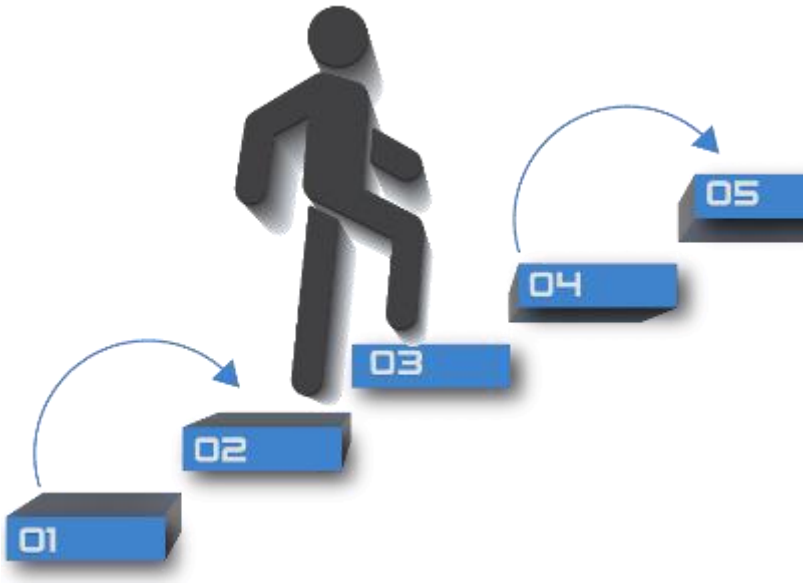
Jaarrapportage gegevensbescherming



Omgevingsdienst Zuid-Holland Zuid

april 2020 – april 2021

Functionaris Gegevensbescherming

Inhoud

Inleiding

De OZHZ heeft in antwoord op de vragenlijst van de jaarlijkse audit door de FG een uitgebreide documentatie overlegd. Hierin is op verwerkingsniveau inzicht te krijgen van de verschillende verwerkingen van persoonsgegevens die binnen OZHZ plaats hebben. Tevens blijkt uit de documentatie en de praktijk van het afgelopen jaar, dat de governance van de privacy verantwoordelijkheden binnen de OZHZ op orde is. Beide zaken gecombineerd geven een beeld van een organisatie die in elk geval "in control" is, dat wil zeggen overzicht heeft over de feiten en in staat is om ook te acteren vanuit welomschreven rollen en verantwoordelijkheden.
Dat wil niet zeggen dat alle AVG facetten even goed zijn geregeld. Met name als het gaat om de definitie van de potentieel hoog risico verwerkingen, het uitvoeren van DPIA's, en de maatregelen die nodig zijn naar aanleiding van de wijzigingen in de Wet Politiegegevens zijn nog verbeteringen noodzakelijk.

Het schenden van de persoonlijke levensfeer van burgers, het (onbewust) discrimineren en volgen van burgers en het slordig omgaan met gegevensbescherming heeft het vertrouwen van de burger in de overheid het laatste jaar de nodige schade berokkend. Het is ook meermaals gebleken dat in de veelheid van de verwerkingen die als gevolg van de digitale transformatie alleen maar groter wordt, een dergelijke schending van de AVG maar al te makkelijk plaats heeft en (enige tijd) onopgemerkt blijft. Hierbij valt te denken 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 op het internet bij fraudeonderzoek door gemeenten en politie. De laatste twee tonen ook hoezeer de betrokken organisaties de maatschappelijke impact van hun handelen hebben onderschat, omdat in hun ogen voldoende maatregelen waren genomen om schadelijke effecten voor de burger te voorkomen. Dat toont hoe belangrijk het is om na te denken over de potentiële risico's en in de huid van de betrokkene te kruipen wanneer de OZHZ als verantwoordelijke moet inschatten of het gaat om een hoog risico verwerking, die wellicht een DPIA en/of specifieke voorlichting vereist. Ondanks de degelijke basis die is gelegd blijft dus het devies: scherp blijven, emphatisch blijven en blijven verbeteren.

