JAARRAPPORTAGE GEGEVENSBESCHERMING

van de Functionaris Gegevensbescherming

Alblasserdam

2022

Samenvatting

Deze rapportage over 2022 voor de gemeente Alblasserdam is opgesteld door de Functionarissen Gegevensbescherming de heren Commandeur en De Vries. Vanaf 1 november 2022 nemen zij tijdelijk deze rol waar ter vervanging van de vorige FG die per 1 november 2022 een andere functie heeft aanvaard.

Deze rapportage is gebaseerd op een door de Privacy Coördinator van de gemeente Alblasserdam ingevulde vragenlijst alsook de eigen ervaringen (gesprekken, bestudering documenten) door de FG's zelf.

Uit de rapportage komt naar voren dat de gemeente Alblasserdam op weg is naar een hoger volwassenheidsniveau qua aandacht voor privacy en invoering van de AVG. Uit de rapportage blijkt echter ook dat een aantal essentiële basisonderdelen ontbreken of onvolledig zijn. Het gaat dan met name om:

- Actualisering Register van Verwerkingsactiviteiten en richt een proces in voor het beheer ervan;
- Volledigheid en juistheid inzake verwerkersovereenkomsten en overeenkomsten inzake gezamenlijke verantwoordelijkheid
- Inzicht in risicovolle verwerkingen en plannen/uitvoeren van DPIA's

Onze aanbevelingen:

- **Actualiseer het register van verwerkingen en richt een proces in om dit register tenminste jaarlijks te actualiseren;**
- **Inventariseer op basis van het register van verwerkingen voor welke verwerkingen nog een verwerkersovereenkomst moet worden afgesloten en sluit deze af;**
- **Inventariseer voor welke verwerkingen nog DPIA's moeten worden uitgevoerd, al dan niet herhaald, en stel een planning op voor de uitvoering hiervan;**

Aangezien dit basisonderdelen zijn voor het naleven van de AVG adviseren wij u aan de uitvoering van deze aanbevelingen in 2023 prioriteit toe te kennen. Daarmee kunnen onrechtmatige verwerkingen en mogelijke schade voor inwoners financiële risico's voor de gemeente worden voorkomen

Andere aanbevelingen betreffen:

- Evalueer het trainingsprogramma;
- Laat privacy regelmatig terugkomen tijdens een managementoverleg en laat de PC-er en FG hier bij aanschuiven. Neem privacy als vast item mee in de kwartaal-/halfjaarlijks-/jaarrapportages;
- Geef op een positieve wijze meer aandacht aan datalekken;
- Werk aan een volledig inzicht in de samenwerkingsverbanden;
- Aandacht voor inrichting sociaal domein (wijkteams en komst Wams per 1-1-2024).

Wet Politiegegevens

Nieuw is aandacht voor de verwerking van persoonsgegevens die onder de werking van de Wet Politiegegevens (Wpg) vallen. Het gaat om de verwerking van politiegegevens door de in dienst zijnde Boa's van de gemeente. De gemeente Alblasserdam heeft geen Boa's in dienst. Deze werkzaamheden zijn uitbesteed aan MBAll en de gemeente hoeft volgens het oordeel van de externe auditor derhalve niet aan deze verplichting te voldoen. Graag worden wij hierover nader geïnformeerd aangezien MBAII een commerciële organisatie is en het voor ons onduidelijk is in hoeverre zij direct verantwoordelijk zouden zijn voor deze publiekrechtelijke gegevensuitwisseling in het Politiedomein.

Register van Verwerkingsactiviteiten

Het Register van Verwerkingsactiviteiten is het register waarin alle werkprocessen van de gemeente 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

De gemeente Alblasserdam maakt gebruik van de diensten van de gemeente Dordrecht inzake het bijhouden van het Register van Verwerkingsactiviteiten. Hiertoe is de software-applicatie iNavigator ingericht. Via dit systeem is op basis van gemeentelijke processen een versie van alle gemeentelijke verwerkingsactiviteiten te genereren. De output is echter niet geactualiseerd en bovendien beperkt tot processen die in de iNavigator voorkomen. Hierdoor is er geen volledig en actueel zicht op de verwerkingsactiviteiten van de gemeente. Dit is in strijd met de AVG en dient zo spoedig mogelijk te worden opgepakt. De wettelijke verplichting in deze bestaat al vanaf 2018 en is boetewaardig.

Ook is dit register nodig voor het vaststellen van de verplichte DPIA's (zie verderop in deze rapportage).

Een Register van Verwerkingsactiviteiten dient te worden overlegd aan de Autoriteit Persoonsgegevens indien daar naar wordt gevraagd. Als FG hebben wij inzage gekregen in het register van de gemeente alleen wel met de mededeling dat deze niet is geactualiseerd. Dit kan een probleem vormen indien derden (betrokkenen, Autoriteit Persoonsgegevens) hier om vragen.

Aanbevelingen:

Ga met voorrang over tot het actualiseren van het Register van Verwerkingsactiviteiten. Dit is nodig om ook andere onderdelen die hierna komen (verwerkersovereenkomsten, dpia's) goed in beeld te krijgen en te houden.

