Werkorganisatie Duivenvoorde

Privacybeleid

WERKORGANISATIE DUIVENVOORDE

Inhoudsopgave

1. Inleiding

De Werkorganisatie Duivenvoorde, hierna WODV heeft persoonsgegevens nodig om haar taken uit te kunnen voeren. Zonder de verwerking van persoonsgegevens is het onmogelijk om bijvoorbeeld aan personeel een uitkering van salarissen te doen. De medewerker moet er hierbij op kunnen vertrouwen dat de werkorganisatie zorgvuldig en veilig met zijn persoonsgegevens omgaat. De verwerking van persoonsgegevens kan risico's met zich meebrengen. Zo kan het voorkomen dat er meer dan noodzakelijk persoonsgegevens van de personeel worden verwerkt, wat kan leiden tot een inbreuk op de persoonlijke levenssfeer. Dat risico kan nog vergroot worden naarmate er meerdere soorten persoonsgegevens worden verzameld. Dit is met name van toepassing op het verwerken van bijzondere persoonsgegevens zoals gezondheidsgegevens.
Een ander risico is dat er persoonsgegevens bij derden terecht komen. Dit kunnen andere medewerkers of inwoners zijn die niet bij de verwerking betrokken zijn. Dat zou bijvoorbeeld tot identiteitsfraude kunnen leiden. Hierbij kan het voorkomen dat de medewerker zich in zijn of haar rechten geschonden voelt als de informatie onbedoeld bekend wordt bij anderen. Het voorkomen daarvan is een belangrijk motief voor het zorgvuldig omgaan met persoonsgegevens.

Het privacybeleid zal moeten bijdragen aan de bewustwording van de AVG binnen en buiten de WODV. Dit houdt in dat er bewust zorgvuldig persoonsgegevens worden verwerkt indien noodzakelijk en zorg dragen dat de betrokkenen goed geïnformeerd zijn over de wijze waarop persoonsgegevens worden verwerkt en de rechten van de betrokkenen.

Met het privacybeleid streven wij als gemeente en daarbij ook de raad en de griffie ernaar dat een ieder zorgvuldig binnen het kader van de AVG persoonsgegevens verwerkt.

2. Principes AVG

Persoonsgegevens worden steeds meer in digitale vorm vastgelegd. Dat stelt nieuwe eisen aan de manier waarop er met persoonsgegevens moet worden omgegaan. Pas als sprake is van een gerechtvaardigd, duidelijk omschreven, doel mogen persoonsgegevens worden verzameld. Er mogen niet meer persoonsgegevens worden verzameld dan nodig zijn om het vooraf omschreven doel te bereiken. De werkorganisatie is verplicht om te zorgen voor passende (technische en organisatorische) maatregelen om de persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking. De werkorganisatie moet ervoor zorgen dat deze digitale persoonsgegevens afdoende worden beveiligd tegen verlies en onrechtmatige toegang (hacks) zodat de privacy zo optimaal mogelijk wordt beschermd. Het zogenaamde lekken van data moet door de werkorganisatie worden voorkomen. Daarvoor neemt de werkorganisatie maatregelen op het gebied van informatieveiligheid en dataminimalisatie. In het kader van de informatieveiligheid zorgt de werkorganisatie voor bewustzijn bij haar medewerkers als het gaat om de goede omgang met persoonsgegevens en zorgt zij voor technische middelen ter bescherming van persoonsgegevens . Dataminimalisatie houdt in dat alleen die persoonsgegevens worden verzameld die noodzakelijk zijn om het doel te realiseren waarvoor de persoonsgegevens worden verzameld.

Aanleiding voor dit privacy-beleid is de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018. Met de AVG is sprake van een versterking en uitbreiding van privacy-rechten van inwoners en ontstaan er meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens, worden uitgebreid.