Strikt genomen geen onderwerp voor deze rapportage, is het evident en bij het OZHZ bekend dat er nog het een en ander moet worden geregeld naar aanleiding van de Wet Politiegegevens (Wpg) die toeziet op de verwerking van persoonsgegevens die aangemerkt kunnen worden als politiegegevens. Met name door het in dienst hebben van Buitengewoon Opsporings Ambtenaren (BOA's) en de specifieke handhavingstaak van de OZHZ, is dit een belangrijk privacy dossier. Zo is het van belang te komen tot de verplichte audits en het regelen van een FG die toeziet op de Wpg. Over deze te nemen maatregelen naar aanleiding van de Wpg gaat deze rapportage verder niet in.

Resultaten Audit

Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten is het register waarin alle werkprocessen van het Omgevingsdienst Zuid-Holland-Zuid 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 in de rapportage periode zijn doorgegeven.

Bevindingen

- OZHZH geeft aan dat het register van verwerkingsactiviteiten compleet en actueel is.
- Het register is in de rapportageperiode niet gewijzigd.
- Er wordt aangegeven dat het register actualisering behoeft op enkele onderwerpen, waarbij worden genoemd het benoemen van de BIO als opvolger van de BIG, het bezien van niet primaire processen op actualiteit, het bezien van veranderingen in processen en systemen. Deze aanpassingen zijn gepland om te worden uitgevoerd in 2021.
- Er is een duidelijke verantwoordelijke voor het bijhouden van het register.
- Er is een procedure vastgesteld dat regelt wanneer het register moet worden gewijzigd. (Werkinstructie Actueel houden Register van verwerkingen AVG Unit SER).
- De procedure voor wijzigingen borgt dat het register doorgaans als compleet en actueel kan worden beoordeeld.

Aanbevelingen

Het register maakt een goede indruk en voldoet voor wat betreft het scheppen van inzicht ruim aan de wettelijke eisen.

- Borg en controleer dat de benoemde actualisering in 2021 ook daadwerkelijk plaats vindt. Idealiter zou bij elke verandering deze zo snel mogelijk moeten worden gemuteerd, aangezien het register de daadwerkelijke, actuele situatie behoort weer te geven.
- Alhoewel niet wettelijk verplicht, verdient het wel aanbeveling om in het register op te nemen bij welke verwerkingen ook gegevens worden verwerkt die behoren onder de Wet Politiegegevens (Wpg).

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 werkinstructies zijn opgesteld, wie verantwoordelijk is en wie 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 is een lopend proces met werkinstructies voor de rechten van betrokkenen. Deze is opgenomen voor alle rechten van betrokkenen in de werkinstructie 'Join Proces AVG verzoek inzage persoonsgegevens'. Tevens biedt de informatie in het Register van Verwerkingen inzicht in de te volgen werkwijze.
- In het proces en de werkinstructie is vastgelegd wie, in welke stap welke taken moet uitvoeren.
- Het in 2020 gegeven advies om werkinstructies te vervaardigen voor elk door betrokkenen uit te oefenen recht, is opgevolgd.

- Het is voor betrokkene mogelijk om zich middels Digi-D te identificeren. De website is hierop aangepast.
- Er is één verzoek tot uitoefening van een recht in behandeling genomen en in overleg met de betrokkene is deze afgehandeld.

Aanbevelingen
Geen. De procedure is duidelijk ingericht, door het gebruik van Digi-D en een speciaal webformulier is een verzoek indienen laagdrempeling voor betrokkene en wordt de identiteit zorgvuldig vastgesteld.

Overeenkomsten in verband met het delen van persoonsgegevens

Verwerkersovereenkomsten zijn een belangrijk instrument om de privacy en bescherming van persoonsgegevens te garanderen als een (deel van) een werkproces is uitbesteed. Op grond van artikel 28 van de AVG moeten schriftelijke afspraken worden gemaakt wanneer de verantwoordelijke persoonsgegevens laat verwerken door een verwerker. Doorgaans wordt hier een verwerkersovereenkomst voor afgesloten. 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.