Werk aan een te publiceren versie van het Register van Verwerkingsactiviteiten. Dit is weliswaar niet wettelijk verplicht vanuit de Algemene Verordening Gegevensbescherming, maar draagt wel bij aan de transparantie vanuit de organisatie naar betrokkenen en derden toe. Op grond van de Wet open overheid is het overigens denkbaar dat het register (op termijn) actief openbaar moet worden gemaakt.

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

De procedures inzake het afhandelen van verzoeken om uitoefening van de rechten van betrokkenen zijn ingericht. Er zijn over 2022 geen verzoeken ingediend.

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. 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.
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.
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

Uit de beantwoording van de vragen blijkt dat de gemeente geen volledig zicht heeft op afgesloten en af te sluiten verwerkersovereenkomsten. Voor zover processen juist en volledig in iNavigator zijn opgenomen is er een beeld van de aanwezige en benodigde verwerkersovereenkomsten. Indien deze dus niet zijn opgenomen in iNavigator ontbreekt dit inzicht. Wel zijn de afgesloten overeenkomsten opgenomen in een aparte applicatie AddVue.

Aangegeven is dat er geen zicht is op mogelijke overeenkomsten waar sprake is van een gezamenlijke verantwoordelijkheid. Ook hier ontbreekt het inzicht. Ook hiervoor geldt dat het juist en volledig opnemen van de processen in iNavigator kan helpen het zicht te krijgen opdat ook op dit onderdeel voldaan wordt aan de AVG.

Aanbevelingen:

Ga met voorrang over tot het actualiseren van het Register van Verwerkingsactiviteiten in iNavigator waardoor ook een beter en goed overzicht ontstaat inzake de volledigheid rond verwerkersovereenkomsten en overeenkomsten inzake gezamenlijke verantwoordelijkheid.

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 gemeente beschikt over een trainings- en bewustwordingsprogramma voor nieuwe medewerkers die voldoet aan de BIO-vereisten. Geen directe bijzonderheden.

Alle collega's, zowel nieuw als de in dienst zijnde , kunnen zich aanmelden voor aangeboden trainingen en e-learnings via SkillsTown. Daarnaast wordt regionaal gezocht naar een passende invulling voor de gehele regio op het gebied van Privacy en Informatieveiligheid.

Aanbevelingen:

Wij stellen voor het huidige programma in 2023 te evalueren op haar werking en zo nodig bij te stellen.

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

Binnen de gemeente Alblasserdam is in de periode 2022 inzichtelijk gemaakt wat nodig is op het gebied van Privacy en Informatiebeveiliging. Eind 2022 is hiervoor formatie beschikbaar gesteld waardoor dit onderdeel geborgd is. Het is van belang dat ‘privacy’ wordt gezien als een eerste verantwoordelijkheid voor de procesverantwoordelijken. Niet de privacy coördinator (dit is ‘slechts’ een ondersteunende staf-functie) maar de procesverantwoordelijken zijn direct verantwoordelijk en aanspreekbaar op het juist uitoefenen van de AVG-wetgeving binnen hun processen. Dit geldt dan voor zaken als:

- Het up to date houden van het register van verwerkingsactiviteiten
- Het afsluiten van verwerkersovereenkomsten en overeenkomsten gezamenlijke verantwoordelijkheid
- Voorkomen en leren van data-lekken
- Uitvoeren van DPIA’s

Let wel: de hierboven genoemde zaken zijn ‘boetewaardig’ vanuit de AP. Het is dan aan het management/de procesverantwoordelijke om hier tekst en uitleg aan te geven. Niet de privacy coördinator.

Aanbevelingen:

Bespreek met management en procesverantwoordelijken op welke wijze privacy bewustzijn beter tot zijn recht kan komen. Doe dit door bijvoorbeeld eens per kwartaal privacy als agendapunt vast te leggen en te bespreken in de daarvoor aanwezige overleggen. Neem privacy ook op als vast onderdeel van de kwartaal-/halfjaarlijks-/jaarrapportages binnen de organisatie.

Privacyverklaring:

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 gemeente Alblasserdam *een privacyverklaring heeft, en of - en op welke wijze - deze vrij beschikbaar is. Daarnaast is het van belang dat de betrokkene afdoende geïnformeerd wordt over (hoog risico) verwerkingen en/of het gebruik van automatische besluitvorming.*

Bevindingen

De privacyverklaring van de gemeente op de website en de papieren versie voldoet in algemene zin en geeft informatie over wat de gemeente met gegevens van betrokkenen (meestal inwoners) doet. Verbeteringen zouden bereikt kunnen worden door voor bepaalde specifieke processen (ondermijning, adresonderzoek, sociaal domein) extra toelichtingen op te nemen.

Aandachtspunt: kijk naar het begrip bijzondere gegevens. De uitleg (met onder andere vermelding financiële gegevens, bsn) sluit niet aan bij wat de AVG onder bijzondere gegevens verstaat.

De privacyverklaring wordt regionaal opgesteld en vervangen door een gelaagde verklaring.

