Functionaris voor de gegevensbescherming Jaarrapportage AVG Drechtsteden 2021

Periode april tot en met december 2021

Gemeenschappelijke Regeling Drechtsteden
Colleges van de gemeenten Alblasserdam, Dordrecht, Hardinxveld-Giessendam, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht en Zwijndrecht
Burgemeester van Dordrecht en Papendrecht
Gemeenschappelijke Regeling Omgevingsdienst Zuid-Holland Zuid

Inhoud

Inleiding

Dit jaar ziet de FG jaarrapportage er anders uit dan de afgelopen jaren. Redenen hiervoor zijn dat de organisaties de behoefte hebben geuit dat de jaarrapportage aansluit op het kalenderjaar, en daarmee op de P&C cyclus van de gemeenten. Daarnaast vormt deze rapportage de afsluiting van de transitieperiode. De Gemeenschappelijke Regeling Drechtsteden (GRD) bestaat sinds 1 januari 2022 niet langer in de vorm zoals we die kenden: de Drechtraad is opgeheven en de organisatieonderdelen BDR en Regiogriffie bestaan niet meer. Taken op het gebied van bedrijfsvoering en belastingen zijn overgenomen door de gemeente Dordrecht, die voortaan optreedt als Servicegemeente voor de gemeenten en hun gemeenschappelijke regelingen. De gemeenschappelijke regeling is voortgezet als collegeregeling GR Sociaal voor het onderdeel SDD. Mede ter afsluiting van deze transitie heeft deze rapportage betrekking op de laatste 9 maanden van het kalenderjaar 2021.

De bestuurlijke en organisatorische wijzigingen die voortvloeien uit de transitie hebben ook (grote) gevolgen voor de naleving van de privacywetgeving. Daarom besteden we in deze rapportage de nodige aandacht aan de verhoudingen in de Drechtsteden op het gebied van gegevensbescherming en staan we stil bij de vraag of de verschillende bestuursorganen deze gevolgen onderkenden en daar voldoende rekening mee hielden.

Daarnaast gaan we in de rapportage in op een deel van de periodiek terugkerende AVG-onderwerpen en staan we stil bij eerdere aandachtspunten.

De Autoriteit Persoonsgegevens (landelijke toezichthouder) heeft het laatste jaar ook niet stilgezeten, vooral op het gebied van normuitleg, positionering van de FG en handhaving.[1] Vooral de verschillende boetebesluiten vallen op, waaronder de eerste boete voor een gemeentelijke overheid. Uit deze besluiten blijkt duidelijk welke zaken bestuursorganen (extra) worden aangerekend bij overtreding van de privacywetgeving. Ook wordt duidelijk hoe de AP de rol van bestuursorganen ziet, bijvoorbeeld bij het bepalen van verwerkingsverantwoordelijkheid, het volgen van een DPIA-procedure en het betrekken van de FG. Op enkele van deze zaken zullen wij nader ingaan.

<u>Aanpak</u>
In maart en april is informatie opgevraagd bij de gemeente Dordrecht (als Servicegemeente), GR Sociaal en OZHZ. Het betreft informatie over:

- Het verwerkingsregister en besluitvorming over eventuele mutaties,
- (Besluitvorming over) verwerkersovereenkomsten en/of gezamenlijke verwerkingsverantwoordelijkheid.

Daarnaast is de aanpak mondeling toegelicht tijdens het regionale overleg van de privacy-coördinatoren van 12 april 2022.

Verder is bij de gemeente Dordrecht (Servicegemeente) nog aanvullend informatie opgevraagd over datalekken en de deelname van de medewerkers aan de e-learning. Daarnaast is informatie opgevraagd bij de colleges waar het oude privacybeleid (uit 2018) nog op de website stond. Dit waren de colleges van Alblasserdam, Hendrik-Ido-Ambacht, Sliedrecht en Zwijndrecht.

De opgevraagde informatie is ontvangen.

De conceptrapportage is op 24 juni 2022 aangeboden aan de secretarissen, privacy coördinatoren en de adviseurs gegevensbescherming. Tijdens het ONS-D van 7 juli 2022, waaraan ook OZHZ en GRS deelnamen, stond de conceptrapportage voor wederhoor op de agenda. Daarnaast konden de

[1] Als Nederlandse toezichthouder, maar ook als lid van de Europese Data Protection Board (EDPB, voorheen WP29).

secretarissen tot uiterlijk 10 juli 2022 nog inhoudelijke opmerkingen op het concept maken. Van deze mogelijkheid is geen gebruik gemaakt. Op 13 juli 2022 is de rapportage, met enkele ondergeschikte wijzigingen, definitief gemaakt en via de secretarissen aan hun bestuur aangeboden.

De verhoudingen tussen de bestuursorganen in de Drechtsteden/ verantwoordelijkheden

In het rapportagejaar 2021 was er binnen de Drechtsteden sprake van een vergaande samenwerking op verschillende taakvelden. Zo werkten de 7 Drechtstedengemeenten onder meer samen in de GRD en in OZHZ. Binnen OZHZ nemen daarnaast nog 3 andere gemeenten deel, en ook de provincie is hier onderdeel van.

Grip op omgang met persoonsgegevens is waar het in de AVG om gaat. Het kernbegrip daarbij is 'verwerkingsverantwoordelijkheid'. Die rust op het orgaan dat de (eind)verantwoordelijkheid heeft om te laten zien dat (en hoe) de AVG wordt nageleefd. Waarbij het de verantwoordelijke vrijstaat om (deel)taken te beleggen bij een derde (verwerker of een medeverantwoordelijke; voor beide gevallen heeft de AVG verschillende verplichtingen opgenomen). Zo moet de verwerkingsverantwoordelijke zich ervan vergewissen dat hij (ook via de derde partij) nog steeds alle AVG-verplichtingen kan naleven en dat de bescherming van de rechten van de betrokkene is geborgd. De verantwoordelijke moet dus echt zijn verantwoordelijkheid nemen en de juiste afspraken maken. Dit moet zowel in de praktijk als op papier kloppen. Is dat niet het geval, dan zijn zowel de verantwoordelijke als de verwerker in overtreding. De gemeenten hebben zichzelf verplicht om in de relatie verantwoordelijke- verwerker de standaardverwerkersovereenkomst van de VNG te gebruiken.

Twee factoren hebben ingrijpende gevolgen voor de relatie verantwoordelijke – verwerker in de Drechtsteden.

1. Richtsnoeren EDPB

De eerste vloeit voort uit Europese ontwikkelingen. In de geüpdatete richtsnoeren 07/2020 bevestigt de EDPB in juli 2021 dat het begrip verwerkingsverantwoordelijke ruim uitgelegd moet worden.[2] Ook Nederlandse jurisprudentie wijst hierop.[3] Kern is dat feitelijke invloed, bijvoorbeeld als opdrachtgever, leidt tot de conclusie dat er sprake is van verwerkingsverantwoordelijkheid. Concreet betekent dit dat een college als opdrachtgever in een gemeenschappelijke regeling altijd (minimaal) óók verwerkingsverantwoordelijke blijft. De opdrachtgever is immers de eerste partij die doel en middelen vaststelt, namelijk door te bepalen dat een taak belegd wordt bij een GR. Dit geldt zeker wanneer het gaat om door de wet(gever) toegekende taken aan bestuursorganen. De wet(gever) heeft daarmee het bestuursorgaan tot verantwoordelijke gemaakt.

