Bestuursnotitie

Datum 25 augustus 2020

Onderwerp Jaarrapportage Privacy & Gegevensbescherming OZHZ april 2020 – april 2021 van de Functionaris Gegevensbescherming

Bijgaand treft u de Jaarrapportage Privacy & Gegevensbescherming OZHZ april 2020 – april 2021 van de Functionaris Gegevensbescherming (FG). De FG heeft deze opgesteld op basis van de door OZHZ aangeleverde beantwoording van de vragenlijst 'privacy audit 2021', aangevuld met eigen constateringen. Dit onderzoek is ook uitgevoerd bij de gemeenten in de Drechtsteden, de Gemeenschappelijke regeling Drechtsteden (GRD) en de Dienst Gezondheid en Jeugd.

De FG concludeert dat OZHZ in antwoord op de vragenlijst van de jaarlijkse audit een uitgebreide documentatie heeft 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 privacyverantwoordelijkheden binnen 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.

De FG benoemt ook een aantal verbeterpunten en doet daarvoor aanbevelingen. Ten eerste specifiek voor OZHZ (zie paragraaf 1), ten tweede regio (= Drechtsteden) breed (zie paragraaf 2). OZHZ gaat in deze bestuursnotitie in op de genoemde verbeterpunten. De reactie van OZHZ is in de tekst hierna steeds cursief aangegeven. Ten behoeve van de leesbaarheid zijn teksten (samengevat) overgenomen uit de rapportage van de FG.

1. Aanbevelingen van de FG voor OZHZ

Register van verwerkingen

Het register maakt een goede indruk en voldoet voor wat betreft het scheppen van inzicht ruim aan de wettelijke eisen. Aanbeveling is om de benoemde actualisering in 2021 ook daadwerkelijk plaats te laten vinden. 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).

OZHZ actualiseert het register van verwerkingen in 2021. Ook de registratie van persoonsgegevens onder de Wpg wordt opgenomen. De implementatie van de Wpg loopt op dit moment. In 2021 voert een extern bureau de verplichte audit uit.

Overeenkomsten in verband met het delen van persoonsgegevens

Op grond van artikel 28 van de AVG moeten schriftelijke afspraken worden gemaakt wanneer de verantwoordelijke persoonsgegevens laat verwerken door een verwerker (verwerkersovereenkomsten). OZHZ heeft een register voor de verwerkersovereenkomsten opgesteld. Hierin zijn 22 verwerkers opgenomen. In de rapportageperiode zijn 6 verwerkersovereenkomsten afgesloten. De verwerkersovereenkomst met het SCD inmiddels is gesloten, als eerste van de klantorganisaties van het SCD. De tekst dient als model voor de andere Drechtstedenorganisaties om te komen tot een verwerkersovereenkomst met het SCD (en vanaf 1 januari 2022 met de gemeente Dordrecht).

Aanbeveling van de FG is om te onderzoeken of er nog verwerkingen zijn waarbij OZHZ een gezamenlijke verwerkingsverantwoordelijkheid heeft die (nog) niet is onderkend. Ook doet de FG (wederom) de aanbeveling te onderzoeken of OZHZ voor bepaalde taken toch als verwerker zou moeten worden aangemerkt.

OZHZ gaat bij elke nieuwe samenwerking met andere partijen na of en hoe persoonsgegevens worden uitgewisseld. Daarover worden dan afspraken gemaakt in de samenwerkingsovereenkomst of in een verwerkersovereenkomst (als sprake is van een externe verwerker). Bij actualisering van het register van verwerkingen zal OZHZ nagaan of met alle externe verwerkers daadwerkelijk een verwerkingsovereenkomst is aangegaan. De FG heeft daarvoor enkele voorbeelden aangereikt.

Landelijk is nog steeds het uitgangspunt dat omgevingsdiensten 'verwerkingsverantwoordelijke' zijn, en geen 'verwerkers'. Op hoofdlijnen is de redenering als volgt: het uitgangspunt in de wetgeving is dat sprake is van een verwerkersrelatie indien de dienstverlening betrekking heeft op het verwerken van persoonsgegevens. Zodra de gegevensverwerking echter een uitvloeisel is van een andere vorm van dienstverlening, is de dienstverlener zelf verantwoordelijk voor de gegevensverwerking. In het geval van omgevingsdiensten ziet de dienstverlening op het uitvoeren van VTH-taken in opdracht van gemeenten en provincie, en dus niet op het verwerken van persoonsgegevens. In het geval dat het verwerken van persoonsgegevens een 'bijproduct' is van de dienstverlening, is de dienstverlener (omgevingsdienst) zelf verantwoordelijk (en dus geen verwerker). OZHZ zal bezien of de recent beschikbaar gekomen Guideline tot andere inzichten leidt en hierover afstemmen met de Zuid-Hollandse omgevingsdiensten en wellicht ook met OmgevingsdienstNL.

