Jaarrapportage gegevensbescherming

Alblasserdam

april 2020 – april 2021

Functionaris Gegevensbescherming

Inhoud

Inleiding

Het afgelopen jaar hebben we in Nederland helaas teveel voorbeelden gezien waarbij de overheid niet zorgvuldig is omgegaan met persoonsgegevens van inwoners. Het schenden van de persoonlijke levenssfeer van inwoners, het (onbewust) discrimineren en volgen van inwoners en een slordige omgang met gegevensbescherming heeft het vertrouwen van de inwoner in de overheid de nodige schade opgeleverd.

Als gevolg van de digitale transformatie wordt de hoeveelheid verwerkingen van persoonsgegevens door de overheid steeds groter. Het risico op schending van de AVG vindt hierdoor steeds makkelijker en sneller plaats en de kans dat een dergelijke schending onopgemerkt blijft is ook aanwezig. Denk bijvoorbeeld aan de welbekende Toeslagenaffaire bij de Belastingdienst Toeslagen, maar ook de datalekken bij de GGD/GHOR met betrekking tot testgegevens, de wifitracking door de gemeente Enschede en de ophef over het gebruik van social media bij fraudeonderzoek door gemeenten en politie.

Bij de laatste twee voorbeelden hebben de betrokken organisaties de maatschappelijke impact van hun handelen behoorlijk onderschat, omdat ze in hun ogen voldoende maatregelen genomen hadden om de schadelijke effecten voor de burger te voorkomen. Hieruit blijkt nogmaals hoe belangrijk het is om na te denken over de potentiële risico's van verwerkingen van persoonsgegevens en de mogelijke gevolgen van deze verwerkingen voor de inwoners.

In deze rapportage is gekeken naar de stand van zaken op het gebied van privacy bij de gemeente Alblasserdam (hierna: GAD). Het rapport is opgedeeld in verschillende onderwerpen, waarop bevindingen en aanbevelingen zijn geschreven. Deze bevindingen zijn opgesteld op basis van de door de GAD aangeleverde beantwoording van de vragenlijst 'privacy audit 2021' en de constateringen over het afgelopen jaar van de FG zelf. De aanbevelingen zijn bedoeld om de privacy van persoonsgegevens het komende jaar naar een hoger niveau te tillen.

Aan het einde van het rapport volgt er nog een paragraaf met regiobrede risico's die voor de gehele Drechtsteden gelden. Tot slot worden de belangrijkste aanbevelingen uit deze rapportage samengevat in de conclusie.

Resultaten Audit

Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten is het register waarin alle werkprocessen van het college van Alblasserdam zijn vastgelegd en beschreven. Het register is wettelijk verplicht op grond van artikel 30 van de AVG. In deze audit is ingegaan op de mate waarin het register compleet en actueel is, of de wijze en het moment van actualiseren is beschreven en vastgelegd, en hoeveel mutaties er dit rapportagejaar zijn doorgegeven.

Bevindingen

- Het college van Alblasserdam geeft aan dat het register van verwerkingen niet compleet en actueel is.
- Er is niet bekend hoeveel mutaties er zijn doorgevoerd in het afgelopen rapportagejaar.
- Het is niet vastgelegd op welke wijze en op welke momenten het register wordt geactualiseerd.
- In de vorige rapportage werd nog geconcludeerd dat de GAD stappen gemaakt had op dit onderwerp en dat het register actief werd gemonitord. De aanbeveling om periodiek het gehele verwerkingsregister door te lopen, zolang het wijzigen van verwerkingen nog geen standaard handeling is, is nog niet overgenomen/ uitgevoerd.
- Momenteel wordt er gewerkt aan het proces Register van Verwerkingen. Er is een beschrijving gemaakt, maar deze is nog niet gecontroleerd/vastgesteld.
- In dit proces moet nog worden bepaald wie wordt aangewezen als eindverantwoordelijke voor het register.

Aanbevelingen

- Zorg ervoor dat er inzicht komt in welke wijzigingen en aanvullingen op het register noodzakelijk zijn. Borg dat deze worden opgenomen in het register waardoor deze compleet en actueel wordt.
- Borg het proces rondom het Register van verwerkingen in werkinstructies en wijs een eindverantwoordelijke aan voor dit proces. Neem hierin op dat het register periodiek gemonitord wordt.

Rechten van betrokkenen en klachten

Met de invoering van de AVG zijn de rechten van betrokkenen uitgebreid en verstevigd. In deze audit is ingegaan op de borging van deze rechten in processen, of er werkinstructies zijn opgesteld, wie er verantwoordelijk is en wie er belast is met de uitvoering van deze processen, hoeveel verzoeken er zijn binnenkomen, of deze verzoeken binnen de wettelijke termijn zijn behandeld, en of het informeren van de FG bij dergelijke verzoeken is geborgd.

Bevindingen

- Er zijn in de rapportageperiode geen klachten ingediend.
- De rechten van betrokkenen kunnen worden uitgeoefend middels formulieren op de website.
- Verificatie vindt plaats via DigiD of via de balie.
- De rechten van betrokkenen zijn deels geborgd in processen.
- De basis voor de werkinstructies staat. Momenteel worden de werkinstructies voor deze processen verder uitgewerkt, dit wordt in 2021 afgerond.
- Er is niet beschreven wie verantwoordelijk is voor en belast met de uitvoering van het proces. Dit wordt meegenomen in de uitwerking van de werkinstructies.
- Het informeren van de FG is nog niet geborgd in de processen. Ook dit wordt meegenomen in de uitwerking van de werkprocessen.