2. Transitie

De tweede factor is de transitie in de Drechtsteden. Onderdeel hiervan is dat de gemeenten 'meer regie' nemen. Dat betekent dat bestaande relaties van verantwoordelijke - verwerker (kunnen) wijzigen en de gevolgen daarvan voorbereid (hadden) moeten worden.

Naar het oordeel van de FG's hadden deze ontwikkelingen redenen moeten zijn om in 2021 uitdrukkelijk aandacht te besteden aan het op orde hebben van de basis en het nemen van voorbereidende besluiten om ervoor te zorgen dat (in ieder geval) per 1 januari 2022 inzichtelijk was wie nu precies waarvoor verantwoordelijk is en hoe partijen zich tot elkaar verhouden. Voor inwoners moet het immers duidelijk

[2] In Richtsnoeren EDPB 07/2020 (aangenomen in juli 2021) over de begrippen verwerkingsverantwoordelijke en verwerker.
[3] Bijvoorbeeld Rb. Rotterdam 19 maart 2021, ECLI:NL:RBROT:2021:2306.

zijn bij wie zij terechtkunnen met vragen over hun persoonsgegevens, en bij wie zij hun rechten kunnen uitoefenen.

Op verschillende momenten hebben wij het belang hiervan benadrukt, onder andere via de verschillende adviseurs en bij de (toenmalige) directeur van de GRD. Helaas moeten wij constateren dat de colleges, en burgemeesters, zowel over de rapportageperiode als per transitiedatum 1 januari 2022 niet voldoen aan de wettelijke verplichting om inzicht te hebben in de AVG-verhoudingen in de Drechtsteden en daartoe de benodigde afspraken te maken en de overige verplichtingen na te komen (bijvoorbeeld transparantieplicht). Voor zover ons bekend zijn geen DPIA's uitgevoerd die gericht waren op de wijzigingen van de verwerkingen als gevolg van de transitie en de daarmee gepaard gaande risico's voor omgang met persoonsgegevens. Ons is (slechts) bekend dat OZHZ (overigens los van de transitie) tijdens de rapportageperiode actief aan de slag is gegaan om hun rol onder de AVG beter in beeld te krijgen. Dit naar aanleiding van eerdere FG-aanbevelingen en de geüpdatete richtsnoeren.

Het gegeven dat de organisaties in de Drechtsteden een begin maakten met het afsluiten van verwerkersovereenkomsten doet aan bovenstaande niet af. Het afsluiten van een overeenkomst kan een passende maatregel zijn om een risico te mitigeren. Hieraan gaat echter een analyse vooraf. Nu deze analyse ontbreekt roept dit de vraag op welke waarde zo'n overeenkomst heeft.

De FG's achten het zorgelijk dat de verhoudingen met betrekking tot de nieuwe dienstverlening die de gemeente Dordrecht gaat leveren niet voldoende is beschreven. Maar ook de dienstverlening op het gebied van burgerzaken, die in het verleden ook al door Dordrecht werd verleend (Dienstverlening Drechtsteden), is al jaren niet (op de juiste wijze) beschreven en de juiste afspraken zijn hierover niet gemaakt.

Hetzelfde geldt voor de dienstverlening die tot 1 januari 2022 door de GRD aan de deelnemers en OZHZ werd geleverd. Er was een begin gemaakt met het afsluiten van verwerkingsovereenkomsten voor de dienstverlening van het onderdeel SCD. Voor de overige (GRD-)onderdelen zijn de verhoudingen niet in kaart gebracht en vastgelegd, en zijn de bijbehorende afspraken niet gemaakt.

Speciaal aandachtspunt zijn ook de werkzaamheden die per 1 januari 2022 vanuit GR Sociaal uitgevoerd worden. In het jaar 2021 was de SDD nog een onderdeel van de GRD. Per 1 januari 2022 is GRS een zelfstandig openbaar lichaam geworden. Toepassing van de geüpdatete richtsnoeren betekent, naar verwachting, dat het bestuur van GRS (in ieder geval niet in zijn eentje) als verwerkingsverantwoordelijke kan worden aangemerkt als het gaat om het uitvoeren van taken die bij wet aan de bestuursorganen van de gemeenten zijn toebedeeld. Zoals bijvoorbeeld het verstrekken van bijstand of het toekennen van maatwerk Wmo. Dus ook niet als taakuitoefening door het gemeentebestuur (aan dit GRS-bestuur) gedelegeerd is. Dit werkt onder meer door in besluitvorming over DPIA's, rechten van betrokkenen en de meldplicht datalekken. Voor de uitvoering van de werkgeverstaken en bedrijfsvoeringstaken is GRS per 1 januari 2022 verantwoordelijke geworden. Naar het oordeel van de FG's hebben GRD en de gemeenten niet voldoende onderkend wat de gevolgen zijn van deze gewijzigde verhoudingen. Zo zijn er bijvoorbeeld geen DPIA's opgesteld en is er geen wijziging van het privacybeleid voorbereid.

Ook de rol van het college van Dordrecht wordt een bijzondere. Vanuit het nieuwe onderdeel Servicegemeente worden een aantal taken op het gebied van bedrijfsvoering voortaan feitelijk uitgevoerd door het college van Dordrecht. Ten opzichte van de andere colleges zal dit voor de meeste verwerkingen tot gevolg hebben dat Dordrecht hun verwerker wordt. Maar wat betekent dit voor taken die Dordrecht zelf in mandaat laat uitvoeren door de GR OZHZ of GR Sociaal? Zij worden (mogelijk) verwerker voor Dordrecht. Terwijl zij hun IT bijvoorbeeld weer afnemen van Dordrecht. Wordt Dordrecht daarmee (sub)verwerker van zichzelf? In hoeverre past een dergelijke constructie bij de AVG? Wat betekent dit voor de te stellen eisen en te treffen waarborgen aan een verwerker? En voor welke verwerkingen moet Dordrecht niet als verwerker maar als (mede) verantwoordelijke worden aangemerkt?

Tot slot: wat betekent dit voor de taken die OZHZ en GRS als verwerkers uitvoeren voor de overige gemeenten? Die op hun beurt weer gebruik maken van de diensten van (de servicegemeente) Dordrecht als subverwerker? Staan GRS en OZHZ dan jegens de gemeenten in voor die dienstverlening van de subverwerker Dordrecht zoals dit volgens de AVG zou moeten? Dit had voorafgaand aan de transitie, tijdens het rapportagejaar volledig in kaart moeten worden gebracht, en de bijbehorende overeenkomsten/ afspraken hadden moeten worden afgesloten.