Bevindingen
- De OZHZ heeft een register voor de verwerkersovereenkomsten opgesteld. Hierin zijn 22 verwerkers opgenomen.
- In de rapportageperiode zijn zes verwerkersovereenkomsten afgesloten. De verwerkersovereenkomst die afgesloten dient te worden met het Service Centrum Drechtsteden (SCD) is onderhanden en bijna gereed. Een verwerkersovereenkomst met Squit (Roxit) zal worden afgesloten tijdens de migratie van het systeem.
- Verwerkersovereenkomsten worden opgeslagen in JOIN, bij voorkeur samen met de hoofdovereenkomst.
- Het afsluiten van verwerkersovereenkomsten is een doorlopend proces bij nieuwe hoofdovereenkomsten.
- OZHZ is deelnemer aan het convenant Meldpunt Zorg en Overlast binnen de regio, een overeenkomst in de zin van Artikel 26 AVG (gezamenlijke verantwoordelijkheid).
- OZHZ is van mening dat zij voor de taken die zij uitvoert als verantwoordelijke moet worden aangemerkt en niet als verwerker. Er zijn om die reden geen verwerkersovereenkomsten afgesloten voor de dienstverlening van OZHZ.

Aanbevelingen

- De ingerichte procedures zijn ruim voldoende ten opzichte van de wettelijke verplichting.
- Onderzoek of er nog verwerkingen zijn waarbij OZHZ een gezamenlijke verwerkingsverantwoordelijkheid heeft die (nog) niet is onderkend. Denk bijvoorbeeld aan samenwerking bij fraude onderzoek in RIEC verband.
- Het is goed om een (eventueel automatische) koppeling te hebben tussen het Register van Verwerkingen en dat van de verwerkersovereenkomsten, zodat je het direct waarneemt als in het RvV een verwerker wordt genoemd die niet in het laatste overzicht blijkt te zijn opgenomen. Dit was nu in een enkel geval aan de hand.
- Onderzoek of OZHZ voor geen van de taken die zij uitvoert als verwerker moet worden aangemerkt. Hiervoor is tot dusver verwezen naar een 2,5 jaar oud advies van de VNG / Pels Rijcken. Neem bij de te maken analyse "Guideline 2020/7 controller and processor" van de European Protection Data Board in ogenschouw. Deze bevat de meest recente inzichten.

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. Binnen de BIO is het ook een vereiste dat nieuwe medewerkers binnen drie maanden een training krijgen op het gebied van privacy en informatiebeveiliging. In deze audit is ingegaan op de vraag of er een dergelijk programma is opgezet, voor zowel bestaande als nieuwe medewerkers.

Bevindingen
Door de OZHZ word aangegeven dat de volgende activiteiten hebben plaatsgevonden

- OZHZ haakt aan bij het trainings- en bewustwordings-programma van de Drechtsteden, zoals de e-learningsmodules en verspreiding van communicatiemateriaal.
- Er zijn uren opgenomen voor medewerkers binnen het dienstbrede opleidingsprogramma.
- Bij indiensttreding van medewerkers legt men de eed of belofte af en is er een gesprek met de directeur en de contactpersoon integriteit. Het omgaan met persoonsgegevens is onderdeel van het integriteitsbeleid en de bijbehorende gedragscodes.
- Via berichten op SID wordt regelmatig gewezen op het zorgvuldig omgaan met persoonsgegevens, meestal als de actualiteit (in de media of naar aanleiding van eigen datalekken of andere informatie) daartoe aanleiding geeft.
- De OZHZ zal zien hoe en wanneer voldaan kan worden aan de gestelde BIO-eis.[1]
- Proceseigenaren van processen waarin persoonsgegevens worden verwerkt, zijn op de hoogte van hun AVG-verantwoordelijkheden.
- Gesprekken met proceseigenaren omtrent verwerking van persoonsgegevens worden momenteel op ad-hoc basis gevoerd, naar aanleiding van een gebeurtenis zoals een datalek.

Aanbevelingen

- Borg in een procedure dat nieuwe medewerkers de eerste drie maanden verplicht worden geïnformeerd conform de BIO-eis. Meet de aanwezigheid van medewerkers.
- Houd bij hoeveel van de medewerkers de eLearning volgen en afronden.
- Voer de gesprekken met proceseigenaren met AVG-verantwoordelijkheden niet op ad hoc basis, maar borg dat deze collega's minstens twee keer per jaar de kans krijgen in een gesprek of een kleine bijeenkomst hun vragen te stellen en kennis op peil te houden v.w.b.t. de AVG.
- Zorg voor mogelijkheden voor privacy functionarissen zowel qua capaciteit als qua scholingsmogelijkheden.