- Informatie over het proces voor het indienen van een verzoek is via de website gecommuniceerd, maar is niet beschikbaar op papier.
- Er zijn 2 verzoeken ingediend met betrekking tot de rechten van betrokkenen.
- 1 verzoek binnen de wettelijke termijn afgehandeld.
- 1 verzoek is ver buiten de wettelijke termijn afgehandeld, namelijk 7 maanden.

Aanbevelingen

- Zorg ervoor dat de werkinstructies zorgvuldig worden uitgewerkt en dat deze processen worden geborgd in de organisatie.
- Wijs een verantwoordelijke aan die verantwoordelijk is voor, en belast met, de uitvoering van het proces. Wacht hier niet mee tot de werkinstructies volledig zijn uitgewerkt.
- Evalueer waarom 1 verzoek ver buiten de wettelijke termijn is afgehandeld en tref waar mogelijk maatregelen om herhaling het komende rapportagejaar te voorkomen.

Overeenkomsten in verband met het delen van persoonsgegevens

Op grond van artikel 28 van de AVG moeten er schriftelijke afspraken worden gemaakt wanneer de verantwoordelijke persoonsgegevens laat verwerken door een verwerker. Doorgaans wordt hier een verwerkersovereenkomst voor afgesloten. Verwerkersovereenkomsten zijn een belangrijk instrument om de privacy en bescherming van persoonsgegevens te garanderen als een (deel van) een werkproces is uitbesteed. In deze audit is ingegaan op hoeveel verwerkersovereenkomsten zijn afgesloten, of deze (centraal) opgeslagen en geregistreerd worden, of het inzichtelijk is hoeveel verwerkersovereenkomsten er nog moeten worden afgesloten en of er verwerkersovereenkomsten zijn afgesloten voor de dienstverlening van of binnen de regio.

Daarnaast is er soms geen sprake van een verantwoordelijke- verwerker relatie, maar zijn er verschillende verantwoordelijken gezamenlijk verantwoordelijk in een proces. Ook dan moeten er schriftelijke afspraken worden gemaakt op grond van artikel 26 van de AVG.

Bevindingen

- Er is deels inzichtelijk met welke partijen gegevens worden uitgewisseld. Aan dit overzicht wordt gewerkt.
- Er zijn in het afgelopen rapportagejaar geen verwerkersovereenkomsten afgesloten. Er zijn wel verwerkersovereenkomsten opgesteld, maar niet door partijen ondertekend.
- Het is niet inzichtelijk hoeveel verwerkersovereenkomsten nog gesloten moet worden.
- Er zijn nog geen verwerkersovereenkomsten afgesloten voor de dienstverlening van of binnen de regio. Er is wel sprake van deze vorm van dienstverlening en er moeten dus nog verwerkersovereenkomsten worden afgesloten. De gemeente geeft aan de verwerkersovereenkomst met het SCD als eerste op te pakken.
- Er is een procesbeschrijving voor het opslaan en registreren van verwerkersovereenkomsten in AddVueConnect, maar deze moet nog worden vastgesteld en geïmplementeerd.
- Bij het inschakelen van een nieuwe partij of de inkoop van een nieuwe applicatie wordt geïnformeerd bij de juiste collega's wat er nodig is en wat er gedaan moet worden op het gebied van privacy. Er is hier geen vastgelegd proces voor aanwezig.
- Er worden art. 26 overeenkomsten gesloten door de GAD. Momenteel ligt er een concept artikel 26 overeenkomst voor het proces Vroegsignalering tussen de SDD en de GAD op tafel.
- Het is niet inzichtelijk of en voor hoeveel processen nog meer een art. 26 overeenkomst afgesloten moet worden.
- Het opslaan en registreren van art. 26 overeenkomsten vindt op dezelfde manier plaats als bij de verwerkersovereenkomsten (in AddVueConnect). Er is een procesbeschrijving opgesteld, maar deze moet nog worden vastgesteld en geïmplementeerd.

Aanbevelingen

Het ontbreken van (een overzicht van) verwerkersovereenkomsten en art. 26 overeenkomsten is een risico. Ten opzichte van de rapportage van vorig jaar en het jaar daarvoor is hier helaas geen vooruitgang geboekt. Vorig jaar is aangegeven dat aan dit onderwerp prioriteit gegeven moet worden. Dit is helaas niet gebeurd. De volgende aanbevelingen worden daarom voor dit jaar gedaan:

- Zorg ervoor dat er een overzicht komt van de afgesloten verwerkersovereenkomsten.
- Zorg ervoor dat concept overeenkomsten worden getekend en op de juiste manier worden geregistreerd/opgeslagen.
- Breng in kaart welke verwerkersovereenkomsten nog moeten worden gesloten. Borg in een plan van aanpak dat alle benodigde verwerkersovereenkomsten binnen een bepaalde termijn worden gesloten, zowel voor verwerkingen door volledige externen, als voor de dienstverlening door/ binnen de regio.
- Borg privacy in een inkoopproces en bij de inschakeling van een nieuwe partij. Ondanks dat de initiatie van nieuwe applicaties grotendeels binnen de regio plaatsvindt, is het belangrijk om dit proces intern ook helder beschreven en geborgd te hebben.
- Zorg dat er een goed overzicht komt van de afgesloten artikel 26 overeenkomsten.
- Zorg dat er inzicht komt in welke artikel 26 overeenkomsten nog moeten worden gesloten en maak een plan hoe wordt gekomen tot een situatie dat aan dit onderdeel van de wet wordt voldaan.