Conclusie
De verhoudingen tussen de verschillende bestuursorganen en de gevolgen daarvan zijn nog niet voldoende in kaart gebracht. Dit is expliciet in strijd met de AVG en dit werkt door in allerlei onderdelen van naleving (zie verderop in deze rapportage). Dit geldt zowel voor de oude situatie als voor de situatie vanaf 1 januari 2022.

Aanbeveling:
Breng de verhoudingen tussen de verschillende bestuursorganen in de regio zorgvuldig in kaart voor de verschillende verwerkingen. Beoordeel deze verhoudingen aan de hand van de richtlijnen die de EDPB over processor en controller heeft opgesteld. Let op dat dit per verwerking kan verschillen. Sluit daarna de benodigde overeenkomsten af en stuur op naleving.

Privacybeleid

In het jaar 2020 bereidden de Drechtstedenorganisaties een nieuw privacybeleid voor. De meeste organen stelden dit ook vast en publiceerden dit op hun website. Wij stelden vast dat een aantal organisaties nog het Privacybeleid 2018 op de website heeft staan. Dit betreft Hendrik-Ido-Ambacht, Sliedrecht en Zwijndrecht. Aan deze colleges zijn de volgende vragen gesteld:

1. Betreft dit het laatst vastgestelde beleid?
2. Zo ja, waarom is het beleid 2020 niet vastgesteld?
3. Indien er later wel beleid is vastgesteld:
   a) wanneer is het beleid vastgesteld, door wie? En wanneer is het bekendgemaakt?
   b) Waarom staat (de verwijzing naar) het verouderde beleid nog op de site?

Door het college van Sliedrecht is het beleid 2020 nog niet vastgesteld. Dit staat op de planning voor 2022, zo is ons desgevraagde medegedeeld. Hetzelfde geldt voor het college van Zwijndrecht. Door het college van Alblasserdam en Hendrik- Ido-Ambacht was het beleid 2020 wel vastgesteld maar niet bekendgemaakt. Dit is in 2022 alsnog gebeurd.

Aanbeveling:
Met de transitie per 1 januari 2022 achten we het huidige privacybeleid niet langer relevant. Dit gaat immers uit van een omvangrijke GRD en die situatie veranderde per 2022. Om die reden bevelen wij aan het privacybeleid, zowel inhoudelijk als kwalitatief te herijken. Ook hier geldt weer dat deze herijking eigenlijk al had moeten plaatsvinden tijdens de rapportage-/ transitieperiode zodat per 1 januari 2022 een juist en actueel privacybeleid gold.

Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten vormt het hart van omgang met persoonsgegevens. Dit helpt de betrokken organisaties om te sturen op AVG-naleving en zo meer grip te krijgen op de verwerkingen van persoonsgegevens. Door dat overzicht is het makkelijker om te controleren of er op de juiste manier met persoonsgegevens wordt omgegaan en of de verwerkingen rechtmatig zijn. Ook kunnen mogelijke risico's voor betrokkenen of de organisatie eenvoudiger worden gedetecteerd.

De AVG kent 2 soorten verwerkingsregisters: een verwerkingsregister voor (mede)verwerkingsverantwoordelijken en een register voor verwerkers.

De verwerkingsregisters van de gemeenten en de GRD waren tijdens het rapportagejaar in beheer bij het GRD-bestuur (via hun recordmanager.SCD) en zijn opgenomen in de i-Navigator. De Sociale Dienst Drechtsteden (onderdeel van GRD) en OZHZ hebben een eigen verwerkingsregister.

OZHZ heeft aangegeven dat een deel van dit register in 2021 is geactualiseerd. Verwerkingen die niet meer worden uitgevoerd zijn verwijderd, en er zijn verwerkingen toegevoegd of de informatie die over verwerkingen is opgenomen is aangevuld. Daarnaast is/wordt de opzet van het verwerkingenregister gewijzigd naar het format van het verwerkingenregister van de AP. Dit heeft deels in 2021 al plaatsgevonden. De rest volgt na inwerkingtreding van de Omgevingswet, zo begrepen wij van OZHZ.

Het verwerkingsregister is een belangrijk instrument om te sturen op AVG-naleving. Vanuit dat oogpunt wekt het verbazing dat binnen 1 organisatie (GRD) één onderdeel (SDD) een eigen register had. Naar het oordeel van de FG's maakte dit het erg lastig voor het bestuur en het MT van GRD om te sturen. Al was het maar omdat de i-Navigator alle gemeentelijke processen bevat (en dus ook de taken die in het eigen register van GRD/SDD staan). Op onderdelen verwijst i-Navigator dan ook naar Mavim. De structuur van Mavim voldeed tijdens de onderzochte periode niet aan de inhoudelijke eisen die de AVG aan een verwerkingsregister stelt. Per 1 januari 2022 wordt SDD (in GRS) een zelfstandige organisatie met een eigen bedrijfsvoering. Het register zal dan inhoudelijk moeten voldoen aan de eisen die de AVG stelt.

Uit onderzoek blijkt dat uit i-Navigator niet (direct) duidelijk is welk bestuursorgaan verwerkingsverantwoordelijke is: het veld verwerkingsverantwoordelijke is niet ingevuld. Wel bevat de i-Navigator meer taken dan alleen die van het college. Ook taken van de burgemeester en van de gemeenteraad zijn erin opgenomen. Op dit punt is het register dus niet volledig. Daarnaast blijkt uit het register niet met welke (categorieën) ontvangers gegevens worden gedeeld. De AVG verplicht hier wel toe.

Globaal onderzoek naar de manier waarop enkele (relatief) nieuwe taken beschreven zijn wijst uit dat het verwerkingsregister voor de colleges niet juist, volledig en actueel is. Zo zijn bijvoorbeeld de gegevens vanuit het proces vroegsignalering schuldhulpverlening niet actueel en niet compleet.

Verder zijn de verwerkingsregisters niet voldoende aangepast aan de situatie waarin sprake is van de verhouding verantwoordelijke-verwerker. Het is in het verwerkingsregister bijvoorbeeld niet inzichtelijk wanneer en voor wie bijvoorbeeld Dordrecht als verwerker optreedt voor de verschillende verantwoordelijke colleges en wanneer als verantwoordelijke. Bijvoorbeeld de verwerkingen die Dienstverlening Drechtsteden voor de verschillende colleges uitvoert. Hetzelfde geldt in ieder geval ook voor de verwerkingen die door de GRD-onderdelen en OZHZ als verwerker (of mede-verwerkingsverantwoordelijke?) voor de colleges worden uitgevoerd.

Desgevraagd is van de recordmanager de volgende informatie ontvangen: "*vanuit de servicegemeente zijn de processen wel doorlopen en zijn er aanpassingen in het register van verwerkingsactiviteiten gedaan. Vanuit de gemeenten is geen enkele aanpassing in het register van verwerkingen doorgegeven.*" Dat terwijl reeds bij de vorige FG rapportage (die betrekking had op de periode van 1 april 2020 tot 1 april 2021) al bij alle gemeenten werd geconstateerd dat het register niet juist en actueel was.

