Gemeente Haarlem

# Rapportage 2020-2021

# Functionaris Gegevensbescherming

Cathérine Konijnenbelt

Mei 2022

## *Inleiding*

In 2018 werd de Algemene verordening gegevensbescherming van kracht, waarmee de aandacht voor privacy een stevige impuls kreeg. In deze rapportage staat de vraag centraal hoe de gemeente er na vier jaar nu voor staat op dit gebied. Hoe staat het met de kennis en bewustwording op het gebied van privacy en de naleving van de AVG en wat is er gebeurd in de afgelopen twee jaar?

Over 2020 is niet apart gerapporteerd. De huidige rapportage beslaat daarom zowel 2020 als 2021. In de cijfers (aantallen datalekken, inzageverzoeken e.d.) zijn de jaren uitgesplitst. In het algemene beeld en de uitgelichte bijzonderheden is geen expliciet onderscheid gemaakt naar welk jaar.

Voor 2020 was een aantal acties aangekondigd. De belangrijkste waren het starten met self assessments en de verdere aanpak om te stoppen met het testen met persoonsgegeven. Beide zijn pas in 2021 echt opgepakt. Ook de andere acties zijn pas later in gang gezet. De jaren 2020 en 2021 zijn twee bijzondere jaren geweest, waarin vanwege corona onder bijzondere omstandigheden moest worden gewerkt. Daarin heeft de organisatie zijn weg moeten zoeken, ook in de manier van samenwerken. Die omstandigheden en het feit dat er relatief weinig capaciteit is voor privacyadvisering, hebben ertoe geleid dat de acties die waren voorzien voor 2020 vrijwel allemaal pas later zijn opgepakt.

### *Stand van zaken algemeen*

Er is steeds meer kennis en bewustzijn in de organisatie. Dat blijkt uit de hoeveelheid en inhoud van de vragen die bij zowel de privacyadviseurs als bij de FG binnenkomen. Tegelijk is daaruit merkbaar dat de meeste vragen ad hoc en vaak ook in een laat stadium worden opgelost. Het hangt nu nog teveel af van toevalligheden of wordt onderkend dat de privacykant ook goed moet worden geregeld. Er wordt dan bijvoorbeeld pas als een plan al grotendeels is uitgewerkt beseft dat ook moet worden nagedacht over de privacyrisico's of laat in een aanbestedingsproces onderkend dat er een DPIA moet worden gedaan. Of het is wel duidelijk dat er gevoelige gegevens worden uitgewisseld met een externe partner maar er zijn geen standaardoplossingen of -afspraken over hoe dat zorgvuldig en veilig te doen. Hoewel aandacht en kennis verschillen en er echt goede stappen worden gezet, lijkt de organisatie nu grosso modo op dit niveau te blijven steken. Afgaand op de self assessments die nu zijn gedaan, scoren de afdelingen gemiddeld een volwassenheidsniveau van tegen de 2 op een schaal van 5.

Om min of meer te voldoen aan de eisen van de AVG is een volwassenheidsniveau 3 nodig. Er is dus een verdere versterking nodig. Dat betekent een verdere investering in kennis en bewustzijn. En ook een investering in middelen (mensen en tijd), zowel in de centrale ondersteuning vanuit de afdeling Interne Dienstverlening (nu net iets minder dan 1,5 fte) als bij de andere afdelingen, daar waar daadwerkelijk met persoonsgegevens wordt gewerkt. Het kennisniveau in de lijnafdelingen is op dit moment erg verschillend. Bij een enkele afdeling is 'privacy' als aandachtsgebied belegd bij een medewerker – al zijn daar niet apart uren voor vrijgemaakt – maar bij de meeste afdelingen is dat niet zo.