Trainings- en bewustwordingsprogramma

Bewustwording en kennis bij medewerkers is een belangrijk instrument om te komen tot een structurele borging van privacy en gegevensbescherming. Een trainings- en bewustwordingsprogramma kan hieraan een belangrijke bijdrage leveren. In deze audit is ingegaan op de vraag of er een dergelijk programma is opgezet, voor zowel bestaande als nieuwe medewerkers.

Bevindingen

- De training voor nieuwe medewerkers is geregeld via een e-learning van Qbit.
- Er wordt binnen de organisatie gestuurd op het afronden van de e-learning binnen 3 maanden na indiensttreding. De praktijk leert echter dat deze termijn niet altijd behaald wordt.
- Bestaande medewerkers zijn tevens verplicht de e-learning van Qbit te volgen. Daarnaast zijn voor hen de modules van Skillstown onder de aandacht gebracht. Het is onduidelijk of hier al gebruik van gemaakt wordt.
- Verdere bewustwording wordt gedaan middels berichten over de AVG via SID.

Aanbevelingen

- Borg de training van nieuwe medewerkers in een proces, waarbij gegarandeerd kan worden dat deze training ook binnen 3 maanden wordt gevolgd/afgerond. Een e-learning kan een goed middel zijn. Ook het verplicht volgen van een workshop kan een goede optie zijn.
- Vorig jaar is er de volgende aanbeveling gedaan: *zet voor bestaande medewerkers een periodiek trainings- en bewustwordingsprogramma op. Hierbij dient de organisatie er zorg voor te dragen dat de trainingsinhoud actueel blijft, de training op regelmatige basis plaatsvindt, leerdoelen worden opgesteld én bereikt en de aanwezigheid bij trainingen wordt gedocumenteerd.* Deze aanbeveling geldt ook voor dit jaar.
- Monitor de deelname van bestaande medewerkers aan de aangeboden trainingen en spreek medewerkers aan als ze geen gebruik maken van het aanbod.

Governance

Om een structurele borging van privacy en gegevensbescherming te borgen, is een gedegen organisatorische inrichting – governance – noodzakelijk. In deze audit is ingegaan op in hoeverre het management betrokken is bij het borgen van privacy in de organisatie, hoe en hoe vaak er vanuit het management wordt gecommuniceerd over het belang van privacy, of de uitvoerende en coördinerende taken op het gebied van privacy conform het privacy beleid worden uitgevoerd, en of er voorzien is in capaciteit voor deze taken.

Bevindingen

- Privacy maakt geen terugkerend onderdeel uit van de vergaderingen van bestuur en management. Datagedreven werken en sturen op informatie is een grote wens van de gemeente, maar is nog niet mogelijk met de huidige budgetten
- Het belang van privacy wordt door het management ad hoc onder de aandacht gebracht, bijvoorbeeld tijdens Keek op de week en de dag van de privacy.
- Het college van Alblasserdam geeft in de vragenlijst aan dat er zoveel mogelijk wordt gehandeld volgens het opgestelde privacy-beleid.
- De huidige capaciteit is momenteel niet voldoende om de privacy in de organisatie te borgen. Er is een tijdelijke PC voor 8 uur en een collega voor 6 uur bezig met privacy. Per 1 augustus a.s. is er een volledige invulling voor de rol van Privacy Coördinator.
- Het is momenteel niet duidelijk wie proceseigenaar is van de verwerkingen van processen met persoonsgegevens. Dit wordt momenteel uitgevraagd en uitgewerkt in een document. Dit document moet verhelderen welke verantwoordelijkheden bij welke persoon of functie liggen.
- Omdat het niet duidelijk is wie precies proceseigenaar is van welk proces, worden proceseigenaren niet actief gewezen op hun verantwoordelijkheden i.h.k.v. de AVG. Voor sommige proceseigenaren is deze verantwoordelijkheid vanzelfsprekend en bij sommige is dit nog echt een aandachtspunt.

Aanbevelingen

- Maak privacy een terugkerend onderdeel van vergaderingen van het bestuur en het management.
- Zorg voor voldoende capaciteit om de privacy in de organisatie te borgen.
- Maak een duidelijk overzicht van de processen met persoonsgegevens en wie proceseigenaren zijn van deze processen.
- Zorg er vervolgens voor dat de verantwoordelijkheden niet alleen inzichtelijk zijn op papier, maar dat de procesverantwoordelijkheden ook weten dat ze verantwoordelijk zijn en wat deze verantwoordelijkheden inhouden.

Privacy verklaring

De AVG legt extra nadruk op het informeren van betrokkenen over hoe er met hun persoonsgegevens wordt omgegaan en welke gegevens er worden verwerkt. Een van de middelen om dit te doen is de privacyverklaring. In deze audit is ingegaan op de vraag of de GAD een privacyverklaring heeft en of - en op welke wijze - deze vrij beschikbaar is.

Bevindingen

- Er is een gepubliceerde privacyverklaring aanwezig op de website van Alblasserdam.
- De privacyverklaring is een algemene verklaring en gaat niet in op specifieke verwerkingen, hoog risico verwerkingen en het gebruik van algoritmen bij het verwerken van persoonsgegevens.

- De privacyverklaring is alleen beschikbaar op de website. De gemeente geeft aan dat er gewerkt wordt aan een papieren versie. De verklaring is dus niet overal vrij beschikbaar.