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

Binnen de gemeente Alblasserdam zijn de tools (processen, richtlijnen) aanwezig om de DPIA’s tijdig uit te voeren. Dit gebeurt echter te weinig. Voor nieuwe risicovolle verwerkingen dient voor de verwerking van persoonsgegevens een DPIA te worden uitgevoerd. Gebeurt dit niet dan is dit in strijd met de AVG en kan hiervoor een boete worden opgelegd.

Lopende processen waarin persoonsgegevens worden gebruikt worden inzichtelijk gemaakt in een overzicht, met daarbij de vermelding DPIA nodig ja/nee, DPIA afgerond ja/nee inclusief de

restrisico's. Hierbij wordt het overzicht aangevuld met de DPIA's met hoog risico vanuit het verwerkingenregister I-Navigator. Vanuit daar wordt gewerkt en wordt een prioritering aangebracht.

Aanbevelingen:

Zorg in navolging van het actualiseren van het Register van Verwerkingsactiviteiten zo spoedig mogelijk voor een volledig overzicht van risicovolle verwerkingen waarvoor een DPIA is voorgeschreven en stel een planning op om tot uitvoering hiertoe over te gaan. Stel hiervoor indien nodig de nodige (financiële) middelen beschikbaar.

Organisatorische en technische maatregelen

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.

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

Voor wat betreft de informatiebeveiliging sluit de gemeente aan bij de gemeente Dordrecht samen met andere Drechtsteden. Van hieruit dient te worden voldaan aan de BIO-normen die voor gemeenten gelden. Voor dit onderdeel verwijzen wij hier naar de rapportage van de CISO van de gemeente.

Datalekken

Bevindingen

Het aantal datalekken binnen de gemeente Alblasserdam is met vier over geheel 2022 spaarzaam te noemen. Dit roept de vraag op of er wel voldoende aandacht voor dit onderwerp is. Het melden van een datalek is voor de betrokken medewerkers altijd een lastige zaak maar wel noodzakelijk om lering uit te trekken voor de gehele organisatie. Wellicht is het te overwegen hier positief mee om te gaan (reik een boekenbon uit voor de eerste tien gemelde datalekken bijvoorbeeld).

De vier gemelde datalekken over 2022 (waarvan geen gemeld bij de AP) geven geen aanleiding tot het maken van op- of aanmerkingen.

Aanbevelingen:

Ga na of het melden van datalekken op een positieve wijze meer aandacht kan krijgen. Het is een belangrijk onderdeel om te leren van fouten binnen de organisatie.

Samenwerkingsverbanden:

Bevindingen

Binnen het samenwerkingsverband Drechtsteden maar ook daarbuiten wordt veel samen opgetrokken door meerdere gemeenten. Dit is op zich een prima zaak. Het is echter van belang om goed zicht te hebben en te houden op deze samenwerkingsverbanden.

Aanbevelingen:

De privacy coördinator en de FG's dragen zorg voor een goed inzicht in de samenwerkingsverbanden en waar zij qua toezicht verantwoordelijk voor zijn.

Sociaal Domein:

Bevindingen

De meeste taken voor wat betreft uitvoering van de Participatiewet, Jeugdwet, Wmo2015 en Wet gemeentelijke schuldhulpverlening zijn gedelegeerd (soms geheel en gedeeltelijk gemandateerd) aan de GRS en de DJG. Binnen de gemeente zelf zijn wijkteams aanwezig. Voor de FG's is het niet duidelijk onder welke juridische voorwaarden qua gegevensverwerking deze zijn ingericht. Voor de duidelijkheid: er kan veel mits goed ingericht. Hier moet duidelijkheid in komen. Een DPIA op dit gebied kan uitkomst bieden.

Verder willen wij hier uw aandacht vragen voor de komst van de Wet Aanpak Meervoudige problematiek Sociaal Domein (Wams). Deze gaat naar verwachting per 1 januari 2024 in en geeft de gemeenten de mogelijkheid om meervoudige casussen te bespreken in persoonsgegevens in deze uit te wisselen waar dit nu binnen de huidige wetgeving een vaak te grote uitdaging is. Hiertoe zullen op gemeenteniveau proces- en werkafspraken moeten worden gemaakt over wat dit betekent voor de inrichting van de organisatie van het sociaal domein. Een impact analyse dus. Wij vragen uw aandacht hiervoor.

Aanbevelingen:

Ga aan de hand van een DPIA na hoe de wijkteams (toegang) binnen het sociaal domein opereren en zorg voor de juist juridische inbedding van deze wijkteams indien nodig.

Ga na wat de impact is van de komst van de Wams voor de gemeente Alblasserdam.

Positionering FG

Bevindingen

In 2022 heeft het adviesbureau BMC een advies uitgebracht over de positionering van de FG binnen de Drechtsteden-gemeenten en de OZHO. Hieruit is het advies naar voren gekomen om de adviestaken van de FG weer bij de FG te beleggen en naast de privacy-coördinatoren bij de gemeenten ook centrale juridische kennis (tweede lijns-ondersteuning) te beleggen bij het JKC van de gemeente Dordrecht. Begin 2023 wordt hierover besloten waarna de functie voor FG wederom zal worden opengesteld voor werving.