In vergelijking met andere gemeenten van vergelijkbare grootte heeft de gemeente weinig privacyadviseurs. Gebaseerd op een vergelijking van 12 gemeenten, variërend van 30.000 tot 900.000 inwoners, heeft de Haarlems-Zandvoortse organisatie de minste adviseurs. Omgerekend naar de bezetting per 100.000 inwoners, hebben deze gemeenten gemiddeld 1,9 fte voor privacyadvisering beschikbaar. De bezetting loopt dan uiteen van 0,7 (Haarlem/Zandvoort) tot 3 (Halderberge, Ermelo/Harderwijk/Zeewolde). Daarbij moet worden gezegd dat kleinere gemeenten relatief een grotere bezetting hebben. Dat is niet gek, aangezien je ongeacht je grootte een bepaalde vaste basis nodig hebt. Maar ook ten opzichte van grotere gemeenten is de bezetting heel mager. Dit

heeft tot gevolg dat de adviseurs vooral reactief zijn in hun werk. Er blijft zo goed als geen tijd over om ook proactief de organisatie te versterken en mee te denken over structurele verbeteringen.

Wel is een start gemaakt met het doen van zogeheten self assessments. Per afdeling wordt daarmee in kaart gebracht wat het niveau van volwassenheid is op een aantal relevante deelthema's, uitmondend in een advies om hierin te groeien. Hiervoor is externe ondersteuning ingehuurd. Op dit moment worden rapportages gemaakt voor tien afdelingen. Ook wordt op dit moment een pilot uitgevoerd om beter uit te werken wat eigenaarschap van mensen (functies), data, processen en applicaties inhoudt en hoe dat op een goede manier in te vullen in de samenwerking tussen lijnafdelingen en ondersteunende afdelingen. Zie ook pagina 6 over *Toegangsrechten.*

***Rechten van betrokkenen***

*Verzoeken*
In 2020 waren er in totaal 11 AVG-verzoeken, waarvan 10 inzageverzoeken en 1 vernietigingsverzoek.
De verzoeken zijn afgehandeld als volgt:

- Bij zes inzageverzoeken zijn de gevraagde persoonsgegevens verstrekt.
- Bij vijf inzageverzoeken is besloten om deze niet in behandeling te nemen in verband met het niet tijdig aanleveren van nadere informatie dan wel legitimatie; in drie gevallen was het achterliggende oogmerk niet het verkrijgen van persoonsgegevens maar het verkrijgen van een dwangsom.
- Het vernietigingsverzoek heeft niet geleid tot vernietiging van persoonsgegevens, omdat de gegevens op grond van de Archiefwet nog moeten worden bewaard.

In 2021 zijn 12 AVG-verzoeken ontvangen, waarvan 11 inzageverzoeken en 1 vernietigingsverzoek.
De verzoeken zijn als volgt afgehandeld:

- Het vernietigingsverzoek is niet in behandeling genomen, omdat de verzoeker niet inging op het verzoek om zich te identificeren en het verzoek te specificeren.
- Bij vier verzoeken zijn de gevraagde gegevens verstrekt.
- Bij één verzoek waren geen persoonsgegevens (meer) aanwezig. Dit ging om camerabeelden.
- Twee verzoeken zijn niet in behandeling genomen in verband met het niet tijdig aanleveren van nadere informatie dan wel legitimatie;
- Twee verzoeken zijn doorgestuurd, omdat een andere organisatie verwerkingsverantwoordelijke was.
- Twee inzageverzoeken bleken niet bedoeld als inzageverzoek op grond van de AVG maar om inzage op grond van de Participatiewet en de BRP en zijn volgens de regels van die wetten afgehandeld.

In één geval wat het achterliggende oogmerk niet het verkrijgen van persoonsgegevens maar het verkrijgen van een dwangsom.