Overheidsorganisaties zijn verplicht ervoor te zorgen dat informatie geordend en toegankelijk is. Dit geldt ook voor informatie in het verwerkingsregister i-Navigator. Koppeling met het zaaksysteem In Proces biedt waarborgen op het gebied van dataminimalisatie en informatiebeveiliging. Uit onderzoek blijkt dat deze koppeling niet altijd gemaakt wordt. Het register vermeldt dan dat de verwerking "niet live" is in In Proces. Dit vinden de FG's zorgelijk omdat daarmee bijvoorbeeld niet duidelijk is of, en zo ja hoe, wordt geborgd dat niet méér informatie wordt verwerkt dan nodig of welke IB-maatregelen zijn getroffen om de beschikbaarheid, integriteit en vertrouwelijkheid te borgen. Ook betekent het dat de opgenomen informatie die over de verwerking is opgenomen in het register mogelijk onjuist is, omdat daarbij wordt uitgegaan van de inrichting in In Proces.

Bits of Freedom

Vanwege het belang van het verwerkingsregister willen wij op deze plaats ook stilstaan bij het rapport van Bits of Freedom. Op 24 mei 2022 is het onderzoeksrapport "De staat van privacy bij gemeenten" gepubliceerd. Ook in dit onderzoek werd de conclusie getrokken dat de basis bij gemeenten te vaak niet op orde is. Bits of Freedom doet daarbij aan gemeenten op dit punt een aantal aanbevelingen. De FG's herkennen deze punten en sluiten zich hierbij aan.

Aanbevelingen:

- Prioriteer het vullen en actueel houden van het verwerkingsregister. Zie dit niet als een eenmalige klus, maar als een doorlopend proces waarbij kritisch gekeken wordt naar welke verwerkingen nog noodzakelijk en rechtmatig zijn, en welke verwerkingen gestopt kunnen worden.
- Publiceer het verwerkingsregister op de website. Dit is weliswaar geen verplichting vanuit de AVG, maar het biedt wel transparantie (zie ook onder kopje betrokkenen).
- Verwerk geen gegevens op een manier die niet te verantwoorden is, bijvoorbeeld door algoritmen geautomatiseerde beslissingen te laten maken die niet transparant en motiveerbaar zijn. Houd ten alle tijden de algemene beginselen van behoorlijk bestuur voor ogen.
- Zorg ervoor dat in beeld wordt gebracht met welke partijen samenwerkingen zijn aangegaan en vanuit welke hoedanigheid en bevoegdheid. Is er sprake van (gedeelde) verwerkingsverantwoordelijkheid of van een verwerker? Documenteer de daarbij behorende overeenkomsten centraal.
- Begin niet aan ‘datagedreven werken’ met behulp van nieuwe technologieën en datatoepassingen zoals big data en algoritmen als de basis niet op orde is.

Een extra punt van aandacht hierbij is ook bijvoorbeeld de geplande migratie naar de cloud. Hoe kan dit zorgvuldig plaatsvinden als het verwerkingsregister niet op orde is en de verhoudingen tussen de verschillende bestuursorganen nog onduidelijk zijn?

DPIA's

DPIA's zijn een belangrijk instrument om vooraf de privacy risico's van een bepaalde verwerking of proces van verwerkingen in beeld te brengen, en daar vervolgens maatregelen op te nemen. DPIA's zijn wettelijk verplicht in verschillende gevallen. Voor de gemeentelijke bestuursorganen geldt al snel een DPIA

verplichting. De verhouding tussen overheid en burger is immers geen vrije verhouding (maar een afhankelijkheidsrelatie waarbij de burger niet kan kiezen met welke overheid hij zaken wil doen) Ook vinden er veel verwerkingen plaats met gevoelige of bijzondere persoonsgegevens. Daarnaast worden de gegevens binnen de Drechtsteden regelmatig verwerkt binnen de Drechtstedelijke samenwerkingsverbanden. We zien dat de bestuursorganen die verplichtingen, inclusief de uitgangspunten die daaraan ten grondslag liggen niet kennen en niet voldoende onderkennen. Met name het accepteren van de "kwetsbaarheid" van de burger die door de Autoriteit Persoonsgegevens expliciet wordt gemaakt. Maar ook het niet (h)erkennen van gevoelige persoonsgegevens bijvoorbeeld wanneer gegevens worden verwerkt van groepen burgers met een bepaald inkomen.

Daarbij maken we onderscheid tussen twee verschillende typen DPIA's: allereerst de effectbeoordeling die voorafgaat aan de invoering van een nieuwe of gewijzigde verwerking (nieuwe taak, nieuwe applicatie, nieuwe aanbieder, etc.). En een periodieke toets om te beoordelen of (nog) conform de eerder uitgevoerde DPIA wordt gewerkt. Zo beveelt de AP aan om minimaal eens per 3 jaar zo'n periodieke DPIA uit te voeren. Gelet op de inwerkingtreding van de AVG in mei 2018 betekent dit dat alle oudere/ bestaande verwerkingen minimaal 2x beoordeeld horen te zijn op AVG-conformiteit. De uitkomst van de DPIA dient te worden verwerkt in het verwerkingsregister.

Bovenstaande veronderstelt dat in het rapportagejaar een aanzienlijk aantal DPIA's is gedaan en daarover FG-adviezen zijn gevraagd. Dit wijkt sterk af van de werkelijkheid. Door een aantal verantwoordelijken is tijdens deze periode helemaal geen FG-advies gevraagd (en ook geen enkele DPIA opgesteld). Vanuit GRD/SDD is eenmaal een periodieke DPIA voor FG-advies aangeboden (maar dit leidde -nog- niet tot een DPIA-besluit). Verder werden DPIA's uitgevoerd op nieuwe of gewijzigde verwerkingen op een moment dat er eigenlijk al geen aanpassing meer mogelijk is (camera's al aangeschaft, aanbesteding al gegund, contracten met verwerker/uitvoerende partij al gesloten, verwerking al gestart). Dit is veelal onrechtmatig en inefficiënt en dit roept de vraag op in hoeverre de waarde van het DPIA-proces en het bijbehorende FG-advies wordt (h)erkend.

Tot slot wijzen wij er hier op dat in de vorige FG-rapportage expliciet een aantal DPIA's zijn benoemd: invoering Wet verplichte ggz per 1 januari 2020, thuiswerken, HR AFAS, etc.). Ondanks het -nog steeds- ontbreken van deze DPIA's vinden deze verwerkingen wel plaats, zo is ons gebleken. Deze ontwikkeling baart ons als FG's de nodige zorgen.