Aanbevelingen

- De basis voor een goede privacyverklaring staat. Bekijk waar de verklaring kan worden uitgebreid, zodat ook voldoende informatie wordt gegeven over specifieke verwerkingen, hoog risico verwerkingen en het gebruik van algoritmen. Denk bijvoorbeeld aan een gelaagde privacyverklaring, waarbij per onderwerp kan worden doorgeklikt voor meer informatie. Start met de verwerkingen met het hoogste risico, waaronder processen waarin geautomatiseerde besluitvorming of profilering plaatsvindt.
- Zorg ervoor dat de privacyverklaring ook op papier beschikbaar is, zodat ook mensen zonder internettoegang deze verklaring kunnen inzien.

DPIA's

(D)PIA's zijn een belangrijk instrument om vooraf de privacy risico's van een bepaalde verwerking of proces in beeld te brengen, en daar vervolgens maatregelen op te nemen. In deze audit is ingegaan op de beschrijving van de verantwoordelijkheden en het proces van het uitvoeren van (D)PIA's, of er richtlijnen zijn wanneer en op welke wijze deze uitgevoerd moeten worden, of er richtlijnen en templates beschikbaar zijn, of er een overzicht is van het aantal uitgevoerde (D)PIA's, of er een overzicht is voor welke verwerkingen er nog (D)PIA's uitgevoerd moeten worden, op welke termijn deze uitgevoerd zullen worden, en of er geborgd is dat de FG's worden geïnformeerd en kunnen adviseren bij deze (D)PIA's.

Bevindingen

- Er is een procesbeschrijving aanwezig voor de uitvoering van een DPIA.
- Er is beschreven wanneer en op welke wijze een (D)PIA uitgevoerd moet worden.
- Voor het uitvoeren van een DPIA wordt het regiobrede template gebruikt, waar de FG positief over heeft geadviseerd.
- Het college van Alblasserdam geeft aan dat de BRA nog niet als standaard wordt meegenomen, maar dat hier wel actief op wordt gelet. Het belang van een DPIA (en voorafgaand een BRA) wordt gezien, maar de volgorde voor het uitvoeren van een BRA, DPIA of het opstellen van een verwerkersovereenkomst binnen een proces is binnen de gemeente niet duidelijk genoeg.
- Er is een overzicht op de T-schijf aanwezig met de DPIA's die in uitvoering zijn (T-schijf is beveiligd door Autorisatie). Op dit moment gaat het om de volgende stukken:
    - DPIA Rederij Cameratoezicht;
    - DPIA Vroegsignalering.
- Er is binnen de gemeente geen overzicht voor welke processen nog DPIA's uitgevoerd moet worden. Hiervoor wordt momenteel actief navraag gedaan. Op basis van deze uitvraag wordt ook een planning gemaakt voor het uitvoeren van deze DPIA's.
- De FG en adviseurs gegevensbescherming worden betrokken bij het uitvoeren van een DPIA en de DPIA's worden ter advies bij de FG voorgelegd. Een voorbeeld hiervan is de DPIA cameratoezicht de Rederij. Hier heeft de FG verbetermaatregelen voorgesteld, welke worden besproken met de proceseigenaar, de Gemeentesecretaris en de betrokken AG. Het college van Alblasserdam geeft hierbij aan dat de DPIA voor een gedeelte herschreven gaat worden.
- Er is in de rapportageperiode geen sprake geweest van een hoog risico-verwerking na het nemen van maatregelen, waarvoor voorafgaande goedkeuring bij de AP gevraagd moet worden. Er is door de FG wel een hoog risico benoemd in de terugkoppeling op de DPIA cameratoezicht De Rederij. Hierop worden de benodigde verbetermaatregelen genomen.

Aanbevelingen

- Zorg voor bewustwording binnen de organisatie over het uitvoeren van verschillende privacy documenten, zoals bijvoorbeeld een BRA, een DPIA en verwerkersovereenkomsten. Pas zo nodig het trainings- en bewustwordingsprogramma hierop aan en zorg voor heldere procesbeschrijvingen op het gebied van deze onderwerpen.
- Leg, zoals aangegeven, vast voor welke processen een (D)PIA moet worden uitgevoerd. Maak een prioritering en een planning voor het uitvoeren van de DPIA's, gebaseerd op urgentie en zorg voor de juiste capaciteit en juridische kennis om de DPIA's goed en zorgvuldig te kunnen uitvoeren.
- Borg dat bij de afronding van DPIA's restrisico's worden vastgelegd en geaccepteerd.

Privacy door Ontwerp en Standaardinstellingen

Artikel 25 AVG

1. Rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, treft de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van deze verordening en ter bescherming van de rechten van de betrokkenen.
2. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen zorgen met name ervoor dat persoonsgegevens in beginsel niet zonder menselijke tussenkomst voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.

Bevindingen

Er zijn door de gemeente Alblasserdam in het rapportagejaar geen eigen applicaties aangeschaft of gedownload. De aanschaf van de benodigde applicaties loopt via het SCD. Gezien er nog geen duidelijk overzicht is of alle benodigde DPIA's zijn uitgevoerd, kan er niet zijn voldaan aan de eis uit artikel 25 AVG.

Aanbeveling

Richt een proces in zodat aan de voorwaarden van artikel 25 uit de AVG kan worden voldaan. Bij processen waarbij een DPIA nodig is betekent dit dat er op tijd gestart moet worden met een DPIA, waarbij privacy bij ontwerp en standaardinstellingen worden meegenomen in de uitvoering. Door dit proces goed in te richten, beperk je aan de voorkant het ontstaan van onrechtmatigheden of datalekken.