*Bezwaar en beroep*
Tegen 4 van de in 2020 afgehandelde AVG verzoeken is een bezwaar ingediend. Alle bezwaren zijn ongegrond verklaard. Er zijn twee AVG-zaken uit 202 in beroep bij de rechtbank behandeld. Beide zijn ongegrond verklaard. Tegen de in 2021 behandelde verzoeken is geen bezwaar of beroep

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, data protection impact assessment) worden gemaakt. Daarbij wordt beoordeeld of de beoogde gegevensverwerking is toegestaan, wat de privacyrisico's zijn en welke maatregelen nodig zijn om die risico's weg te nemen of te beperken. Om te beoordelen of een DPIA nodig is, is een 'privacy-checklist' ontwikkeld.

Het doen van een DPIA blijft vaak lastig. Om de vragen goed te kunnen beantwoorden, is behoorlijk wat kennis nodig. De privacyadviseurs begeleiden de DPIA's maar de uiteindelijke verantwoordelijkheid ligt bij de betrokken afdeling. Zeker als een afdeling of team voor het eerst een DPIA doet of als het om een wat ingewikkelder proces gaat, is het een intensieve klus. Idealiter zouden afdelingen zelf de DPIA doen en doet de privacyadviseur vervolgens de eerste review. Zover is de organisatie echter nog zeker niet.

In de periode 2020-2021 zijn vijf DPIA's gedaan: voor de vervanging van de parkeerrechtendatabase, voor de scanauto (gericht op het stellen van de juiste privacyeisen bij de aanbesteding, afgerond in 2021), een vervolg-DPIA voor het in gebruik nemen van de scanauto's, voor een pilot met bodycams, voor een webapplicatie ten behoeve internetonderzoek door de sociale recherche en voor verwerkingen in het kader van vroegsignalering bij schulden.

***Meldingen van datalekken***

*Datalekken in 2020*
Er zijn 25 meldingen van een datalek gedaan. In vijf gevallen is het lek ook gemeld aan de Autoriteit Persoonsgegevens (AP), bijvoorbeeld omdat het een groot aantal betrokkenen raakte of omdat op voorhand niet zeker was hoe groot het risico was voor betrokkene (dan wordt voor de zekerheid een melding gedaan). De meeste meldingen gaan om een mail aan de verkeerde persoon of met de verkeerde bijlage, mailadressen in het veld CC in plaats van BCC en verloren of gestolen devices. Eén melding springt eruit: mogelijk was een geheim adres doorgegeven aan de ex-partner van de bewoner. Dat zou een zware integriteitsschending zijn en is uiteraard meteen onderzocht door het management. De gegevens bleken uiteindelijk gelukkig niet bij de gemeente vandaan te zijn gekomen. Daarmee was het slachtoffer echter natuurlijk niet geholpen en het is helaas voor zover bekend niet duidelijk geworden wie of wat wel de bron was van het lek.

*Datalekken in 2021*
Er zijn in 2021 29 datalekken gemeld. In 7 gevallen is het lek gemeld aan de AP. Ook in dit jaar waren de meeste lekken het gevolg van een mail aan een verkeerd adres of met een verkeerde bijlage. Een andere oorzaak van datalekken die ook dit jaar een paar keer terugkwam is verlies of diefstal van een telefoon, tablet of laptop. Telefoons in beheer van de gemeente worden na melding van verlies meteen op afstand gewist. Ook is een paar keer een brief gericht aan de ene persoon meegevouwen in een brief voor iemand anders en zijn gegevens van de ene werknemer gekoppeld aan het account van een andere werknemer.

Het aantal meldingen is iets hoger dan voorgaande jaren (21 in 2018 en 20 in 2019) maar ligt nog steeds lager dan mag worden verwacht. Voor 2020 was voorzien een centrale meldknop te maken op

intranet voor alle typen incidenten met data. Die wordt uiteindelijk naar verwachting gerealiseerd in 2022. Medio 2022 start een bewustwordingscampagne. Naar verwachting zullen dan meer datalekken worden herkend als zodanig en worden gemeld.