Feitelijk is de verantwoordingsplicht (‘accountability’) het centrale begrip binnen de AVG. Het is opgenomen in artikel 5 AVG. De essentie van de verantwoordingsplicht is dat de verwerkingsverantwoordelijke (bij gemeenten in de meeste gevallen het college van burgemeester en wethouders) verantwoordelijk is voor het naleven van deze beginselen, en dat ook kan aantonen. Dus niet de burger hoeft aan te tonen of de WODV een fout heeft gemaakt, maar de WODV moet aantonen geen fout te hebben gemaakt.

<u>De 6 principes zijn:</u>

1. Rechtmatigheid, behoorlijkheid, transparantie: De WODV mag niet in strijd met de wet handelen, moet behoorlijk handelen en voor betrokkenen duidelijk maken en zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Alle communicatie richting betrokkenen moet begrijpelijk zijn, ook met betrekking tot de rechten van betrokkenen.
2. Doelbinding: Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld, en vervolgens alleen verder verwerkt worden wanneer er sprake is van een verenigbaar doel.
3. Minimale gegevensverwerking (‘ dataminimalisatie’): Er mogen niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is voor het doel. Verder moet steeds worden gekeken of het doel niet op een minder ingrijpende wijze kan worden bereikt (dit zijn de principes van proportionaliteit en subsidiariteit).
4. Juistheid: Het is van belang dat voortdurend moet worden nagegaan of de persoonsgegevens die de WODV van betrokkenen verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn moeten ze door de WODV gewijzigd of verwijderd worden.
5. Opslagbeperking: Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel van de verwerking.
6. Integriteit en vertrouwelijkheid: De WODV dient te zorgen voor een goede beveiliging van persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen. De WODV moet er voor zorgen dat ongeoorloofde toegang tot- en gebruik van persoonsgegevens voorkomen wordt.

In dit beleid wordt richting gegeven hoe de WODV om gaat met privacy. Zij laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de WODV (inclusief WODV) waarin persoonsgegevens worden verwerkt.

2.1 Bijzondere en gevoelige persoonsgegevens

Bijzondere persoonsgegevens en gevoelige persoonsgegevens spelen een belangrijke rol. Bijzondere persoonsgegevens worden in de AVG geregeld, in de praktijk speelt ook het ruimere begrip 'gevoelige gegevens' een rol.

Er worden in de AVG een aantal categorieën van bijzondere persoonsgegevens gehanteerd, die extra privacygevoelig zijn. Het betreft: ras of etniciteit, politieke opvattingen, religie/levensbeschouwing, vakbondslidmaatschap, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens betreffende seksualiteit.

Genetische en biometrische gegevens behoren tot de bijzondere persoonsgegevens. Bij biometrische gegevens moet gedacht worden aan een pasfoto op een rijbewijs of paspoort of een vingerafdruk. Deze gegevens worden enkel gebruikt om iemand te identificeren. Ook hier geldt dus: verwerking is verboden.

Strafrechtelijke gegevens behoren tot de bijzondere persoonsgegevens. Er wordt onder de AVG hiervoor een apart artikel 10 aan gewijd.

Onder gevoelige persoonsgegevens worden dus ten eerste de bijzondere persoonsgegevens gerekend. Daarnaast behoren financiële persoonsgegevens tot de gevoelige gegevens (bijvoorbeeld gegevens over schulden, salarisstroken, enz.). Verder vallen persoonsgegevens op grond waarvan mensen kunnen worden 'nagewezen' (stigmatisering), zoals bijvoorbeeld gegevens over een goksverslaving, ook onder gevoelige persoonsgegevens. Tenslotte worden wachtwoorden, inloggegevens, Inwonerservicenummers, kopieën van identiteitsbewijzen, en bankrekeningnummers tot de gevoelige gegevens gerekend. Indien iemand ten onrechte toegang krijgt tot deze gegevens, kan daarmee (identiteits)fraude gepleegd worden. Dat is een groot risico.

Van belang is dat ook al zou iemand vinden dat het niet erg is als een gevoelig persoonsgegeven bekend wordt ('ze mogen alles van me weten') niet relevant is bij de beoordeling of een persoonsgegeven gevoelig is.