Daarnaast zijn er twee punten die opvallen bij de DPIA's die wel voor FG-advies zijn aangeboden. Allereerst valt op dat bevoegdheidsgebreken regelmatig voorkomen. Het gaat dan om situaties waarin niet duidelijk is op welke grond het betreffende overheidsorgaan bevoegd is de beoogde verwerking uit te voeren. Soms is dit omdat de bevoegdheid niet juist is benoemd. Maar vaker is dit omdat de bevoegdheid ontbreekt. Dit is zorgelijk. Overheidsorganen ontlenen hun bestaansrecht en bevoegdheden aan de wet. Inwoners moeten erop kunnen vertrouwen dat de overheid de wet naleeft. Het is zorgelijk als de overheid zelf niet weet op basis van welke wetgeving hij de bevoegdheden heeft en hoever die bevoegdheden gaan. Nog zorgelijker is het wanneer de overheid zich bewust buiten die bevoegdheden begeeft. In de DPIA's zien we beide varianten bestaan.

Het tweede punt dat we willen benoemen is de DPIA-besluitvorming. Een DPIA is een systematische beoordeling van effecten op gegevensverwerking. Bij de hoge risico's die aan een voorgenomen verwerking (lijken te) kleven is het verplicht de DPIA-procedure te doorlopen. Daarbij hoort dat de risico's in kaart gebracht worden (en waar mogelijk gemitigeerd) en dat de FG wordt gevraagd te adviseren over de juistheid van deze beoordeling. Met het advies van de FG wordt beslist óf en zo ja op welke wijze de voorgenomen verwerking uitgevoerd zal gaan worden. Kortom het gaat om het (deel)beleid dat de verwerkingsverantwoordelijke wenst te voeren en hoe daartoe processen worden ingericht en/of (deels) extern worden belegd.

In de praktijk merken wij dat het besluit doorgaans ontbreekt en dat de DPIA eindigt met het FG-advies. Dit is onvolledig. Daarnaast valt op dat risico's niet op juiste waarde worden geschat. Daarmee bedoelen we dat ambtelijk wordt geoordeeld dat risico's (bijvoorbeeld over buitenwettelijk handelen) geaccepteerd worden. Dit is niet het juiste niveau. Immers, een ambtenaar kan slechts mandaat hebben om 'binnen' een bevoegdheid te handelen. Bij het ontbreken van een bevoegdheid kan een ambtenaar derhalve nooit bevoegd zijn.

Ook constateren we dat de bestuursorganen bij hoge restrisico's niet bereid zijn om daarbij het wettelijk voorgeschreven proces te doorlopen (vragen om voorafgaande goedkeuring bij de Autoriteit Persoonsgegevens).

Het afwijken van FG advies dient gemotiveerd en gedocumenteerd te worden. Beide punten zien wij binnen de Drechtsteden doorgaans niet terug.

Aanbevelingen:

1. Inventariseer voor welke (bestaande) processen een DPIA moet worden gehouden, en op welke termijn die zal plaatsvinden. Geef daarbij voorrang aan verwerkingen met hoge risico's voor omgang met persoonsgegevens.
2. Onderken dat een nieuwe of gewijzigde verwerking pas mag starten als de DPIA-besluitvorming hierover is afgerond (inclusief voorafgaande raadpleging bij de AP als dat nodig is). Als gestuurd wordt op een beoogde ingangsdatum voor de nieuwe verwerking, dan betekent dit dat tijdig gestart moet worden met de DPIA-procedure.
3. Zorg voor voldoende kennis en capaciteit om de DPIA's te kunnen uitvoeren.
4. Betrek de FG tijdig en win tussentijds FG-(deel)advies in.

Betrokkenen

Onder de AVG draait het om de betrokkenen. Het zijn immers hun persoonsgegevens die verwerkt worden. Overheidsorganen mogen voor hun wettelijke taken, voor zover die wet dit toestaat, persoonsgegevens verwerken. Maar moeten er wel voor zorgen dat betrokkenen dit (kunnen) weten en dat zij dit kunnen controleren en hierover, waar nodig, ook hun beklag kunnen doen. Dit komt tot uitdrukking in drie verschillende onderdelen: een informatieplicht (transparantie), de rechten van de betrokkenen en de klachtenprocedure.

Verschillende gebeurtenissen, zoals de toeslagenaffaire, bevestigen hoe belangrijk het is dat overheidsorganen dit erkennen. Voor ons als FG is dit reden om hiernaar een kwalitatief onderzoek te doen (planning 2023). De organisaties kunnen het jaar 2022 gebruiken om, op basis van de juiste toedeling van verantwoordelijkheden (zie kopje verhoudingen in de Drechtsteden) hun beleid ten aanzien van de betrokkenen te herijken.

In deze rapportage staan we stil bij een aantal aspecten.

<u>Informatieplicht/transparantie</u>
Om te kunnen controleren of overheidsorganen netjes omgaan met persoonsgegevens moet eerst duidelijk zijn dát persoonsgegevens worden verwerkt. De AVG verplicht organisaties hierover transparant te zijn en om hierover 'beknopt, transparant, in begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal' te communiceren. In de Drechtsteden is ervoor gekozen hiervoor een privacyverklaring op te nemen op de eigen website. Uit onderzoek blijkt dat alle organisaties tijdens de rapportageperiode beschikten over een privacyverklaring.

Inhoudelijk valt op dat deze verklaringen erg summier zijn. In die zin dat een inwoner, na het lezen van de privacyverklaring, zich er veelal niet van bewust zal zijn dat persoonsgegevens bijvoorbeeld worden verwerkt in het kader van cameratoezicht, het ontwikkelen van nieuw beleid, het maken van data-analyses, het gebruiken van een afvalpas of bodycams. Dit zijn wel zaken die doorgaans door inwoners als ingrijpend worden ervaren. Naar het oordeel van de FG's doen de organisaties er goed aan de verklaringen zo op te stellen dat inwoners ook kunnen begrijpen waarom hun gegevens verwerkt worden. Een gelaagde privacyverklaring is aan te bevelen. Dit wordt overigens ook aanbevolen door de EDPB.

In het verlengde hiervan verdient het wellicht aanbeveling om de (geïnteresseerde) lezer in staat te stellen een extract van het verwerkingsregister te raadplegen. Dit kan bijdragen aan transparantie. Als de betrokkene vervolgens wil weten of zijn eigen gegevens op juiste wijze verwerkt worden, kan hij hiertoe een aanvraag rechten betrokkene indienen.

Rechten van de betrokkene

Onder de AVG hebben betrokkenen een aantal rechten. Via een aanvraagprocedure en een besluit kunnen zij deze rechten uitoefenen en daartegen (indien nodig) bezwaar en beroep instellen. Besluitvorming is aan een termijn gebonden: onverwijld maar in ieder geval binnen een maand. Bij complexe aanvragen kan deze termijn met maximaal twee maanden verlengd worden. Overschrijding van de beslistermijn kan leiden tot het betalen van een dwangsom wegens niet tijdig beslissen.

De FG's verrichtten geen onderzoek naar de vraag of in de rapportageperiode (juiste) besluitvorming plaatsvond binnen de termijnen. Zij volstaan hier met het maken van enkele inhoudelijke opmerkingen.