***Register van verwerkingen***

Jaarlijks wordt een uitvraag gedaan bij alle afdelingen om het register van verwerkingen waar nodig te actualiseren. Alle nodige gegevens zijn erin vermeld. Er is geen publieksversie beschikbaar. Dat zou wel de transparantie versterken en voor iedereen inzichtelijk maken voor welke doelen persoonsgegevens worden verwerkt door de gemeente. Er is op dit moment echter geen ruimte om daaraan tijd te besteden.

In het register ontbraken tot voor kort de werkprocessen van het RIEC (Regionaal informatie- en expertisecentrum, ondersteunt partners bij de aanpak van georganiseerde criminaliteit). Het RIEC is geen juridische entiteit, waardoor elk van de deelnemende partijen zelf verantwoordelijk is voor het eigen aandeel in de werkzaamheden. Die zijn praktisch gesproken niet uit te splitsen per partij, waardoor alle werkprocessen in de registers van alle deelnemers horen te worden opgenomen. Haarlem is de beheerorganisatie van het RIEC Noord-Holland en heeft daarom het voortouw genomen samen met de collega's van het RIEC om het register in te vullen. Het wordt beschikbaar gesteld aan de andere deelnemende partijen.

***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. Na een gesprek hierover en het uitwisselen van informatie heeft de AP in december 2019 laten weten een onderzoek in te stellen. Naar aanleiding daarvan heeft PI-Lab (een samenwerking van TNO, de universiteiten van Nijmegen en Tilburg en de stichting Internet Domeinregistratie Nederland) een advies geschreven hoe parkeerhandhaving aan de hand van het kenteken op een privacyvriendelijke manier kan worden ingericht. Dat advies is eind 2020 afgerond. In 2020 is er verder geen contact geweest met de AP over het onderzoek. Pas in oktober 2021 is het onderzoek weer opgepakt en is verzocht om aanvullende informatie. Die is verstrekt en sindsdien is er nog niets vernomen van de AP.

Aan de feitelijke manier van werken is ook nu nog niets aangepast. Er wordt inmiddels wel gezocht naar oplossingen van de gesignaleerde problemen. Dat zijn er drie:

1. Volgens de regeling bezoekersparkeren hebben bewoners die mantelzorg ontvangen recht op extra uren. Daarvoor wordt dus geregistreerd dat iemand mantelzorg ontvangt en dat is een bijzonder persoonsgegevens want het zegt iets over de gezondheid van de betrokkene. Voor het verwerken van bijzondere persoonsgegevens gelden extra strenge regels en er is discussie met de AP over de vraag of daaraan wordt voldaan in dit geval.
2. Een van de klagers is bang dat de gemeente aan de hand van het kenteken kan nagaan wie er op bezoek komt. In de werkprocessen moet daarom worden gewaarborgd dat dat niet zal gebeuren.
3. Een aanvraag om deel te nemen aan de regeling bezoekersparkeren wordt volledig geautomatiseerd behandeld. Dat is niet per se verboden maar er gelden wel bijzondere eisen, zoals transparantie en er moet een menselijke tussenkomst mogelijk zijn.

*Geautomatiseerde besluitvorming*
Omdat de geautomatiseerde besluitvorming in het bezoekersparkeren nog niet goed geregeld is en omdat de verwachting is dat er in de toekomst meer gebruik gemaakt zal worden van geautomatiseerde besluitvorming is de stadsadvocaat gevraagd een juridisch kader te schrijven voor geautomatiseerde besluitvorming. De regels omtrent geautomatiseerde besluitvorming gelden overigens ook voor het geautomatiseerd maken van risicoprofielen, zoals bijvoorbeeld heel in het klein gebeurt bij het proces rond meldingen van verhuizingen. Het juridisch kader zoals nu opgesteld, heeft nog een 'vertaling' nodig – het is nog wat te juridisch geformuleerd om algemeen bruikbaar te zijn – en kan dan worden gebruikt als toevoeging aan de standaardvragen bij het doen van een DPIA.