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 Baseline Informatiebeveiliging Overheden (BIO) is het ook een vereiste dat nieuwe medewerkers binnen drie maanden een training krijgen op het gebied van privacy en informatiebeveiliging.

De FG doet de aanbeveling om in een procedure te borgen dat nieuwe medewerkers de eerste drie maanden verplicht worden geïnformeerd conform de BIO-eis. Aanbeveling is ook om met

de proceseigenaren met AVG-verantwoordelijkheden binnen de organisatie (i.e. de unitmanagers) afspraken te maken om niet alleen op ad hoc basis (bijvoorbeeld naar aanleiding van een datalek) maar ook meer structureel het omgaan met persoonsgegevens te bespreken.

OZHZ heeft naar aanleiding van de audit intern actie ondernomen voor het (verplicht) volgen van de e-learning modules. Iedereen, zowel nieuw als zittend personeel, wordt geacht dit in 2021 te doen. Het is nu ook expliciet opgenomen in het onboardingsprogramma voor nieuwe medewerkers. In het kader van het actualiseren van het register van verwerkingen zal met de unitmanagers worden gesproken over hun verantwoordelijkheden in het kader van de AVG.

DPIA's (data protection impact assessments)

(D)PIA's zijn een belangrijk instrument om vooraf de privacyrisico's van een bepaalde verwerking of proces in beeld te brengen, en daar vervolgens maatregelen op te nemen. De FG constateert dat OZHZ nog geen DPIA's heeft uitgevoerd. Voor een aantal gegevensverwerkingen is wel een Basis Risico Analyse (BRA) uitgevoerd, met de conclusie dat het uitvoeren van een DPIA niet noodzakelijk is. Bij de overgang naar een ander VTH-systeem zal OZHZ in elk geval een DPIA uitvoeren. De voorbereidingen daarop zijn al gestart. OZHZ volgt in deze de landelijke richtlijnen en de sjablonen van de Drechtsteden voor wat betreft de BRA en DPIA.

Aanbeveling van de FG is om kritischer te kijken 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. Daarnaast kunnen de lijst en richtlijnen van de Autoriteit Persoonsgegevens worden gebruikt. Een lijst met potentieel hoog risicoverwerkingen die in het oog springen voor de FG is bij OZHZ aangeleverd.

OZHZ heeft met de FG al besproken wat wordt bedoeld met het 'bruto risico' van een verwerking. Met het actualiseren van het register van verwerkingen kan worden bezien bij welke verwerkingen aanvullend een DPIA noodzakelijk is. OZHZ zal de van de FG verkregen informatie daarin meenemen.

2. Regiobrede bevindingen aanbevelingen van de FG

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

Bij het gebruik van mobiele apparaten moeten passende technische en organisatorische maatregelen worden genomen. Hoe gevoeliger de gegevens, des te meer technische en organisatorische maatregelen moeten worden genomen. Er is binnen de Drechtsteden ook geen actueel beleid op het gebied van Mobile Device Management (MDM) en het begrip Bring Your Own Device. Het is daarom nu mogelijk om eigen mobiele devices zonder maatregelen (MDM) te gebruiken voor werkdoeleinden.

Constatering bij OZHZ is dat de dienst 184 smartphones heeft waarvan er 52 geen MDM hebben. OZHZ heeft 102 tablets waarvan er 50 geen MDM hebben. OZHZ heeft toegelicht dat op devices waarop geen MDM zit tweefactor-authentification van toepassing is. Daarnaast wordt gebruik gemaakt van bitlock voor versleuteling van gegevens op toestellen zonder MDM. Bij uitlevering wordt toegelicht hoe om te gaan met informatiebeveiliging. Er is sprake van een uitsterfconstructie. Aanbeveling van de FG is om voor EDM (Endpoint Device Management, waarvan MDM deel uitmaakt) schriftelijk beleid vast te leggen en te implementeren.

OZHZ merkt op dat EDM/MDM al onderdeel is van het eigen informatiebeveiligingsbeleid. Op operationeel niveau blijkt het echter lastig er goede uitvoering aan te geven. SCD beziet thans de verschillende varianten van MDM. Daarover moeten besluiten worden genomen waarna het verder kan worden uitgerold. OZHZ werkt niet met BYOD.