Het is aan de verwerkingsverantwoordelijke om te besluiten op een aanvraag in het kader van rechten van de betrokkene. Dit betekent dat helder moet zijn welk orgaan dit is. Zie ook de toelichting onder het kopje verhoudingen in de Drechtsteden. Als er sprake is van gezamenlijke verwerkingsverantwoordelijkheid zullen partijen op dit punt heldere afspraken moeten maken en dit aan de betrokkenen communiceren.

Het is belangrijk dat personen slechts inzage krijgen in hun eigen persoonsgegevens. De organen moeten er dan ook voor waken dat informatie niet aan onbevoegden worden verstrekt (datalek). Tijdens het rapportagejaar merkten we dat een aantal organisaties om die reden hoge eisen stellen op het gebied van het vaststellen van de identiteit van de aanvrager.

Ander aandachtspunt is de wijze van afdoening. Een aanvraag is een formeel verzoek en het startpunt van een procedure. Dit eindigt met een besluit: een schriftelijke beslissing. Wij constateren dat deze procedure niet altijd correct wordt gevolgd. Bijvoorbeeld als iemand verzoekt om inzage of verwijdering, dan wordt weliswaar actiegericht meegedacht. Maar dat neemt niet weg dat ook formele besluitvorming moet plaatsvinden (tenzij de betrokkene zijn aanvraag intrekt).

Klachten/FG-contactpunt

Betrokkenen kunnen, bij de FG, klagen over omgang met hun persoonsgegevens. Tijdens de rapportageperiode hebben 13 personen hun beklag gedaan. De FG fungeert hierbij als een soort ombudsfunctie. In de meeste gevallen bracht de FG de betrokkene in contact met het betreffende bestuursorgaan dat de vraag/klacht vervolgens afhandelde. In sommige gevallen bleek er sprake van een datalek. Verder klaagden enkele betrokkenen (samengevat) over het gebrek aan transparantie. Hier zal de FG in de toekomst mogelijk nader onderzoek naar verrichten.

Contact met de FG verloopt via de FG e-mailbox fg@drechtsteden.nl. Dit is één mailbox voor alle organisaties gezamenlijk. Op zich is dit vreemd. Tijdens het rapportagejaar liep het contact met de FG altijd via de GRD. Dit terwijl de betreffende inwoner de FG zich meestal richt tot één van de deelnemende organisaties. Richting de inwoner komt dit onvriendelijk over: de FG moet altijd eerst vragen in welke

hoedanigheid men de FG benadert (lees: tot welke organisatie de vraag/klacht zich richt). Daarnaast lijkt dit in strijd met de eisen van informatiebeheer en informatiebeveiliging.

Aanbevelingen:

Zorg ervoor dat het beleid ten aanzien van de betrokkenen aansluit op juiste verwerkingsverantwoordelijkheid.

Overzicht Datalekken

De AVG kent een meldplicht datalekken. Het register van de datalekken werd tijdens deze rapportageperiode voor alle organisaties bijgehouden door de adviseurs gegevensbescherming, die werkzaam waren bij het onderdeel GRD/ SCD (nu gemeente Dordrecht/Servicegemeente). Zij hebben de volgende gegevens aangeleverd.

1-4-2021																	
31-12-2021																	
	DD	GAD	GBD	GDD	GHG	GHA	GSD	GZD	GPD	SCD	GRD	OZHZ	BD	SDD	OCD	IBD	TOTAAL
TOTAAL DATALEKKEN	2	3	2	4	1	1	3	3	1	3	0	3	1	17	0	0	44
Systeem of applicatie werkt niet	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gevonden USB stick	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Verkeerde autorisaties/rechten	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Persoonsgegevens gevonden	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	2
Persoonsgegevens naar verkeerde ontvanger	2	0	2	2	0	0	1	0	0	2	0	2	0	13	0	0	24
Persoonsgegevens in logging	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persoonsgegevens per ongeluk toegankelijk	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	2
Persoonsgegevens per ongeluk gepubliceerd	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Apparaat, gegevensdrager of papier kwijtgeraakt of gestolen	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Brief of postpakket kwijtgeraakt	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Hacking, malware en/of phishing	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persoonsgegevens van verkeerde klant getoond in klantportaal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Teveel persoonsgegevens gepubliceerd	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Verloren/gestolen hardware	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Verkeerd verzonden post of e-mail	0	0	0	1	0	0	1	1	0	0	0	0	1	3	0	0	7
Ongeautoriseerde toegang	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Brief of postpakket geopend retour ontvangen	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Persoonsgegevens zonder toestemming afgegeven	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tijdig ingediend Bij AP = Ja	1	0	0	0	0	0	1	0	0	0	0	0	0	6	0	0	8
Tijdig ingediend = Nee	0	0	0	1	0	0	1	2	0	0	0	0	0	7	0	0	11

Het valt de FG op dat er grote verschillen tussen de organisaties zijn. Daarnaast sluit het register niet aan bij de verantwoordelijkheid (degene op wie de wettelijke meldingsplicht rust). Zie hiervoor ook hier wat onder het kopje over verhoudingen/verantwoordelijkheden binnen de Drechtsteden in deze rapportage is opgemerkt. In het register zijn bijvoorbeeld Dienstverlening Drechtsteden, SDD en het SCD als verantwoordelijke aangemerkt. Naast het feit dat zij geen zelfstandige entiteiten waren (want onderdeel van bestuur GRD) lijken zij ook niet (althans zeker niet als enige) verwerkingsverantwoordelijkheid te hebben. Ook is er geen onderscheid gemaakt tussen de colleges en burgemeesters.

Daarnaast valt op dat (volgens het register) van de meldingsplichtige datalekken bij de Autoriteit Persoonsgegevens 58% van de meldingen te laat is ingediend. Over het algemeen lijkt ook de conclusie gerechtvaardigd dat er te weinig datalekken in het proces gemeld worden. Bijvoorbeeld alleen al door het feit er geen geopende retourpost is gemeld. Of omdat iedere e-mail die verkeerd wordt verzonden waar persoonsgegevens instaan al moet worden aangemerkt als datalek. Als FG kunnen wij ons niet voorstellen dat dit soort situaties niet (veel vaker) voorkwamen tijdens het rapportagejaar.

Zoals al is aangegeven in het jaarplan zal de FG in het jaar 2022 onderzoek verrichten naar de omgang met de meldplicht datalekken. Dit omvat ook kwalitatieve aspecten. Daarom wordt nu volstaan met enkele

algemene aandachtspunten en worden alleen de volgende algemene aanbevelingen gegeven. Deze aanbevelingen werden vorig jaar overigens ook al aan de meeste bestuursorganen gegeven.

Aanbevelingen
Blijf scherp op het herkennen van mogelijke datalekken en zorg voor tijdige actie. Onderzoek of er maatregelen nodig zijn om te borgen dat nog meer datalekken binnen de wettelijke termijn kunnen worden gemeld.