Het is een onderwerp dat naar verwachting vaker gaat spelen en waar de organisatie mee moet leren werken. Zeker waar het gaat om het werken met risicoprofielen (maar niet alleen daar) zullen daarbij ook ethische vragen aan de orde komen.

*Dataverzameling in de openbare ruimte*
Er is in 2020 veel te doen geweest over het voornemen van de binnenstadondernemers (BIZ) om informatie over bezoekersstromen te verzamelen via wifitracking. De gemeente was geen opdrachtgever voor deze aanpak maar was aanvankelijk wel van plan er een financiële bijdrage voor te verlenen. Nadat de wijkraden in de binnenstad meldden dat zij zich zorgen maakten over hun privacy, bleek dat de AP in Enschede een onderzoek deed naar precies dezelfde manier van werken. Dat was reden voor het college om de BIZ te vragen de uitkomst van dat onderzoek af te wachten of anders op en andere – privacyvriendelijke – manier gegevens te verzamelen. Na gesprekken met de BIZ, de wijkraden en de gemeenteraad heeft de BIZ uiteindelijk besloten tot dat laatste. In de raad is naar aanleiding van deze kwestie een eerste gesprek gevoerd over de vraag of in hoeverre de gemeente een rol heeft in het reguleren van dataverzameling in de openbare ruimte. Een technische sessie over dit onderwerp heeft na een aantal keren verschuiven uiteindelijk plaatsgevonden in maart 2022 en komt dit jaar ook terug op de agenda van college en raad.

*Privacy en security in de Jeugdzorg*
Op 29 september 2020 bleek er een gevoelig datalek te zijn bij één van de ketenpartners in het sociaal domein, Kenter Jeugdhulp. Een journalist bleek toegang te hebben tot vertrouwelijke gegevens van cliënten. Kenter heeft het lek daarna gedicht. Het viel uiteraard ook onder verantwoordelijkheid van Kenter maar raakt wel bewoners van de gemeente, aangezien sommigen van hen naar Kenter zijn doorverwezen. Naar aanleiding van dit incident hebben de CISO en FG de handen ineen geslagen met de collega's van Zaanstad, Haarlemmermeer en Amstelveen. Zonder een volledige audit te doen, zijn gesprekken gevoerd met een aantal (deels gemeenschappelijke) ketenpartners, groot en klein, over de stand van zaken rond informatiebeveiliging en privacy. Het doel was een beeld te krijgen van de stand van zaken, om zo realistische eisen te kunnen stellen bij de nieuwe verwervingsronde. Het beeld is dat alle partners het belang onderschrijven. Grotere organisaties zijn verder dan kleinere organisaties en grotere organisaties die zich nu aan het vormen zijn door samenwerking tussen kleinere organisaties zitten daar tussenin. Dat laatste hoeft geen probleem te zijn, als zij wel aan een aantal basismaatregelen voldoen.

| **Onderwerp** | **Groot, stabiel** | **Groot, consoliderend** | **Klein** |
|---|---|---|---|
| Informatiebeveiliging en Privacy staat op de agenda | Ja | Ja | Ja |

| | | | |
|---|---|---|---|
| NEN 7510 Certificering is een reële eis | Ja, binnen 2-3 jaar | Ja, is de ambitie | Nee |
| Basismaatregelen zijn geborgd | Ja | Onzeker | Wisselend |

*Datadiefstal bij de GGD*
Begin 2021 bleek dat er gegevens waren gelekt of eigenlijk gestolen uit de systemen van de GGD. Dit leidde niet verwonderlijk tot onrust en zorgen. Bij de gemeenten kwamen bijvoorbeeld vragen van bewoners die een nieuw burgerservicenummer wensten. Dat mag de gemeente niet geven. Wel is contact gezocht met koepelorganisaties als VNG en NVVB en met het rijk om ervoor te zorgen dat alle betrokken instanties met dezelfde boodschap antwoordden op de zorgen. GGD-GHOR heeft hierin het voortouw genomen.