Of een persoonsgegeven gevoelig van aard is speelt ook een rol bij de bepaling of de WODV persoonsgegevens die voor een bepaald doel zijn verzameld ook mag verwerken voor een ander doel. Hoe gevoeliger het persoonsgegeven, hoe minder snel de WODV mag en zal aannemen dat er sprake is van een verenigbaar doel.

3. Verantwoordelijkheden binnen de AVG

3.1 Verwerkingsverantwoordelijke

In de AVG wordt derhalve de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties (in de AVG aangeduid als 'verwerkingsverantwoordelijken') om te kunnen aantonen dat zij zich aan de wet houden (accountability). De verwerkingsverantwoordelijke is degene die alleen of samen met anderen het doel van en de middelen voor de verwerking vaststelt.

Het bestuur WODV is de verantwoordelijke die, ieder voor zover het hun taakuitoefening betreft, invulling geven aan de taken en verantwoordelijkheid die krachtens de AVG zijn toebedeeld aan de verwerkingsverantwoordelijke. Formeel is het bestuur van de WODV dan ook verantwoordelijk voor alle verwerkingen die onder de reikwijdte van de AVG vallen.

De verwerkingsverantwoordelijken zijn verantwoordelijk voor:

- De naleving van de beginselen voor de verwerking van persoonsgegevens.
- De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met dit beleidskader verordening wordt uitgevoerd.

Het bestuur van de WODV is privacy-verwerkingsverantwoordelijke voor een aantal bedrijfsvoeringsprocessen. In het verwerkingsregister wordt vastgelegd wie voor welk proces verantwoordelijk is.

3.2 Lijnmanagement en Privacy-Officer

De dagelijkse verantwoordelijkheid voor de zorgvuldige omgang met persoonsgegevens ligt (logischerwijze) bij de afdelingshoofden. Dat betekent dat de lijn zelf wordt aangesproken op het nakomen van de uit het privacy-beleid voortvloeiende eisen. Privacy is immers niet een op zichzelf staand iets, maar is onlosmakelijk verbonden met de dienstverlening. Het eigenaarschap van bepaalde processen en systemen waarmee wordt gewerkt, is belegd bij afdelingsmanagers. In die rol zijn zij verantwoordelijk voor het zorgvuldig beheer van alle gegevens in deze systemen, in het bijzonder voor persoonsgegevens, voor deugdelijke classificatie van gegevens en bijbehorende bescherming en voor het toekennen van rechten in deze systemen. Zij zijn verantwoordelijk voor het zodanig uitvoeren van het beleid dat privacy-risico's tot een minimum worden beperkt. De Privacy Officer (PO) biedt ondersteuning op het gebied van advisering bij het handelen conform het privacy-beleid en de privacy-administratie.

3.3 Functionaris voor de gegevensbescherming (FG)

De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. De FG ziet er op toe dat de organisatie voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij is een interne toezichthouder en toetst onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy, het privacy-beleid en informatiebeveiligingsbeleid. De FG is een onafhankelijke functionaris die de verwerkingsverantwoordelijke, het bestuur WODV rechtstreeks kan adviseren. De functie kent een beperkte overlap met de CISO, die zorg moet dragen voor een samenhangend pakket aan maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen een gemeente te waarborgen. De FG werkt samen met de CISO en de PO.

3.4 CISO

De Concern Informatie Security Officer (CISO) is verantwoordelijk voor het informatiebeveiligingsproces binnen het concern. De CISO stelt kaders op voor informatiebeveiliging en adviseert het bestuur en lijnmanagement hierover. De CISO houdt toezicht op de informatiebeveiligingsmaatregelen, waaronder persoonsgegevens, te beveiligen. De CISO werkt hierbij samen met de FG en PO.

3.5 Verantwoordingsplicht

De verantwoordingsplicht van de WODV, ook wel accountability genoemd, brengt met zich mee dat de WODV niet alleen de regels moet naleven, maar ook moet kunnen aantonen deze regels nageleefd te hebben.