Organisatorische en technische maatregelen

MDM en Bring-Your-Own-Device (BYOD)

Zowel in de privacyrapportage van vorig jaar, als die van het jaar daarvoor is aangegeven dat bij het gebruik van mobiele apparaten passende technische en organisatorische maatregelen moeten worden genomen. Wanneer bijzondere of gevoelige persoonsgegevens worden verwerkt, of op grote schaal algemene persoonsgegevens worden verwerkt moeten meerdere (technische) maatregelen worden genomen. Hoe gevoeliger de gegevens, des te meer technische en organisatorische maatregelen moeten worden genomen.

Gebruik van mobiele gegevensdragers zonder de benodigde beveiligingsmaatregelen leidt tot een hoger risico dat de data bij onbevoegde personen terecht komt. En wanneer dat gebeurt, je daar niet de benodigde maatregelen voor kan nemen. In 2020 zijn er regionaal 12 mogelijke datalekmeldingen van gestolen/verloren/kwijtgeraakt/gevonden tablets/smartphones ingediend.

Uit navraag is gebleken dat er op het gebied van Mobile Device Management en het begrip Bring Your Own Device geen actueel beleid is voor de GRD (het laatste beleid is van 2014).

<u>Bevindingen</u>

- Er is een overzicht van alle devices waarop wordt gewerkt met persoonsgegevens.
- Alle Mobile Devices uitgeleverd vanuit het SCD hebben MDM. In 2021 wordt dit uitgerold op de medewerkers die eerder uitgegeven Mobile Devices hebben ontvangen.
- Momenteel is MDM geïnstalleerd op 58% van de mobiele telefoons en 42% van de tablets.
- Het college van Alblasserdam geeft aan zelf beleid te hebben opgesteld, waarbij Bring your own device niet meer mogelijk is. De devices die nog wel in gebruik zijn onder deze noemer worden momenteel uitgefaseerd. De FG heeft dit beleid niet gezien.

<u>Aanbeveling</u>

Ga na of met het vastgestelde beleid is voldaan aan de volgende aanbevelingen. Volg de aanbevelingen op voor zover daar nog niet aan voldaan is.

- "Borg dat bij het gebruik van mobiele apparatuur de noodzakelijke beveiligingsmaatregelen worden genomen, zodat uiteindelijk binnen afzienbare tijd minimaal is ingericht dat bij de verwerking van gevoelige en bijzondere persoonsgegevens, of grootschalige verwerking van standaard persoonsgegevens op mobile devices altijd voldoende technische en organisatorische maatregelen zullen worden genomen" is hiermee onvoldoende opgevolgd.
- Stel (bij voorkeur Drechtsteden-breed) EDM beleid (waar MDM een onderdeel van is) vast en implementeer dit beleid, zowel voor zakelijke mobiele gegevensdragers, als voor eigen devices. Zorg ervoor dat het nemen van voldoende informatiebeveiligingsmaatregelen op mobiele gegevensdragers is opgenomen in dit beleid, waarbij als minimaal uitgangspunt de aanbeveling van vorig jaar wordt meegenomen.

Thuiswerken en MS Teams

Als gevolg van Covid-19, wordt er nu al meer dan een jaar massaal thuisgewerkt. Hierbij wordt gebruikt gemaakt van verschillende soorten software. De twee belangrijkste hiervan zijn MS Teams, voor video overleggen en VMWare horizon cliënt software bij de thuiswerkers op de fysieke werkplek, waardoor medewerkers vanuit huis kunnen inloggen op de omgeving van de Drechtsteden. Andere informatiedragers (zoals printers in de thuisomgeving bijvoorbeeld) zijn in dit stuk buiten beschouwing gelaten.

Het grootste en belangrijkste risico voor de privacy wordt gevormd door het gebrek aan een goede inrichting van MS Teams. Er is geen DPIA beschikbaar en het ontbreekt aan een goede inrichting die conform de privacywetgeving is. MS Teams wordt bovendien binnen de gehele Drechtsteden buiten het beveiligde netwerk om toegepast, omdat het netwerk de belasting anders niet aan kan. Thuiswerken zal naar alle waarschijnlijkheid ook in de toekomst niet meer weg te denken zijn, waarmee de noodzaak voor een goede inrichting des te groter is.

<u>Aanbeveling</u>

Maak een (Drechtsteden brede) impact analyse voor het thuiswerken als geheel en MS Teams in het bijzonder, waarbij de risico's in kaart worden gebracht middels een DPIA en maatregelen worden getroffen om risico's te verlagen en tot een inrichting van de applicatie te komen die voldoet aan de AVG.

Regiobrede risico's

Het verwerken van persoonsgegevens biedt de samenleving en de overheid vele kansen. Tegelijkertijd zijn er ook grote risico's. Wanneer er iets mis gaat, schendt dat bijna per definitie het vertrouwen van de burger in de overheid en zijn de gevolgen schadelijk voor de maatschappij. Niet zelden is alleen de schijn dat het misgaat al schadelijk.

De AVG is zo opgesteld, dat vòòr nieuwe toepassingen en verwerkingen worden opgestart, zorgvuldigheid in acht is genomen. De AVG borgt dit belangrijke aspect door het verplicht betrekken van de FG en het (soms) verplicht uitvoeren van DPIA's en toepassen van "privacy door ontwerp" voordat een nieuwe verwerking wordt gestart.

Dat betekent dat privacy vragen moeten worden gesteld vòòrdat een formeel besluit een verwerking met persoonsgegevens te starten wordt genomen en dat management, politiek en bestuur goed op de hoogte moeten zijn van risico's en genomen maatregelen. Daarbij moet worden benadrukt dat het hier in de AVG primair gaat om potentiële risico's voor de betrokkene.