Inmiddels heeft de stichting ICAM namens de gedupeerden het Rijk, de GGD-en en ook alle gemeenten aansprakelijk gesteld voor de geleden dan wel potentiële schade. Het is niet waarschijnlijk dat de gemeente hiervoor aansprakelijk is, aangezien het gaat om systemen die op landelijk niveau zijn aangeschaft en worden beheerd. Het is ook het Rijk dat de gesprekken voert met de stichting.

*Wet politiegegevens*
Als BOA's (buitengewoon opsporingsambtenaren) persoonsgegevens verwerken, valt dat sinds 2019 niet onder het regime van de AVG maar onder de Wet politiegegevens. Veel regels lopen min of meer parallel met de AVG maar niet alles. Meer dan de AVG is deze wet gericht op het op een zorgvuldige manier mogen delen van persoonsgegevens in het kader van politietaken. De afdelingen waar BOA's werken hebben hiervoor een implementatieplan gemaakt. Elk jaar hoort hierover een audit te worden uitgevoerd, en eens in de vier jaar moet dit door een externe partij gebeuren. De eerste externe audit zou in 2021 moeten zijn afgerond. De Autoriteit Persoonsgegevens heeft de deadline echter een jaar uitgesteld. De externe audit is in 2021 gestart met een nulmeting en wordt in 2022 afgerond.

*Toegangsrechten*
Als de gemeente persoonsgegevens verwerkt, is de eerste vraag die wordt beoordeeld of dat is toegestaan. Als dat zo is, betekent dat niet dat die gegevens vrijelijk in te zien zijn voor iedere medewerker. Er is een verfijning nodig door te bepalen wie binnen de organisatie dan toegang moet en mag hebben tot die gegevens. Op dat punt gaan geregeld dingen mis.

Ten eerste ontbreken op dit moment heldere spelregels over hoe je bepaalt wie toegang mag hebben. Daarbij beoordeel je voor welk doel de persoonsgegevens mogen worden gebruikt en wie daarin vanuit zijn functie of rol een taak heeft. Op sommige plekken gebeurt dit keurig maar niet overal. Ook wordt het niet altijd goed actueel gehouden. Dit raakt aan eigenaarschap van data, mensen (functies), processen en applicaties. Uitwerking van eigenaarschap is geprioriteerd, zoals terug is te lezen in de Informatienota informatiebeveiliging juni 2022 (bijlage 4 punt 1). Dit is de pilot zoals genoemd op pagina 2.

Een meer praktisch probleem is dat de manier waarop nu is georganiseerd dat alle toegangsrechten worden aangepast wanneer iemand een andere functie of een andere taak krijgt op dit moment niet waterdicht is. De betrokken applicatiebeheerders moeten na elkaar iets aanpassen – toegang geven of juist dichtzetten – maar daar kan gemakkelijk iets mis gaan. Als iemand vergeet de volgende applicatiebeheerder een seintje te geven, wordt dat meestal niet opgemerkt en stokt de verdere

actualisering van de toegangsrechten. Dit moet verder worden verbeterd. Ook dit punt is geprioriteerd, zie dezelfde bijlage 4 punt 4.