In dit kader worden in ieder geval de volgende maatregelen getroffen:

1. Een actueel en volledig register van verwerkingen en het publiceren van een abstract van het register.

2. Opname in het verwerkingenregister van (een verwijzing) naar alle relevante documenten die betrekking hebben op de naleving van de verplichtingen uit de AVG, zoals informatieplicht en de afspraken met verwerkers.

3. Openbaarmaking van het onderhavige privacy-beleid.

4. Zorgen voor de aantoonbaarheid van de juiste behandeling van informatie. Tevens houdt de verantwoordingsplicht in dat de WODV een register van datalekken die zijn opgetreden, bijhoudt en, waar passend, een gegevensbeschermingseffect-beoordeling (DPIA) uitvoert.

NB. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is of toegestaan is.

4. Governance

Het bestuur van de WODV is integraal verantwoordelijk voor de bescherming van persoonsgegevens en de uitvoering van de AVG binnen de werkprocessen van de WODV en voor de WODV door de WODV. De specifieke rol van het college is het vaststellen van kaders en normen voor privacybescherming en het voldoen aan wet- en regelgeving (compliance) op dit gebied. Het bestuur van de WODV legt verantwoording af over uitvoering en handhaving van deze kaders en normen.

4.1 Privacy-administratie

Het systematisch vastleggen van verwerkingen van persoonsgegevens, het bewijs van effectieve werking van de getroffen beheers- en beveiligingsmaatregelen, en incidenten en datalekken dienen te worden opgenomen in een administratie. De leiding, het Bestuur, gebruikt de administratie voor het afleggen van verantwoording gegevensbescherming aan het maatschappelijk verkeer. Er is dus een privacy administratie nodig op basis waarvan de WODV de naleving van "de wet" kan aantonen (artikel 5.2 AVG, de verantwoordingsplicht/accountability).

4.2 Accountable

De WODV is accountable en verantwoord zich aan het maatschappelijk verkeer. Hierbij zijn 2 soorten te onderscheiden:

a. De betrokkenen (medewerkers) kunnen hun passieve en actieve rechten uitoefenen. Passieve rechten hebben voornamelijk betrekking op het door de WODV accountable zijn en dat aan de betrokkene informeren. Dus: de juiste informatie verstrekken, ook wel transparant zijn over de wijze van verwerken van persoonsgegevens. De betrokkene kan zijn / haar actieve rechten uitoefenen door vragen te stellen aan de WODV. Voor de betrokkene (medewerkers) is de FG met assistentie van de PO het eerste aanspreekpunt om mee te communiceren. Als die er niet is dan kan de betrokkene zich wenden tot de AP.
b. De WODV verantwoordt zich over hoe zij omgaat met privacy, wat haar beleid in deze is en verantwoordt zich achteraf over hoe dat is uitgevoerd.

4.3 Hoe zou de governance en compliance van de privacy georganiseerd moeten worden?

De planning en control cyclus is in essentie zo opgebouwd dat in het jaar t-1 (het jaar voor het begrotingsjaar) de voornemens worden opgesteld en de daarbij behorende middelen worden bepaald in de vorm van een kadernota of Perspectiefnota en vervolgens worden vastgesteld in de begroting. Met de vaststelling van de begroting wordt daarmee het ambitieniveau van een onderwerp voor het volgende jaar vastgelegd.

Na afloop van een jaar, in het voorjaar t+1, worden vervolgens een jaarverslag en jaarrekening opgesteld, waarmee door het bestuur van de WODV verantwoording over het afgelopen jaar wordt afgelegd.

4.4 De voornemens

Het governance- en compliance-model van privacy volgt dit stramien van de Planning en Control. Het start met het opstellen en vaststellen van Privacy-beleid, de voornemens worden in de begroting meegenomen en uiteindelijk is het dan onderdeel van het jaarverslag en jaarrekening als onderdeel van de algehele maatschappelijke verantwoording. In de loop van het jaar en na afloop van het jaar vindt evaluatie van het beleid plaats, die zo nodig tot aanpassing van het beleid kan leiden.
Het privacy-beleid, de voornemens, zal opgebouwd gaan worden aan de hand van een normenkader en een indeling in volwassenheidsniveau. Door het hanteren van volwassenheidsniveaus kan het privacy-beleid een groeimodel worden.

