren.

Geen persoonsgegevens per mail
Als het toegestaan en nodig is persoonsgegevens uit te wisselen, moet dat op een veilige manier gebeuren. Het is in elk geval niet veilig via onbeveiligde email of via Pleio. Dit is een probleem waar alle gemeenten tegenaan lopen en dat nog niet is opgelost. Er wordt op dit moment gewerkt aan een goed beveiligd alternatief. Voor jeugdhulp wordt Zorgmail geïmplementeerd, voor andere uitwisselingen is het het veiligst gebruik te maken van FileCap. De organisatie wordt daarover geïnstrueerd.

Dilemma
Hoe belangrijk privacy ook is, soms ontstaat er toch een dilemma. Als bijvoorbeeld in een gezin sprake is van problemen die volgens de zorgverlener wellicht beter kunnen worden aangepakt in samenwerking met een andere zorgverlener, kan hierover afstemming worden gezocht. Hoewel dit anoniem zou moeten gebeuren, kan het voorkomen dat gegevens over het gezin worden doorgegeven aan die andere zorgverlener. Het is belangrijk de afweging om wel of niet gegevens te delen expliciet te maken. Kun je uitleggen waarom een beslissing is genomen om gegevens te delen of niet? In het voorbeeld hiervoor van het gezin dat met een andere hulpverlener gebaat zou kunnen zijn, kan het gezin zelf worden uitgenodigd bij het gesprek met die andere hulpverlener, zodat het zelf ook grip houdt op wat wel en niet wordt verteld. Hoe moeilijk dit soms ook is voor professionals. Door mensen zoveel mogelijk zelf de controle te laten behouden en door transparant te zijn, wordt een dergelijke afweging op een controleerbaar integere manier gemaakt. Een eenvoudige richtlijn is voor dit soort dilemma's niet te geven. Door de afweging bespreekbaar te maken, wordt het ook mogelijk de kwestie voor te leggen aan een leidinggevende of bestuurder op het moment dat er niet een vanzelfsprekende conclusie is.

Role based access
Of je toegang hebt tot bepaalde gegevens is afhankelijk van je taak. Elk systeem waarin persoonsgegevens worden verwerkt, heeft een functioneel beheerder, degene die verantwoordelijk is voor het werkproces waarvoor het systeem wordt gebruikt. Deze functioneel beheerder kent autorisaties toe aan diegenen die met het systeem moeten kunnen werken vanwege hun taak. De autorisaties worden bijgehouden en ook weer ontnomen zodra de medewerker de taak waarvoor hij de gegevens nodig had niet meer verricht. Het gebruik van de systemen wordt gelogd en steekproefsgewijs gecontroleerd. Deze aanpak wordt systematisch doorgevoerd.

5. Waar staan we nu?

Privacy is niet een nieuw onderwerp. In sommige werkgebieden van de gemeente is het al heel lang nadrukkelijk een aandachtsgebied. Denk bijvoorbeeld aan het raadplegen van de BRP en van Suwinet. Hier gelden van oudsher strikte regels en is ook de controle op naleving daarvan doorgaans goed geregeld. Ook bij de start van de nieuwe taken in het Sociaal Domein is van meet af aan aandacht besteed aan privacy van de mensen om wie het gaat. Op sommige andere

terreinen is er minder aandacht aan besteed. Alles bij elkaar is het beeld divers. In de nota 'Informatievoorziening in samenhang' (2014/267561) is besloten om vier uur per week beschikbaar te stellen voor een adviseur Privacy. Deze adviseur maakt deel uit van het team van de CIO (Chief Information Officer) en adviseert daarbinnen over hoe privacy te bewaken. Deze heeft ook het initiatief genomen om een informeel netwerk op te zetten met medewerkers uit verschillende delen van de organisatie. Doel is kennis te delen en voor de organisatie aanspreekpunten te creëren. Tegelijk wordt ook de beveiliging van data steeds verder verbeterd, wat natuurlijk ten goede komt aan privacybescherming. Voor het melden van datalekken is een vast werkproces vastgelegd.

Al met al is dit een redelijke aanzet maar het blijkt onvoldoende. Data worden steeds belangrijker en met de nieuwe taken in bijvoorbeeld het sociaal domein en straks de nieuwe Omgevingswet zijn de gemeenten ook verantwoordelijk voor steeds meer data. Daarbij gaat de nieuwe wetgeving hogere eisen stellen aan een goede organisatie van de privacybescherming. Dit alles leidt tot de conclusie dat versterking nodig is. Er zal een Functionaris Gegevensbescherming moeten worden aangesteld en er is in de organisatie als geheel meer tijd en aandacht nodig voor het onderwerp privacybescherming.

6. Wat gaan we doen?

Om het beleid verder in te vullen en praktisch te vertalen wordt vooruitlopend op de verplichting onder de Europese verordening een privacy-adviseur aangesteld. Deze zal het interne privacynetwerk dat nu bestaat verder uitbouwen en verstevigen, om te zorgen dat voldoende kennis voorhanden is in de organisatie. Het gaat om een tactische vertaling en uitvoering van het privacybeleid. Om deze taken uit te voeren en de gemeente voor te bereiden op de nieuwe regels van de AVG is een FG nodig die de functie voltijds uitvoert, in schaal 11A. De functie komt dan naast die van de huidige privacy adviseur (0,1 fte, schaal 13, aangesteld op grond van de nota Informatievoorzienig in samenhang), die de strategische advisering blijft doen in deeltijd. In type taken zijn deze functies te vergelijken met de functies van Information Security Officer en Strategisch adviseur Informatievoorziening. Het jaar 2017 is dan een jaar van transitie, voor 2018 wordt bezien waar en hoe precies de formele functie van Functionaris Gegevensbescherming in de zin van de Europese verordening wordt belegd.

Ter uitvoering van deze nota en ter voorbereiding op de nieuwe regelgeving zullen in elk geval de volgende taken worden uitgevoerd:

- Deze beleidsnota heeft een meer praktische vertaling nodig voor het dagelijks werk. Die is te vinden in de bijlage (Privacy Baseline) en maakt onderdeel uit van deze nota.

- Op verschillende manieren zal aandacht worden gevraagd voor het belang van privacy en wat dat betekent voor ieders werk om het bewustzijn hiervan te verhogen. Waar nodig worden opleidingen aangeboden.

- Vanaf 2018 zullen audits worden gehouden op het gebied van privacy, gecombineerd met de onderwerpen beveiliging en informatiebeheer

- Role based access is van belang uit oogpunt van privacy maar ook vanuit belang van informatiebeveiliging. Deze werkwijze wordt – voor die werkprocessen waar het nog niet zo is – verankerd, inclusief steekproefsgewijze controle.

- Als vervolg daarop wordt een eenduidig proces ontworpen om mensen te antwoorden die vragen hebben over welke gegevens wij van hen hebben en welke daarvan wij met wie delen.