Afgelopen jaar is binnen de Drechtsteden weliswaar hard gewerkt aan DPIA's en risico analyses, maar helaas gebeurt dit vaak te laat, zelfs nadat de besluiten al genomen zijn en de verwerking al plaats heeft. Dat is niet alleen onrechtmatig, maar ook inefficiënt. Dat dit probleem zich voordoet binnen vrijwel de gehele regio Drechtsteden, geeft aan dat we hier te maken hebben met een regiobreed risico. Soms is ook verwarring over de verdeling van verantwoordelijkheden en bevoegdheden tussen de GRD en de gemeenten de oorzaak van deze handelswijze. Met de bestuurlijke transitie op komst is dit dan ook een extra belangrijk punt van aandacht.

Terugkijkend op het afgelopen jaar kan worden geconcludeerd dat het tijdig uitvoeren van risico analyses en betrekken van de FG nog niet voldoende is geborgd. Zowel op politiek, bestuurlijk als ambtelijk niveau zal dit proces in de toekomst beter ingericht moet worden. Dat is een opdracht aan de organisatie en het bestuur. Zolang dat niet gebeurt, loopt de burger een risico op een inbreuk van zijn gegevens, en de overheid voldoet niet aan de wet: met alle gevolgen van dien.

Voor een actueel beeld van het privacy niveau in de eigen organisatie is er vanuit het CIP een Self Assessment instrument beschikbaar, de PriSa. De tool (Excel document) is bedoeld als instrument voor het management van de organisatie. Het management vult de tool in, zelfstandig of met behulp van alle afdelingen, en kan de uitkomsten gebruiken als gespreksonderwerp om privacy naar een hoger niveau te tillen in de organisatie. Gezien de landelijke ontwikkelingen en het huidige volwassenheidsniveau op het gebied van privacy in de Drechtsteden wordt aanbevolen om deze tool in te vullen en te gebruiken om privacy beter te borgen in de organisaties.

Positionering Functionaris Gegevensbescherming

In de vorige rapportages is ingegaan op de positionering van de FG. De benodigde vaststelling van de het Reglement Functionaris voor de gegevensbescherming Drechtsteden heeft nog steeds niet plaatsgevonden. Een nieuwe functiebeschrijving van de FG is wel vastgesteld. De transitie naar Dordrecht geeft ook weer zorgen voor het komende jaar in verband met de benodigde onafhankelijke positionering. De FG wordt bij de overgang opnieuw geplaatst bij de gemeente Dordrecht, die vanaf 1 januari 2021 servicegemeente voor de overige Drechtsteden gemeenten is. Het is van belang dat de (wettelijk verplichte) onafhankelijke positie van de FG vanaf 1 januari 2022 geborgd wordt.

Aanbeveling

Borg de onafhankelijke uitvoering van de FG taken door vaststelling van een FG Reglement en een juiste positionering per 1 januari 2022. Voor de huidige situatie is ook vaststelling van een Reglement noodzakelijk.

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."*

Te vaak nog wordt aan deze informatieverplichting door de organisaties voorbij gegaan. Dat betreft met name het niet of te laat informeren van de FG over belangrijke aangelegenheden. 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 verantwoordelijke en gaat ten koste van het beschermen van de privacybelangen van de betrokkenen.

Aanbeveling

Onderzoek hoe kan worden geborgd dat de FG wordt geïnformeerd in de gevallen waarin dit in de AVG bedoeld is.

Samenwerkingsverbanden

Regelmatig worden persoonsgegevens in samenwerkingsverbanden gedeeld. Te denken valt bijvoorbeeld aan het delen van gegevens binnen het RIEC, het Veiligheidshuis of de districtelijke ondermijningstafel. Op grond van de AVG is in deze gevallen doorgaans het houden van een DPIA verplicht. De Autoriteit Persoonsgegevens heeft dit expliciet opgenomen in de lijst die zij hiervoor heeft vastgesteld:

Een DPIA is verplicht wanneer sprake is van het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (zoals gegevens over gezondheid, verslaving, armoede, problematische schulden, werkloosheid, sociale problematiek, strafrechtelijke gegevens, betrokkenheid van jeugdzorg of maatschappelijk werk) met elkaar uitwisselen, bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

Tot nu toe heeft alleen de Burgemeester van Dordrecht een DPIA afgerond die mede betrekking had op het verwerken van gegevens binnen dergelijke samenwerkingsverbanden. Op dit moment zijn er hoge risico's aanwezig op het delen van de gegevens binnen deze samenwerkingsverbanden, omdat nog niet alle verantwoordelijken de benodigde DPIA's hebben uitgevoerd. Daarnaast heeft dit inhoudelijk ook gevolgen, omdat er verschillende knelpunten bestaan in de juridische rechtmatigheid voor het structureel delen van gegevens binnen deze samenwerkingsverbanden. Er is wel een wetsvoorstel aanhangig bij de eerste kamer (al meer dan een jaar) die het laatste knelpunt deels kan oplossen. Het is echter nog maar de vraag of, en met welke inhoud, deze wordt goedgekeurd door de eerste kamer.

Aanbeveling

Inventariseer in welke samenwerkingsverbanden gegevens worden gedeeld. Houdt de noodzakelijke DPIA's op de gegevensdelingen in deze samenwerkingsverbanden.