4.5 De vastlegging

Een belangrijke voorwaarde is dat de Privacy Organisatie gebruik maakt van een adequate administratie met overzicht en inzicht in het verantwoordelijkheids- en aansprakelijkheidsdomein van de WODV, actuele verwerkingen, een aan wet- en regelgeving gerelateerde normenset, bewijs van effectieve werking beheers- en beveiligingsmaatregelen, incidenten / datalekken en overzicht van besluiten van de feitelijk leidinggevenden alsmede uitkomsten van beheer. Een verwerkingenregister en een register van incidenten is reeds aanwezig. Het register van verwerkingen wordt geactualiseerd en zal ook daarna regelmatig een actualisatie behoeven. De andere administraties worden komende periode opgebouwd.

In situaties waarin het niet direct rechtstreeks duidelijk is of in een bepaalde situatie persoonsgegevens gebruikt mogen worden of gedeeld mogen worden, zal, indien het de bedoeling is een betere kwaliteit na te streven van het desbetreffende beleid, de afweging om de persoonsgegevens toch te gebruiken navolgbaar worden vastgelegd.

4.6 De verantwoording

Artikel 5.2 AVG: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van "de wet" en kan dit aantonen ("verantwoordingsplicht"). In artikel 24 AVG wordt het duidelijk dat het gaat om het kunnen overleggen van het bewijs van effectieve werking van getroffen beheers- en beveiligingsmaatregelen die naleving van de AVG borgen. Een samenvattende verantwoording wordt opgenomen in het jaarverslag en is daarmee een onderdeel van de maatschappelijke verantwoording.
In het bovenstaande governance & compliance model kunnen wij vier actoren met een wettelijke status onderkennen. Het bestuur van de WODV verantwoordt zich voor de gang van zaken van de werkorganisatie met behulp van jaarrekening plus jaarverslag / bestuurdersverslag aan het maatschappelijk verkeer. Hier past ook in een (maatschappelijke) verantwoording over het gevoerde privacy-beleid.

4.7 Uitvoering

Indien daar aanleiding toe is, kan in de voortgangsrapportages gedurende het jaar worden gerapporteerd over de lopende uitvoering van het privacybeleid.

4.8 Plaats in de P&C-producten

De voornemens en verantwoording van privacy zou voor de WODV het beste passen in het hoofdstuk Beleidsbegroting op de nemen.

4.9 Rol FG in governance

<u>De FG heeft, conform zijn wettelijke taken, in dit kader een tweetal taken:</u>

1. Hij ziet er op toe dat privacy-administratie inderdaad gedegen wordt uitgevoerd.
2. Voordat het bestuur van de WODV een besluit neemt over de privacy-verantwoording of voornemens brengt de FG hierover een advies uit.

5. WODV

De WODV heeft zelf als verantwoordelijke slechts een beperkt aantal eigen processen, waarvoor zij in privacy-termen verantwoordelijke is, namelijk op het terrein van bedrijfsvoering.

6. Rechten van betrokkenen

Binnen het beleid worden de volgende rechten van betrokkenen geborgd:

Recht op informatie
De WODV verwerkt gegevens om haar taken te kunnen uitvoeren. Indien dit persoonsgegevens betreffen, heeft de WODV de plicht om betrokkenen, voor zover deze daar niet reeds van op de hoogte zijn, te informeren over verwerkingen van hun persoonsgegevens. De WODV verstrekt dan aan betrokkenen informatie over de verwerking, zoals het doel daarvan, welke persoonsgegevens worden verwerkt en of de gegevens aan anderen worden verstrekt. Dit met inachtneming van de beperkingen zoals die neergelegd zijn in wet- en regelgeving.