Positionering FG/ capaciteit

Tijdens de rapportageperiode waren de FG-taken verdeeld over twee verschillende functies. De Adviseurs Gegevensbescherming (AG's), onderdeel van GRD/SCD voeren de wettelijke algemene adviestaak van de FG uit. De overige FG taken (toezicht op naleving, advisering op DPIA's, aanspreekpunt voor inwoners en AP) zijn belegd bij de FG's. Tijdens het rapportagejaar was hun capaciteit als volgt:

- Periode van 1 april tot en met 31 december 2021: Ingrid Huizer (1 FTE) als FG van alle organen zoals in deze rapportage benoemd.
- Periode van 1 april tot en met 31 juli 2021: externe inhuur (1FTE) voor alle organen.
- Periode van 1 augustus tot en met 31 december 2021: Esther Verhage (0,89 FTE) als FG van alle college, GRD en OZHZ.

Deze beschikbare capaciteit wringt, net als het opsplitsen van taken tussen AG en FG. De FG's zijn van oordeel dat er niet voldoende tijd en capaciteit beschikbaar is om de wettelijke FG taken uit te voeren voor de hoeveelheid aan bestuursorganen voor wie we als FG waren aangewezen. Zo is er bijvoorbeeld geen tijd om actief onderzoek te doen naar de stand van zaken met betrekking tot onderwerpen die niet (uitgebreid) in deze rapportage zijn opgenomen. Ook hebben de adviseurs gegevensbescherming te weinig tijd om de adviesrol van de FG goed uit te voeren. Zo worden er doorgaans geen ongevraagde adviezen uitgebracht. Er dient voldoende tijd beschikbaar te zijn om alle wettelijke FG taken voor alle bestuursorganen uit te voeren. De bestuursorganen dienen ook aan te tonen dat hieraan wordt voldaan. Tot nu toe is dit niet gebeurd. Dit baart de FG's zorgen, zeker nu het volwassenheidsniveau van de organisatie zo laag is. Indien de organisaties bijvoorbeeld wel zouden voldoen aan hun DPIA-verplichtingen, of aan hun informatieverplichtingen zou de FG-capaciteit bij lange na niet meer voldoen.

Daarnaast constateren we dat het beleggen van de FG adviestaak bij de adviseurs gegevensbescherming in de praktijk niet goed werkt. Door de FG taken over verschillende functies te verdelen, die niet eens in hetzelfde organisatieonderdeel zijn geplaatst, ontstaat frictie. Dit is niet goed voor de relatie tussen de FG en de adviseurs en daarnaast niet voor de bestuursorganen. Het is nu onduidelijk wanneer sprake is van FG-advies en wanneer van een gewoon advies van de adviseurs gegevensbescherming. Bovendien zou het vooraf duidelijk moeten zijn met welke pet de adviseur aan tafel zit. Het is immers een andere situatie wanneer de adviseur echt als adviseur van de organisatie een advies moet geven, of vanuit diens rol als toezichthouder adviseert. Naar ons oordeel is het daarnaast zeer de vraag of deze verdeling van taken tussen verschillende functies toelaatbaar is. De FG's waren hierdoor niet in staat volle verantwoordelijkheid te nemen voor taken die bij wet aan de FG zijn toegekend.

Net als voorgaande jaren ontbrak het tijdens de rapportageperiode aan een FG-reglement. Dit is een noodzakelijke waarborg om te borgen dat de FG in onafhankelijkheid zijn werk kan uitvoeren voor de verschillende bestuursorganen. Vooral met het oog op verwachte ontwikkelingen in 2022, zoals uitbreiding van taken (Wpg) en werkzaamheden (raden) is dit nóg urgenter.

Daarnaast is het nu voor de FG's onduidelijk of de FG's tijdens dit rapportagejaar ook benoemd waren/worden als FG voor (het bestuursorgaan) de burgemeester. Door de burgemeester van Dordrecht en Papendrecht heeft hierover separaat besluitvorming plaatsgevonden, in die zin dat één FG expliciet is

aangewezen als (ook) hun FG. Door de overige burgemeesters niet. Door geen FG aan te wijzen voldoen deze organen niet aan de AVG. Daarnaast zorgt het voor onduidelijkheid als niet alle gemeenten in de Drechtsteden op dezelfde wijze hun FG aanwijzen. Wij doen een dringend beroep om aan deze onduidelijke situatie een einde te maken.

Aanbevelingen
Ga na voor welke bestuursorganen de FG is benoemd. Onderzoek hoeveel FG-capaciteit en middelen er noodzakelijk zijn om aan de wettelijke verplichtingen te voldoen en of het opsplitsen van taken tussen FG en AG hier wel bij past. Betrek hier ook de FG tijdig bij. De wettelijke verplichting om voldoende FG capaciteit en middelen beschikbaar te stellen gelden per verantwoordelijk bestuursorgaan. Vanuit de aantoonbaarheidsverplichting uit de AVG wordt geadviseerd om per bestuursorgaan aan te geven hoeveel capaciteit en middelen er beschikbaar zijn voor de uitvoering van de FG taken.

Informatieverplichting aan de FG

Artikel 38 van de AVG vereist dat de verantwoordelijke en de verwerker erop toezien dat de FG “naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens”. De EDPB heeft in de Richtlijnen voor functionarissen voor de gegevensbescherming een verdere invulling aan deze bepaling gegeven. Hierin is onder andere opgenomen:

"Het is van cruciaal belang dat de FG zo vroeg mogelijk betrokken wordt bij alle aangelegenheden die de bescherming van persoonsgegevens betreffen. Wat betreft privacy impact assessments, stelt de AVG expliciet dat de FG daar in een vroeg stadium bij betrokken dient te worden en vereist de AVG dat de verantwoordelijke bij het uitvoeren van dergelijke privacy impact assessments het advies van de FG inwint. Wanneer de FG direct geïnformeerd en geraadpleegd wordt, is het makkelijker de AVG na te leven en wordt privacy by design geboden. Daarom dient dit een standaardprocedure binnen de organisatie te zijn. Daarnaast is het belangrijk dat de FG als een gesprekspartner binnen de organisatie gezien wordt en dat hij of zij deel uitmaakt van de relevante werkgroepen die binnen de organisatie gegevens verwerken. Daarom dient de organisatie er bijvoorbeeld op toe te zien dat:
• De FG regelmatig wordt uitgenodigd om aan vergaderingen van het hoger management en het middenmanagement deel te nemen.
• Er wordt aangeraden hem uit te nodigen wanneer beslissingen met gevolgen voor gegevensbescherming worden genomen. Alle relevante informatie dient tijdig aan de FG doorgegeven te worden om hem in staat te stellen passend advies te geven.
• Aan de mening van de FG dient altijd passende waarde gehecht te worden. Bij geschillen raadt WP29 aan om vast te leggen waarom het advies van de FG niet gevolgd is.
• De FG dient onmiddellijk geraadpleegd te worden indien zich een datalek of ander incident heeft voorgedaan."