***Wat gebeurt er in de wereld om ons heen?***

- Het kabinet heeft aangekondigd toezicht te willen organiseren op het gebruik van algoritmes en dat te beleggen bij de AP. Het toezicht moet zich richten op de transparantie en het (verbod op) discriminatie en willekeur. Ook moet de overheid een register gaan bijhouden van de gebruikte algoritmes. Staatssecretaris Van Huffelen (digitalisering) heeft een uitwerking van deze punten aangekondigd voor juni 2022. Deze is op het moment van schrijven nog niet beschikbaar.
- Voor steeds meer toepassingen wordt gebruik gemaakt van een 'cloud' om gegevens te bewaren. Data staan dan niet meer op de eigen servers maar op servers van techbedrijven. Dat kunnen ook persoonsgegevens van burgers tussen zitten en die moeten veilig zijn. Zeker als de cloud zich bevindt op grondgebied waar de AVG niet van toepassing is, zijn daar risico's aan verbonden. De toezichthouders van de lidstaten van de EU doen dit jaar onderzoek naar het gebruik van clouddiensten door overheden. Als gevoelige gegevens in een cloud buiten het AVG-gebied worden bewaard, moet een zogeheten DTIA worden gedaan (data transfer impact assessment) om de risico's te beoordelen.
- Er zijn verschillende nieuwe wetten op komst: de Wet aanpak meervoudige problematiek in het sociaal domein moet een grondslag creëren voor het delen van data in het sociaal domein. De Wet gegevensverwerking door samenwerkingsverbanden beoogt iets soortgelijks maar is meer gericht op het veiligheidsdomein. Beide wetsvoorstellen zijn nog in behandeling.
- Op 1 mei 2022 is de Wet Open overheid in werking getreden, de opvolger van de Wet openbaarheid van bestuur. Doel is de transparantie van de overheid te versterken door op steeds meer gebieden niet alleen op aanvraag maar proactief overheidsinformatie te publiceren. Dit wordt in fases verplicht voor verschillende informatiecategorieën. Dat vraagt een verbetering in de informatiehuishouding. Dit komt ook ten goede van bescherming van persoonsgegevens. Een goede ordening en archivering van gegevens is immers voorwaarde om vertrouwelijkheid (privacy), beschikbaarheid (zonder data en systemen stopt alles) en integriteit (kloppende data voor de juiste besluiten) te kunnen garanderen. Ze zijn ook nodig om op een toegankelijke manier transparant te zijn.

***Conclusie***

De gemeente verwerkt enorm veel persoonsgegevens van met name haar bewoners maar ook van medewerkers en soms van andere personen. Alle betrokkenen moeten erop kunnen rekenen dat hun gegevens bij de overheid in veilige handen zijn. De alsmaar verder groeiende digitalisering zorgt immers niet alleen voor gemak en efficiency maar tegelijk ook voor grotere privacyrisico's. Hoe meer gegevens, hoe groter de kans dat er iets mis gaat. Kopiëren en verspreiden van gegevens gaat digitaal bovendien een stuk sneller en gemakkelijker dan op papier. De basisidee in de AVG is dat iedereen zoveel mogelijk zelf de controle houdt over wat er gebeurt met zijn of haar gegevens. Tegelijk ben je voor verschillende zaken verplicht gegevens te verstrekken aan de gemeente. Daarmee is de gemeente verantwoordelijk voor een zorgvuldige omgang met die gegevens. Om die verantwoordelijkheid waar te maken, is het nodig gegevens vertrouwelijk en geordend (vindbaar en correct) te houden en de risico's te herkennen en zoveel mogelijk weg te nemen.

Er zit zeker een stijgende lijn in de kennis en alertheid en daarmee in de veiligheid van de gegevens. Tegelijk is de constatering dat de organisatie nu veelal blijft hangen op hetzelfde niveau en dat kennis en zorgvuldig werken nog te weinig zijn geborgd in voor iedereen toegankelijke kennis en in

standaarden. Privacybescherming krijgt niet op alle onderdelen de gewenste prioriteit en er zijn te weinig adviseurs beschikbaar, op centraal niveau en in de meeste lijnafdelingen. Dat remt het in gang zetten van organisatiebrede verbeteringen en versterken van de kennis. De risico's die hierdoor ontstaan, zijn vooral voor rekening van bewoners en andere betrokkenen. Om te voldoen aan hun terechte verwachtingen en om te voldoen aan de wet is meer inzet nodig.