Governance

Om structureel de onderwerpen privacy en gegevensbescherming te waarborgen, 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 voorzien is in capaciteit voor deze taken.

[1] Artikel 7.2.2.2 BIO: Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.

Bevindingen

- Binnen het Management wordt gesproken over privacy bij vaststelling van officiële stukken, zoals het beleid (privacy en informatiebeveiliging) en bij de jaarrekening als integraal onderdeel van de bedrijfsvoering.
- Bij gebeurtenissen wordt gecommuniceerd met het voltallige personeel via het intranet.
- Er is een privacy coördinator, die ondersteuning heeft van een jurist en een medewerker informatiebeveiliging. Met de GRD is contractueel dienstverlening geregeld van het Juridsch Kenniscentrum en de Functionaris en Adviseur Gegegevensbescherming.
- De unitmanager zijn op de hoogte van hun verantwoordelijkheid, evenals de directeur.
- De privacy coördinator bewaakt de behandeling van privacy aspecten in de vergaderingen van het management, daar deze tevens directiesecretaris is.

Aanbevelingen

De Governance is in de basis goed geregeld. Wel zij nog verwezen naar de positie van FG, die in de regiobrede risico's wordt besproken.

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 het Omgevingsdienst Zuid-Holland-Zuid een privacyverklaring heeft, en of - en op welke wijze - deze vrij beschikbaar is.

Bevindingen

- De OZHZ heeft een privacyverklaring.
- De privacyverklaring is voor een ieder te vinden op www.ozhz.nl/privacy
- Op het informatiepaneel bij de receptie is de privacyverklaring ook te lezen voor alle bezoekers van de OZHZ.
- Er is een aparte privacy verklaring voor het personeel.
- Het Register van Verwerkingen is openbaar en kan door iedereen worden gedownload vanaf de website.
- De OZHZ geeft aan dat het aan betrokkenen specifiek voorlichting geven over hoog risico verwerkingen en/of algoritmen niet aan de orde is, omdat deze verwerkingen zich niet voordoen.
- In basis is de voorlichting over de gegevensbescherming goed geregeld. Met het openbaar zetten van het Register van Verwerkingen behoort de OZHZ tot de voorhoede als het gaat om transparantie richting de burger. Dat is zeer positief.

Aanbevelingen

- Het is belangrijk in het oog te houden dat een 'hoog risico' verwerking, en ook het gebruik van een algoritme, zich eerder voordoet dan je denkt. Bekijk waar de privacyverklaring moet worden aangevuld zodat ook voldoende specifieke informatie wordt gegeven. 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.

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
OZHZ geeft het volgende aan

- De unitmanagers zijn verantwoordelijk voor het zorgvuldig omgaan met persoonsgegevens. Indien nodig zorgen zij ervoor dat een DPIA wordt uitgevoerd, met ondersteuning van de privacycoördinator, de medewerker informatiebeveiliging van de unit INF en het SCD. Het is bekend dat ook de FG er dan bij betrokken moet worden.
- Er zijn nog geen DPIA's uitgevoerd. OZHZ geeft aan dat er BRA's (Basis Risico Analyse) zijn uitgevoerd, met de conclusie dat het uitvoeren van een DPIA niet nodig is.
- Bij deze B.R.A.'s is vooral gekeken naar het "netto risico", dat wil zeggen het risico na het nemen van maatregelen.
- De verwachting is dat de OZHZ één verplichte DPIA moet en zal uitvoeren, namelijk naar aanleiding van het invoeren van het systeem "Squit 20/20".
- Het OZHZ geeft aan de landelijke richtlijnen te volgen en de sjablonen van de Drechtsteden te volgen v.w.b.t. de BRA's en DPIA's.