Bevindingen
Het is niet duidelijk hoe de Drechtsteden invulling geven aan deze richtlijn. Het opsplitsen van taken tussen FG en AG is daarbij (op zijn minst) een complicerende factor. Als FG merken wij in ieder geval dat de FG te vaak niet, onvolledig of te laat wordt betrokken: systemen worden aangeschaft en in gebruik genomen zonder FG advies, de gehele transitie is verlopen zonder DPIA's en bijbehorend FG advies en er vindt besluitvorming plaats (zelfs over positionering en FG capaciteit) zonder dat de FG daar op de juiste wijze bij betrokken wordt. Op een FG-adviesmemo van 8 oktober 2021 (welke was gericht aan secretarissen als hoogste ambtelijk leidinggevenden) is zelfs geen enkele reactie gekomen. En sommige informatie wordt alleen kenbaar door toevallige kennisname van krantenartikelen (Bueno app) of reguliere informatieberichten die aan alle medewerkers wordt verstrekt. Hierin is weinig tot geen verbetering ten aanzien van voorgaande jaren waargenomen.

Dit is in strijd met de wettelijke bepaling, doet geen recht aan de positie van de FG, is niet goed voor de verhouding tussen de FG en de verantwoordelijken en gaat ten koste van het beschermen van de privacybelangen van de betrokkenen.

Als FG betreuren wij het dat wij regelmatig niet op de juiste wijze worden betrokken. Daarnaast lopen de betreffende bestuursorganen hiermee ook een risico. Recent verhoogde de Autoriteit Persoonsgegevens de boete aan de Belastingdienst met € 450.000 wegens het niet tijdig en naar behoren betrekken van de FG terwijl dit wel wettelijk verplicht was.[4]

Aanbeveling:
Onderzoek hoe kan worden geborgd dat de FG op de juiste wijze wordt geïnformeerd en betrokken bij alle zaken die verband (kunnen) houden met bescherming van persoonsgegevens.

E- learning informatiebeveiliging en Privacy

Tot 31 augustus 2021 was er een e-learning met betrekking tot informatiebeveiliging en privacy van Q bit beschikbaar. Zoals de onderstaande tabel laat zien zitten er tussen de verantwoordelijken grote verschillen in het aantal personen die de e-learning hebben gevolgd. Zoals uit de aangeleverde informatie volgt zijn er organisaties waarbij de e- learning goed werd gevolgd (bijvoorbeeld Papendrecht waar zelfs meer dan 100 personen de e-learning in 2021 hebben gevolgd) , maar zelfs ook 2 organisaties waarbij geen enkele medewerker de beschikbare e-learning in 2021 heeft gevolgd (Sliedrecht en Hardinxveld-Giessendam). Per 31 augustus was de e-learning van Q bit in zijn geheel niet meer beschikbaar. Dit is een ongewenste situatie in het kader van training en bewustwording rondom privacy en informatiebeveiliging en het kunnen voldoen aan de vereisten van de BIO die hierop betrekking hebben.

Organisatie	module 1 30-04	module 2 30-04	module 3 30-04	module 1 31-08	module 2 31-08	module 3 31-08	module 4 31-08
Bureau Drechtsteden	1	1	0	1	1	0	0
Gemeente Alblasserdam	2	4	4	4	6	6	2
Gemeente Dordrecht	4	2	3	4	2	4	0
Gemeente Hardinxveld-Giessendam	0	0	0	0	0	0	0
Gemeente Hendrik-Ido-Ambacht	4	2	2	8	7	6	2
Gemeente Papendrecht	97	95	106	111	107	116	13
Gemeente Sliedrecht	0	0	0	0	0	0	0
Gemeente Zwijndrecht	6	4	3	7	4	4	2
Gemeentebelastingen Drechtsteden	32	31	30	40	41	42	34
Ingenieursbureau Drechtsteden	0	0	0	0	0	0	0
Omgevingsdienst	4	2	2	77	79	87	85
Regionale Ambulancevoorziening ZHZ	0	0	0	0	0	0	0
Servicecentrum Drechtsteden	82	85	82	83	88	87	30
Sociale Dienst Drechtsteden	3	1	0	3	1	0	0

Aanbeveling:
Zorg voor bewustmaking op het gebied van omgang met persoonsgegevens en maak dit een periodiek terugkerend thema. Zorg dat medewerkers opgeleid worden op een niveau dat aansluit op hun werk. Betrek hier ook de CISO bij, vanuit oogpunt van informatiebeveiliging.

[4] Zie: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-zwarte-lijst-fsv

Conclusie

Op het gebied van de benoemde onderwerpen in de rapportage is door de verschillende bestuursorganen nog een hoop werk te verzetten om aan de wet te kunnen voldoen. Op bijna alle onderzochte gebieden zijn de resultaten immers onvoldoende. Er is over het algemeen, op OZHZ na, weinig tot geen vooruitgang te ontdekken ten opzichte van de vorige rapportageperiode. De basis is niet op orde. Dat baart zorgen nu dit direct leidt tot de conclusie dat de bestuursorganen daarmee de grondrechten van hun inwoners en hun medewerkers niet voldoende borgen. Voor inwoners geldt bovendien dat zij geen enkele keuze hebben en als het ware "veroordeeld" zijn tot de bestuursorganen van de gemeente waarin zij wonen en de organen van de gemeenschappelijke regelingen. Als zij een paspoort, een vergunning of schuldhulpverlening willen aanvragen kunnen zij dit namelijk alleen doen in de gemeente waar zij wonen.

Beperkte FG capaciteit maakt dat niet kan worden gedifferentieerd in welke mate de aanbevelingen per bestuursorgaan van toepassing zijn. Daarnaast zijn een aantal aandachtspunten minder relevant door de ontwikkelingen in de Drechtsteden. Als bijvoorbeeld toch nieuw privacybeleid vastgesteld moet worden is minder relevant dat het beleid uit 2020 nog niet bekendgemaakt is. Aan de andere kant laat de aanloop naar de transitie zien dat de basis nog steeds niet op orde is en dat dit knelt bij omvangrijke complexe ontwikkelingen zoals de verantwoordelijkheden na de transitie en de migratie naar de cloud. Ook de FG-positionering en beschikbare capaciteit is een onderwerp dat al zorgen baarde. Die zorgen namen tijdens deze rapportageperiode toe. Zo was er onvoldoende tijd beschikbaar om inhoudelijk in te gaan op alle relevante privacy onderwerpen.

Reden voor ons om alle organen op te roepen voor zichzelf na te gaan waar zij staan (0-meting). En op basis hiervan elk voor zich een eigen plan van aanpak te maken waaruit blijkt hoe zij aan de (basis)beginselen van de AVG gaan voldoen. Dit vereist actieve sturing (door bestuur en management) en waarschijnlijk betekent dit ook dat geïnvesteerd moet worden in de privacy-organisatie. Het gaat immers om het verrichten van achterstallig onderhoud terwijl de winkel 'gewoon' open is.

Dit soort acties is echt van belang om omgang met persoonsgegevens goed te managen, vanuit een heldere governance en heldere doelstellingen. Inclusief het sturen op het bereiken ervan en het periodiek informeren van de FG over de voortgang.