De gemeentelijke infrastructuur en digitale toepassingen

In 2020 vond er een (ethische) hack plaats van stoplichten in de gemeente Dordrecht. Het bleek dat deze hack mogelijk was geworden door de toepassing van een app bedoeld om fietsers indien mogelijk een groene golf te geven op de stoplichten. Bij deze app werden alleen gepseudonimiseerde persoonsgegevens verwerkt. De impact van een mogelijke hack zal dan ook vooral groot zijn op de infrastructuur en slechts in beperkte mate op persoonsgegevens. Dat neemt niet weg dat de informatiebeveiliging en tevens de bescherming van persoonsgegevens, bij de keuze van de gemeente om de infrastructuur ter beschikking te stellen aan particuliere ondernemingen, niet was meegenomen. Te verwachten valt dat dergelijke verzoeken in de toekomst steeds meer zullen voorkomen. Het is dan ook verstandig om beleid te maken op keuzes om (delen van) de infrastructuur voor IoT achtige toepassingen beschikbaar te stellen, waarbij privacy en informatiebeveiliging standaard worden meegenomen.
De gemeente zelf past ook steeds meer digitale technieken toe, waarbij persoonsgegevens worden verwerkt in de openbare ruimte. Het bekendste voorbeeld is de groei van het gebruik van camera's. Daarbij blijkt echter dat verantwoordelijkheden van burgemeester, politie en particulieren en de verschillende doeleinden van het cameratoezicht (openbare orde en veiligheid, bescherming van goederen) niet altijd goed gescheiden zijn. DPIA's zijn niet (altijd) (van te voren) uitgevoerd en de burger wordt niet (altijd) (afdoende) geïnformeerd. Ook ontbreekt het aan een overkoepelende visie op het gebruik van camera's of IoT toepassingen en de risico's hiervan voor de betrokkenen.

Aanbeveling

Formuleer een beleidsvisie op het inzetten van IoT en andere digitale toepassingen in de openbare ruimte waarbij persoonsgegevens worden verwerkt. Denk in het bijzonder aan het gebruik van camera's, waarbij enerzijds de ethische en rechtmatige aspecten worden beschouwd en anderzijds een afwegingskader wordt geformuleerd. Dit afwegingskader gaat in op het belang van de toepassing en het nadelige effect van de inbreuk op de persoonlijke levenssfeer van de burger (betrokkene).

AFAS HR systeem

Per 1 januari 2021 is het HR systeem gewijzigd van ADP naar AFAS. AFAS is een externe verwerker. De implementatie van AFAS is verzorgd door het Service Centrum Drechtsteden. Het SCD is ook verantwoordelijk voor het beheer van het systeem.

Tijdens de voorbereiding van de migratie is ooit wel gestart met het uitvoeren van een DPIA, maar deze is tot op heden niet afgerond. De wettelijke verplichte FG advisering op dit onderdeel heeft dan ook nog steeds niet kunnen plaatsvinden. Daarmee voldoen alle organen binnen de regio, die aangemerkt kunnen worden als werkgever, niet aan hun wettelijke verplichting daartoe.

Bij het live gaan van AFAS bleek dat met name op het gebied van de verschillende autorisaties en het gebruik van BSN-nummers de inrichting niet compliant was aan de AVG. Het gevolg was een serie datalekken en een aantal maatregelen die achteraf zijn genomen. Deze hadden voorkomen kunnen worden indien de wettelijk verplichte DPIA tijdig was gehouden.

Hierbij bleek het ook nog een complicerende factor, dat het SCD verwerker is voor de gemeenten, en dat er geen wettelijk verplichte verwerkersovereenkomst is tussen gemeenten en de GRD-SCD. De rolverdeling verwerker - verwerkingsverantwoordelijke is daardoor niet vastgelegd en in de praktijk wordt deze ook niet gevolgd. Het is immers een verplichting van alle verantwoordelijken (dus de werkgevers) om de DPIA tijdig in te dienen en de noodzakelijke maatregelen te nemen. De verantwoordelijken hebben dan ook in dit proces hun verantwoordelijkheid zoals deze in de wet is vastgelegd niet genomen.

De FG vindt het zorgelijk dat door de werkgevers voor de verwerking van zoveel gevoelige persoonsgegevens van werknemers niet de wettelijke verplichte procedure is gevolgd. Het was geen verassing dat deze overgang van ADP naar AFAS zou plaatsvinden en dat het houden van een DPIA wettelijk verplicht was. Tussen werknemers en werkgever bestaat geen gelijke verhouding, waardoor een werknemer extra afhankelijk is van de naleving van de privacyregels door de werkgever. De werkgever zou hiermee rekening moeten houden en juist extra zorgvuldig moeten handelen.

Aanbevelingen[1]

- Rond alsnog het DPIA proces af en leg deze ter advisering voor aan de FG. Accepteer daarna officieel de overgebleven risico's en beleg de te nemen maatregelen.
- Werk nauw samen met AFAS om de resterende problematiek op te lossen.
- Sluit een verwerkersovereenkomst tussen de GRD en de afnemers.
- Zorg als verwerker dat de verwerkingsverantwoordelijken juist worden geïnformeerd en neem als verantwoordelijke de rol en verplichtingen die daarbij horen.
- Evalueer de toepassing van de AVG bij de implementatie van AFAS en stel aan de hand hiervan een lijst met aanbevelingen dan wel eisen op, te volgen bij een volgend inkoop-, migratie- of implementatietraject van een systeem met persoonsgegevens.

[1] Deze aanbevelingen gelden momenteel voor de GRD, maar vanaf 1 januari 2022 ook voor GR Sociaal.