Aanbevelingen

- Kijk kritischer naar het bruto risico voor betrokkenen bij het uitvoeren van BRA's en DPIA's, waarbij het "bruto risico" is bedoeld als zijnde het potentieel risico, dus zonder de inachtneming van maatregelen. De bruto risico's voor het nemen van maatregelen bepalen immers of een DPIA op een proces/verwerking noodzakelijk is. Dit is ook belangrijk voor de verantwoording en evaluatie van de al genomen maatregelen.
- Kijk tevens kritischer naar de lijst en richtlijnen van de Autoriteit Persoonsgegevens, bijvoorbeeld bij het gebruik van (mobiele) camera's of het doen van (heimelijk) onderzoek en gevolgen voor betrokkenen. Op die manier, is het de inschatting van FG, zullen nog enkele verwerkingen in aanmerking komen voor een DPIA. Een lijst met potentieel hoog risico verwerkingen die in het oog springen voor de FG is bij OZHZ ingeleverd.

Privacy door Ontwerp en Standaardinstellingen

Privacy door ontwerp en bij standaardinstellingen is opgenomen in AVG artikel 25, als één van de eerste verantwoordelijkheden voor verantwoordelijken.

De Europese Commissie omschrijft het principe van privacy door ontwerp als volgt:

"*Ondernemingen/organisaties worden aangemoedigd om in het vroegste stadium van het ontwerp van de verwerkingsactiviteiten de technische en organisatorische maatregelen te treffen die nodig zijn om de beginselen inzake privacy en gegevensbescherming vanaf het begin te waarborgen („gegevensbescherming door ontwerp"). Standaard moeten ondernemingen/organisaties ervoor zorgen dat persoonsgegevens worden verwerkt met het hoogste niveau van privacybescherming(bijvoorbeeld alleen de noodzakelijke gegevens worden verwerkt, korte opslagperiode, beperkte toegankelijkheid) zodat*

persoonsgegevens standaard niet toegankelijk zijn voor een onbeperkt aantal personen („gegevensbescherming door standaardinstellingen").[2]

Bevindingen
De OZHZ geeft de volgende bevindingen van toegepast privacy door ontwerp aan:

- Uitvraag ICT-dienstverlening aan het SCD
- Uitvraag datawarehouse OCD waarbij gegevens over ziekteverzuim niet op persoonsniveau worden ingevoerd.

Daarnaast geeft de OZHZ voorbeelden uit eerdere jaren:
- Afscherming BSN in de systemen van OZHZ voor medewerkers die er niet functioneel mee werken.
- Verwijdering passage in aanvraagformulieren van lokale vergunningen waarbij om een kopie van het ID-bewijs wordt gevraagd.
- In de ICT uitvraag aan het SCD staat bijvoorbeeld:
  - "Er moet voldaan worden aan de wettelijke eisen die gelden vanuit de AVG. Dit geldt dus ook als de File dienstverlening gebaseerd zou worden op een public cloud/SaaS-oplossing."
  - "Opdrachtnemer dient de Beheerde ICT-dienst zo te hebben ingericht dat zij Opdrachtgever ondersteunt en in staat stelt om te voldoen aan haar informatiebeveiligingsbeleid (zie appendix C1 en C2 en alle relevante wet- en regelgeving, zoals AVG en de BIO-norm (Baseline Informatiebeveiliging Overheid), HKZ-norm en NEN-7510. Dit dient u ook te kunnen aantonen indien Opdrachtgever een externe controle ondergaat."
- Met zo'n uitvraag kan OZHZ dan de rechtenstructuur zelf naar behoren invullen. Voorheen was dat bijv. bij Squit niet mogelijk. De leverancier heeft toen op verzoek aanpassingen gedaan m.b.t. de BSN-velden. OZHZ bepaalt nu zelf met een extra profiel welke medewerkers nog wel kennis kunnen nemen van het BSN.

Aanbevelingen
Blijf privacy door ontwerp in het oog houden bij het de migratie van Squit en eventuele andere implementaties van applicaties. Handel daarbij per proces vanuit de geëigende rol (verwerkingsverantwoordelijke of verwerker).

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.