Daartoe zal een relevant deel van het register van verwerkingen ook worden gepubliceerd op de website van de WODV.

Recht op inzage
Betrokkenen hebben de mogelijkheid om te controleren of en op welke manier hun gegevens worden verzameld en verwerkt. Dit wordt uitgevoerd met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving. Voor de verwerking van deze verzoeken is een procedure opgesteld.

Recht op correctie
Als de WODV persoonsgegevens van betrokkenen verwerkt die naar hun oordeel onjuist zijn, kunnen zij een verzoek indienen bij de WODV om dit te verbeteren. Dit met inachtneming van de beperkingen zoals neergelegd in wet- en regelgeving.

Recht om vergeten te worden
Betrokkenen hebben het recht persoonsgegevens te laten verwijderen indien de WODV niet langer een goede grond heeft voor het gebruik hiervan, bijvoorbeeld indien betrokkenen een gegeven toestemming intrekken, indien de gegevens onjuist zijn of de gegevens niet langer nodig zijn.

Recht op bezwaar tegen verwerking
Betrokkenen hebben het recht aan de WODV te vragen hun persoonsgegevens niet meer te gebruiken en bezwaar te maken tegen de verwerking van hun persoonsgegevens. De WODV moet hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Recht op beperking van de verwerking
Het recht op beperking houdt in dat de WODV de persoonsgegevens (tijdelijk en onder voorwaarden) niet mag verwerken en niet mag wijzigen, bijvoorbeeld wanneer betrokkenen de juistheid van de gegevens ter discussie stellen.

Recht op overdraagbaarheid van gegevens (dataportabiliteit)
De WODV is vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens voor zover het werkzaamheden betreft in het kader van algemeen belang, de uitoefening van een openbaar gezag, wanneer deze zijn openbare taken uitoefent of aan een wettelijke verplichting voldoet. Desondanks zal de WODV in voorkomende gevallen voorzieningen treffen in het kader van dataportabiliteit.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profiling
Uitgangspunt in de AVG is dat er geen geautomatiseerde besluitvorming op basis van profilering mag plaatsvinden, als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kan gedacht worden aan bijvoorbeeld de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst.

6.1 Uitoefening van rechten

Om gebruik te maken van de bovenstaande rechten kunnen de betrokkenen een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de website van de WODV ingediend worden. Binnen vier weken beoordeelt de WODV of het verzoek gerechtvaardigd is. De WODV laat binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of de WODV de behandeling van het verzoek met twee maanden verlengt. De WODV behandelt het verzoek volgens de daarvoor door haar vastgestelde en bekendgemaakte procedure.

Als het verzoek niet op tijd wordt opgevolgd, deelt de WODV uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven. De betrokkene heeft dan de mogelijkheid om bezwaar te maken bij de WODV of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

6.2 Bewustwording

Er wordt gezorgd voor voldoende bewustwording bij de medewerkers op het gebied van privacy. Hierbij dienen zij minimaal op de hoogte te zijn van de privacyregels en de voor hun werkzaamheden relevante bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen.

7. Interne regelingen afspraken

7.1 Meldplicht datalekken

Indien zich een datalek voordoet, waarbij bijvoorbeeld gegevens van personen in verkeerde handen kunnen komen of zijn gekomen, handelt de WODV in overeenstemming met de vastgestelde werkwijze in het Protocol Meldplicht en afhandeling van (vermoedelijke) datalekken. Dit protocol bevat een vastgesteld proces van te doorlopen stappen om de eventuele schade of de kans hierop, bij een datalek te beperken en de getroffen perso(o)n(en) te beschermen. In ieder geval wordt een datalek intern gemeld aan de FG.

Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden of kan plaatsvinden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn, en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

De plicht tot het melden aan de Autoriteit Persoonsgegevens van een (vermoeden van een) datalek geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene(n), dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit bestanden en/of gegevens waarvoor de WODV verantwoordelijkheid draagt. Wanneer er een dergelijk datalek heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de Autoriteit Persoonsgegevens. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval wordt dit datalek ook aan de betrokkenen gemeld, in eenvoudige en duidelijke taal.