Thuiswerken en MS Teams

Bij het thuiswerken wordt gebruikgemaakt 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. De FG is van mening dat 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. De FG doet daarom de aanbeveling om samen met het SCD een (Drechtstedenbrede) impactanalyse op te stellen voor het thuiswerken als geheel en MS-Teams in het bijzonder.

OZHZ zal de aanbeveling bespreken met andere partijen binnen de Drechtsteden. Bij de uitrol van het nieuwe werkconcept is expliciet aandacht aan informatieveilig werken en gebruik van de beschikbaar gestelde devices. Het werken binnen en buiten de GRID-omgeving is dan een belangrijk aandachtspunt. Uitgangspunt is dat OZHZ-medewerkers alleen binnen de GRID-omgeving werken. Bij het gebruik van MS-teams buiten de GRID-omgeving geldt dat met dit programma geen (gevoelige) (persoons) gegevens of bestanden worden gedeeld. Overleggen worden ook niet opgenomen en bewaard, met uitzondering van een enkele digitale presentatie (webinar) die medewerkers van OZHZ verzorgen voor gemeenten en provincie. Ook dan worden geen (gevoelige) (persoons) gegevens gewisseld en vooraf wordt altijd gecommuniceerd of een bijeenkomst wordt opgenomen.

Positionering van de FG

De FG heeft zorgen over de onafhankelijke positionering van de FG, met name vanwege de taakuitvoering per 1 januari 2022 door de gemeente Dordrecht. Voor de taken op het gebied van de Wpg is nog geen FG aangewezen.

OZHZ heeft de overgang van de FG-functie naar Dordrecht al aangekaart in het kader van het aangaan van een nieuwe dienstverleningsovereenkomst met het SCD/Dordrecht. Ook binnen het overleg van privacycoördinatoren in de Drechtsteden is het aangekaart. In het kader van de transitie wordt het meegenomen.

Met de FG is al een eerste gesprek gevoerd over de Wpg. Alternatief is dat OZHZ de FG voor de gegevensverwerkingen in het kader van de Wpg samen met de 4 andere omgevingsdiensten in Zuid-Holland organiseert of op de markt inkoopt. Naar aanleiding van de externe audit die nu loopt pakt OZHZ dit actiepunt verder op.

Privacybeleid Drechtsteden

Het DB heeft in 2020 het actuele privacybeleid en informatiebeveiligingsbeleid vastgesteld. Vanwege de uitvoering van de Wpg zal OZHZ eind 2021 of begin 2022 een addendum agenderen in het bestuur.

Samenwerkingsverbanden

Regelmatig worden in de regio 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, omdat sprake is van het delen van bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard, bijvoorbeeld in wijkteams, veiligheidshuizen of informatieknooppunten.

Constatering van de FG is dat tot nu toe alleen Dordrecht een DPIA heeft afgerond die mede betrekking had op het verwerken van gegevens binnen dergelijke samenwerkingsverbanden. Aanbeveling is om in de regio te inventariseren in welke samenwerkingsverbanden gegevens worden gedeeld en de noodzakelijke DPIA's te doen.

OZHZ is alert op het delen van persoonsgegevens in samenwerkingsverbanden. Thans spelen in de regio onder andere vraagstukken in het kader van de samenwerking bij het aanpakken van ondermijning. De FG en de AVG-adviseurs van het SCD zijn bij dit traject betrokken.

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 SCD. Het SCD is ook verantwoordelijk voor het beheer van het systeem. Het SCD is een verwerker van OZHZ. 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.

Aanbeveling van de FG is daarom de DPIA alsnog af te ronden en deze ter advisering voor te leggen aan de FG. Zowel de werkgevers (als verwerkingsverantwoordelijke) als het SDC (als verwerker) moeten daarin hun rol en verantwoordelijkheid pakken.

OZHZ is van mening dat hierover, via het Netwerk MT-Middelen, goede afspraken moeten worden gemaakt met het SCD. De betrokken werkgevers zullen dit gezamenlijk agenderen.

Overzicht datalekken OZHZ

In de periode van 1 april 2020 tot en met 1 april 2021 hebben zich 7 datalekken voorgedaan bij OZHZ. De FG is van oordeel dat dit aantal datalekken voor een organisatie als de OZHZ zeker niet als (te) hoog is aan te merken. Aanbeveling is om deze positieve trend in het melden van datalekken vast te houden.

Het privacybewustzijn binnen OZHZ is hoog. Datalekken worden (snel) herkend en door de betrokken medewerker snel gemeld bij het SCD. Regelmatig brengt OZHZ deze verplichting en de geldende afspraken/procedure onder de aandacht bij de medewerkers. Ook in de e-learningmodules is er aandacht voor.