[2] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_nl

De organisaties zijn er in een van de vorige rapportages al op gewezen dat zij een groter risico lopen, omdat de Autoriteit Persoonsgegevens al voor één van de organisaties expliciet erop heeft gewezen dat deze normen bestaan, en moeten worden toegepast.
Uit navraag is gebleken dat er op het gebied van Mobile Device Management en het begrip Bring Your Own Device geen actueel beleid is (het laatste beleid is van 2014). Het is momenteel mogelijk om eigen mobiele devices zonder maatregelen (MDM) te gebruiken voor werkdoeleinden. Er zijn enkele maatregleen genomen in de Outlook App, maar er is geen gedegen risico analyse verricht waaruit blijkt of deze maatregelen afdoende zijn. Er is geen duidelijk standpunt ingenomen over BYOD en zijn er geen eisen gesteld aan de inrichting van de privacyaspecten. Ook is het niet duidelijk of het SCD beleid smartphones, het enige relevante beleidstuk ons bekend, is geimplementeerd.
De aanbeveling van vorig jaar: "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.

Bevindingen

- OZHZ heeft 184 smartphones waarvan er 52 geen MDM hebben.
- OZHZ heeft 102 tablets waarvan er 50 geen MDM hebben.
- Door OZHZ wordt de volgende maatregel genomen: "Op devices waarop geen MDM zit is tweefactor-authentification van toepassing. Daarnaast wordt gebruik gemaakt van bitlock voor versleuteling van gegevens op toestellen zonder MDM. Bij uitlevering wordt toegelicht hoe om te gaan met informatiebeveiliging. Wat mag je wel en niet doen? En hoe ga je om in bepaalde situaties?"

Aanbevelingen
Stel voor EDM (Endpoint Device Management, waarvan MDM deel uitmaakt) schriftelijk beleid vast, en implementeer dit beleid, zowel voor zakelijke mobiele gegevensdragers, als voor 'eigen' devices van medewerkers. Draag er zorg voor dat het EDM beleid borgt dat er voldoende informatiebeveiliginsmaatregelen op mobile devices worden genomen, waarbij als minimaal uitgangspunt de aanbeveling van vorig jaar wordt genomen.

Thuiswerken en MS Teams

Als gevolg van de maatregelen in het kader van de bestrijding van de Covid-19 pandemie, 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 client software bij de thuiswerkers op de fysieke werkplek, waarmee de externe verbinding tot stand wordt gebracht. Daarnaast zijn andere informatiedragers (printers in de thuisomgeving bijvoorbeeld) buiten beeld.

Bevindingen
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. Bij navraag bij de verwerker van het OZHZ op dit punt, het SCD, kon deze niet worden overlegd.
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.

Aanbevelingen
Maak in overleg en met medewerking van de verwerker 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

Positionering FG

Bevindingen
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 vastgesteld.
- De transitie naar Dordrecht geeft ook zorgen voor het komende jaar in verband met de benodigde onafhankelijke positionering.

Aanbevelingen

Borg de onafhankelijke uitvoering van de FG taken door vaststelling van het Reglement en een juiste positionering. Ook dit is een Drechtsteden brede taak. Met name doordat de gemeente Dordrecht, als service gemeente, een aantal taken op het gebied van verwerking van persoonsgegevens voor andere gemeenten en organisaties zal gaan uitvoeren als verwerker in de zin van de AVG, en de FG is aangesteld in deze processen door zowel de verwerkingsverantwoordelijke als de verwerker, terwijl de belangen van deze partijen niet (altijd) parallel lopen, is het noodzakelijk de onafhankelijkheid van de FG te borgen door deze goed te positioneren en een reglement vast te stellen waarin deze onafhankelijkheid nog verder geborgd wordt. De onafhankelijkheid van de FG is een expliciete wettelijke verplichting.

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
OZHZ heeft vorig jaar de FG middels het privacy coördinatoren overleg en soms rechtstreekse contacten enkele keren goed geïnformeerd. Ook de overlegde documentatie bij de rapportage is afdoende compleet. Desondanks is bijvoorbeeld bij de casus van de "beveiligingscamera's en tags" zoals die door de OZHZ bij de rapportage is meegeleverd, geen contact gezocht met de adviseur gegevensbescherming of de FG.