7.2 Het register van verwerkingsactiviteiten

De functionaris voor gegevensbescherming (FG) houdt namens de verantwoordelijke er toezicht op dat er een register van verwerkingen van persoonsgegevens wordt bijgehouden. De PO draagt zorg voor de inschrijving van de verwerkingen van persoonsgegevens in dit register. Afdelingsmanagers dienen (nieuwe) verwerkingen of wijzigingen direct aan de PO te melden.

Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:

a. de naam van de verwerking;

b. wie de verantwoordelijke is voor de verwerking;

c. het doel van de verwerking;

d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);

e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;

f. de ontvangers van de gegevens;

g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;

h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;

i. de verwijderingstermijnen die in acht genomen worden;

De FG houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende documenten (eventuele verwerkersovereenkomst, model Gegevensbeschermingseffectbeoordeling, privacy-protocol, informatieverplichting), de registratie van incidenten.

7.3 Gegevensbeschermingseffectbeoordeling (DPIA)

Een Gegevensbeschermingseffectbeoordeling (DPIA) is een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een Gegevensbeschermingseffectbeoordeling wordt doorgaans uitgevoerd met ondersteuning van de PO, voorafgaand aan de verwerking en maar ook bij bestaande verwerkingen waarvoor hij nog niet eerder was uitgevoerd en waar sprake is van een gegevensverwerking die een hoog privacy-risico oplevert voor de betrokkenen.

Tevens heeft de AP nog een lijst samen gesteld voor verwerkingen waarbij een Gegevensbeschermingseffectbeoordeling altijd verplicht is.

Of er sprake is van een hoog privacy-risico, toetst de WODV aan de hand van een Risk Impact Assessment (RIA). De RIA wordt uitgevoerd op het moment dat een van de BIV-classificaties 2 of hoger scoort. Dus naast de Vertrouwelijkheid, waar privacy geraakt wordt, ook op Beschikbaarheid en Integriteit.

<u>Op grond van de AVG is verder in ieder geval sprake van een hoog privacy-risico indien de WODV:</u>

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens verwerkt of op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied; Hierbij wordt gelet op het aantal betrokkenen, het volume van gegevens en/of het bereik van verschillende gegevens/items die worden verwerkt, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit;
- Indien wordt voldaan aan twee of meer criteria van de in bijlage 1 opgenomen criteria van de werkgroep van Europese privacy-toezichthouders (WP29).

<u>Voor de Gegegevensbeschermingseffectbeoordeling gelden de volgende kaders:</u>

1. Een Gegevensbeschermingseffectbeoordeling vindt plaats voordat met de betreffende verwerking wordt gestart.

2. Een Gegevensbeschermingseffectbeoordeling wordt herhaald bij wijzigingen waardoor de risico's van de verwerking toenemen.

3. Bij het uitvoeren van een Gegevensbeschermingseffectbeoordeling wordt de FG altijd geïnformeerd.

4. Het afdelingshoofd ziet toe op het nemen van maatregelen die blijkens de Gegevensbeschermingseffectbeoordeling nodig zijn om de risico's te verkleinen.

5. Het resultaat van de Gegevensbeschermingseffectbeoordeling en de genomen maatregelen om het risico te beperken worden aan de FG voorgelegd ter toetsing en opneming in het registerverwerkingen.

6. Gegevensbeschermingseffectbeoordelingen die binnen de WODV worden uitgevoerd vinden plaats volgens een standaard.

7.4 Overgangsregeling

Voor verwerkingen met een hoog privacy-risico die voor 25 mei 2018 al bestonden is een Gegevensbeschermingseffectbeoordeling (DPIA) na deze datum verplicht indien:

1. De verwerking verandert, bijvoorbeeld door nieuwe technologie of wijziging van doel;
2. Het risico verandert;
3. De omgeving verandert, bijvoorbeeld door maatschappelijke veranderingen.