Centric

Binnen de regio wordt voor de essentiële dienstverlening gebruik gemaakt van systemen en software van Centric. Binnen deze systemen worden enorme hoeveelheden gegevens, waaronder bijzondere en gevoelige persoonsgegevens, verwerkt.

Vanuit verschillende signalen van verschillende organisaties is naar voren gekomen dat Centric zelfs test met productiegegevens. Daarvoor is geen verwerkersovereenkomst gesloten. Daarnaast zou geen verwerkersovereenkomst zijn gesloten voor overige dienstverlening waarvoor dat wel noodzakelijk is.

Aanbevelingen[2]

- Breng in kaart voor welke verwerkingen Centric moet worden aangemerkt als verwerker van de verschillende verantwoordelijken in de regio. Sluit hiervoor de benodigde verplichte verwerkersovereenkomst.
- Breng in kaart of het testen met productiegegevens door Centric op grond van privacy en informatiebeveiliging regelgeving überhaupt is toegestaan en breng de risico's hiervan in kaart.

Sociaal Domein

In het afgelopen jaar is naar voren gekomen dat de taakverdeling tussen de gemeenten en de Sociale Dienst verschillende privacy risico's met zich meebrengt. Er wordt allereerst niet altijd gewerkt conform hetgeen is afgesproken in de Gemeenschappelijke Regeling Drechtsteden. Gemeenten voeren nu deels taken uit waarvoor de juridische bevoegdheid ontbreekt, omdat deze taken formeel gedelegeerd zijn aan de Sociale Dienst Drechtsteden.

Ook in de gevallen waarin de taakverdeling tussen de SDD en gemeenten wel conform de Gemeenschappelijke Regeling plaatsvindt, is deze dusdanig ingewikkeld ingericht dat dit bij een aantal onderwerpen om nauwe afstemming en samenwerking vraagt. Dit zal naar verwachting alleen maar toenemen, in het kader van de huidige transitie.

De komst van de Wams zal voor 2022 van die samenwerking het uiterste vragen. Juist als er ook een transitie plaatsvindt, is er een groot risico dat verantwoordelijkheden en taken door elkaar gaan lopen. Ook nu al zijn er een aantal processen (vergelijk onder meer de zgn. Aandachtshuishoudens, oftewel Multi-Problematiek Gezinnen) die op basis van toestemming plaatsvinden, terwijl de AP in het verleden heeft aangegeven deze grondslag niet toereikend te vinden.

Aanbevelingen

- breng de gevolgen van de transitie en de komst van de Wams voor het Sociaal Domein in beeld;
- zorg voor een goede inrichting van taken en verantwoordelijkheden en een goede uitvoering van de bescherming van persoonsgegevens in de nieuwe situatie;
- stem processen die deels door de gemeente en deels door de Sociale Dienst worden uitgevoerd goed op elkaar af, zodat de privacy zo goed mogelijk geborgd is en er geen rechtsongelijkheid ontstaat.

[2] Deze aanbevelingen gelden momenteel voor de GRD, maar vanaf 1 januari 2022 ook voor GR Sociaal.

Overzicht Datalekken

Bevindingen

Bij Alblasserdam hebben zich in de periode van 1 april 2020 tot en met 1 april 2021 4 datalekken voorgedaan. Hierbij ging het om de volgende type datalekken:

a)	Persoonsgegevens verstuurd aan verkeerde ontvanger	2
b)	Verkeerd verzonden post of email	0
c)	Brief of postpakket kwijtgeraakt of geopend retour ontvangen	0
d)	Persoonsgegevens gedeeld met onbevoegde personen	0
e)	Persoonsgegevens per ongeluk toegankelijk	0
f)	Overig	2

Van de 4 datalekken zijn er 4 gemeld bij de Autoriteit Persoonsgegevens. Alle 4 de datalekken zijn binnen de termijn van 72 uur gemeld bij de Autoriteit Persoonsgegevens. Daarmee wordt voldaan aan de AVG.

Evenals vorig jaar en het jaar ervoor is de FG van oordeel dat dit aantal datalekken voor een organisatie als gemeente Alblasserdam erg laag is. Enerzijds is dat positief, anderzijds kan het ook het gevolg zijn van het niet onderkennen of herkennen van een datalek. Een beveiligingsincident is namelijk al snel een datalek.

Aanbevelingen

Wees scherp op het signaleren en melden van datalekken. Naast dat het niet melden van datalekken significante gevolgen kan hebben, bieden datalekken namelijk ook een uitgelezen kans om verbeterpunten te identificeren, de bewustwording (verder) te vergroten, en processen waar nodig aan te scherpen.

Conclusie

De wil om te verbeteren is zichtbaar aanwezig bij de gemeente Alblasserdam, of in ieder geval bij een aantal betrokken medewerkers. Er zijn veel processen in werking gezet, maar de gemeente voldoet helaas op geen van de onderzochte punten aan alle wettelijke verplichtingen. Dit zal met name het gevolg zijn van de zeer beperkte capaciteit die het afgelopen jaar beschikbaar is geweest. De verbetering valt vooral te behalen op het inzichtelijk maken van informatie en het periodiek monitoren hiervan. De gemeente is nog niet in control als het gaat om de implementatie van privacy en dit is een groot risico voor de gemeente en inwoners.

Veel van deze punten zijn geen nieuwe aandachtspunten ten opzichte van voorgaande jaren. Het is dan ook van belang dat de gemeente Alblasserdam het komende jaar investeert op de mogelijke verbeterpunten die benoemd zijn in de rapportage.