Aanbevelingen
Wees er bewust van dat de informatieverplichting aan de FG daadwerkelijk een verplichting is. Tevens is het juist in gevallen als de overlegde casus goed in de FG een partij te hebben die onafhankelijk is en een objectieve inschatting van de risico's van betrokkenen kan maken. Onderzoek hoe kan worden geborgd dat de FG wordt geinformeerd in de gevallen waarin dit in de AVG bedoeld is.

Privacy beleid Drechtsteden

In de vorige rapportage is de organisatie-brede aanbeveling gedaan om het privacybeleid aan te passen. Voor de inhoud wordt u verwezen naar de rapportage van vorige jaar. Een nieuw privacybeleid is door de OZHZ vastgesteld.

Aanbevelingen
Geen.

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.

Bevindingen
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 lopen de verantwoordelijken binnen de regio hoge risico's op het delen van de gegevens binnen deze samenwerkingsverbanden. Allereerst omdat de wettelijk verplichte DPIA's niet zijn gehouden, en meer inhoudelijk 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, maar het is nog maar de vraag of, en met welke inhoud, deze gaat worden goedgekeurd door de eerste kamer.

Aanbeveling
Inventariseer in welke samenwerkingsverbanden gegevens worden gedeeld. Houdt de noodzakelijke DPIA's op de gegevensdelingen in deze samenwerkingsverbanden. Volg de ontwikkelingen rondom de Wet Gegevensdeling Samenwerkingsverbanden.

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. Het SCD is een verwerker van de OZHZ.

Bevindingen
- Tijdens de voorbereiding van de migratie is door het SCD wel gestart met het uitvoeren van een DPIA, maar deze is (nu nog steeds) niet afgerond. De wettelijke verplichte FG advisering op dit onderdeel heeft dan ook nog steeds niet plaats kunnen vinden. Daarmee voldoen alle organen binnen de regio, die aangemerkt kunnen worden als werkgever en verwerkingsverantwoordelijke, niet aan hun wettelijke verplichting.
- 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. 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

- Rond alsnog het DPIA proces af en leg deze ter advisering voor aan de FG. Accepteer daarna offcieel 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.

Overzicht Datalekken

Het overzicht datalekken wordt voor de OZHZ bijgehouden door de adviseurs gegevensbescherming van het SCD. Datalekken worden in eerste instantie ook door hen opgepakt en in overleg met de OZHZ afgehandeld.

Bevindingen
In de periode van 1 april 2020 tot en met 1 april 2021 hebben zich 7 datalekken voorgedaan waarbij de OZHZ de veroorzaker was. Hierbij ging het om de volgende type datalekken:

a)	per ongeluk publiceren van persoonsgegevens:	
b)	diefstal of vermissing van gegevensdragers:	
c)	verkeerd ingerichte autorisaties/rechten:	1
d)	het geopend retour ontvangen van brieven of postpakketten:	
e)	Persoonsgegevens verstuurd/geplaatst naar/bij de verkeerde ontvanger:	6

Van deze datalekken zijn van vier datalekken melding bij de Autoriteit Persoonsgegevens gedaan, allen binnen de daartoe geldende maximale termijn van 72 uur na ontdekking van de inbreuk.

Er zijn interne mitigerende maatregelen genomen naar aanleiding van de datalekken.

De FG is van oordeel dat dit aantal datalekken voor een organisatie als de OZHZ zeker niet als (te) hoog is aan te merken. Het melden van deze datalekken wordt gezien als een goede uitwerking van het bewustzijn wanneer iets als datalek aangemeld moet worden, en welk proces dan moet worden gevolgd.

Aanbeveling
- Houdt deze positieve trend in het melden van datalekken vast. Zorg ervoor dat de werknemers datalekken blijven herkennen en melden. Blijf passende maatregelen nemen indien dit mogelijk (b)lijkt.

Conclusie

De Omgevingsdienst Zuid-Holland-Zuid heeft goede stappen gezet op het gebied van de naleving van de AVG. De OZHZ is er op de meeste onderdelen goed van op de hoogte waar zij staat op het gebied van de gegevensbescherming en heeft deze informatie ook goed beschikbaar.

Enkele onderwerpen vormen echter nog aandachtspunten voor de OZHZ. Over deze punten zijn in de rapportage aanbevelingen gedaan. Geadviseerd wordt om deze aanbevelingen op te pakken.