Deze overgangstermijn eindigt op 25 mei 2021. Dan dient derhalve voor iedere verwerking met een hoog risico een DPIA te zijn uitgevoerd.

7.5 Inschakeling verwerkers, verwerkersovereenkomst

Wanneer de WODV een partij inschakelt om ten behoeve van de WODV persoonsgegevens te verwerken en het verwerken van de persoonsgegevens de primaire taak is van deze partij, kan deze partij worden beschouwd als verwerker. De WODV schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd in een verwerkersovereenkomst. Deze worden vastgelegd voordat de dienstverlening aanvangt. Daarna worden deze afspraken periodiek of steekproefsgewijs getoetst.

Verder kan het voorkomen dat de WODV een andere partij inschakelt, die geen verwerker is, maar waarmee wel persoonsgegevens worden uitgewisseld. Ook dan maakt de WODV passende afspraken. In dat geval zal de WODV een overeenkomst sluiten omtrent de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin de respectieve verantwoordelijkheden worden vastgelegd.

De WODV laat regelmatig taken door anderen uitvoeren. Daarbij zullen de organisaties die deze taken uitvoeren ook meestal persoonsgegevens verwerken. Voor deze verwerkingen zal de WODV in de meeste gevallen niet de privacy-verantwoordelijke zijn, maar de WODV heeft wel een zekere kwaliteitsverantwoordelijkheid. In dat kader zal de WODV er op toezien dat deze organisaties veilig met persoonsgegevens omgaan.

7.6 Toegang medewerkers

Medewerkers mogen alleen toegang tot die persoonsgegevens hebben die zij voor hun werk nodig hebben. Het is gewenst dit zorgvuldig vast te leggen en hierop regelmatig een controle op te houden. Hiertoe worden zo veel als mogelijk in de systemen harde toegangsgrenzen ingericht. Hiertoe moeten alle systemen van logging zijn voorzien en dient er op gezette tijd een controle te worden uitgevoerd op basis van die logging-gegevens. De uitkomsten hiervan worden gedurende een bepaalde tijd bewaard.

8. Deelnemingen

Vaak hebben gemeenten taken uitbesteed aan Gemeenschappelijke Regelingen (GR'en; op basis van juridische titel) en samenwerkingsverbanden (zonder juridische titel). Meestal is er dan sprake van uitbesteding van en of meerdere verwerkingen. Maar soms is een GR zelfstandig verwerkingsverantwoordelijke en voeren zij een resultaatsverplichting uit (Bijvoorbeeld in de uitvoering van de participatiewet of gemeentelijke belastingwetten).

Bij de meeste deelnemingen heeft de WODV wel invloed, maar is niet alleen bepalend voor het uitzetten van de koers.

Voor het beantwoorden van de vraag of deze deelnemingen een eigen privacy-beleid behoeven en of ze zelf verwerkingsverantwoordelijke zijn, zijn de volgende criteria van belang:

1. Verwerkt de deelneming veel persoonsgegevens?
2. Bepaalt de deelneming zelf doel en middelen van de persoonsgegevens?

De deelnemingen betreffen voor Voorschoten en Wassenaar veelal gemeenschappelijke regelingen. Deelnemingen en samenwerkingen moeten door de komst van de AVG in zoverre in een ander daglicht worden beschouwd dat in veel gevallen het gemeentebestuur toch verantwoordelijk en aansprakelijk is en blijft voor de uitvoeringsprocessen door de GR'en en samenwerkingen voor wat betreft privacy.

Het is een kwestie van de juiste balans vinden tussen de inspanningen die gedaan moeten worden en de middelen die beschikbaar zijn voor de uitvoering. Gevolgen voor de WODV, GR'en en samenwerkingsverbanden zijn:

· Er is ketenaansprakelijkheid door gebruik te maken van GR'en en samenwerkingsverbanden, leveranciers, etc.;

· Aandacht voor privacy-overeenkomsten door de ketenaansprakelijkheid is belangrijk teneinde heldere onderlinge afspraken te hebben.