AUTORITEIT
PERSOONSGEGEVENS

Rapportage

Verkennend onderzoek Gegevensbeschermings-beleid

Openbare versie | Rapport definitieve bevindingen
z2018-27134

AUTORITEIT
PERSOONSGEGEVENS

De Autoriteit Persoonsgegevens (AP) hecht veel waarde aan een goed gegevensbeschermingsbeleid, omdat dit organisaties dwingt om vooraf na te denken over hoe zij persoonsgegevens beschermen. De AP heeft daarom een verkennend onderzoek uitgevoerd naar de kwaliteit van het gegevensbeschermingsbeleid van twee soorten zorginstellingen en een aantal lokale politieke partijen, omdat zij bijzondere persoonsgegevens verwerken. In dit rapport deelt de AP de resultaten en doet zij aanbevelingen.

Samenvatting en aanbevelingen

Samenvatting

De AP heeft het gegevensbeschermingsbeleid gecontroleerd bij bloedbanken, IVF-klinieken en de politieke partijen van drie gemeenten. Het gaat om drie gemiddelde gemeenten met meer dan 100.000 inwoners. Het onderzoek richtte zich op drie verplichte onderdelen van het gegevensbeschermingsbeleid: een omschrijving van de (categorieën van) persoonsgegevens, een beschrijving van de doeleinden van de gegevensverwerking en de rechten van betrokkenen. Uit de beoordeelde documenten valt op dat zij erg verschillend zijn in aard en omvang. In de AVG zijn geen vereisten vastgelegd over de vorm.

Alle gecontroleerde bloedbanken en IVF-klinieken hebben een gegevensbeschermingsbeleid. Bij de zorginstellingen schortte er in veel gevallen iets aan de drie verplichte onderdelen: bij ongeveer de helft van de documenten ontbrak bijvoorbeeld een omschrijving van de categorieën van persoonsgegevens of was het onvoldoende. En ontbrak een omschrijving van de doelen van de gegevensverwerkingen. De AP heeft 21 documenten beoordeeld van lokale politieke partijen. Deze documenten bleken in de meeste gevallen in orde. Niet alle partijen hebben een beschermingsbeleid, omdat zij geen leden hebben.

De resultaten van het onderzoek zijn voor de AP aanleiding om zes aanbevelingen te doen aan organisaties om hun gegevensbeschermingsbeleid goed in te richten.

Zes aanbevelingen voor gegevensbeschermingsbeleid

Toelichting

- *Beoordeel of u het verplicht bent*
  Het is afhankelijk van de verwerking of uw organisatie een gegevensbeschermingsbeleid moet inrichten. Het is belangrijk aan de hand van de AVG na te gaan welk soort gegevens uw organisatie verwerkt en op welke schaal. Wanneer u bijvoorbeeld op grote schaal bijzondere persoonsgegevens verwerkt dient uw organisatie een gegevensbeschermingsbeleid op te stellen en te hanteren. Het is uw eigen verantwoordelijkheid om deze beoordeling te maken. Wacht niet totdat de AP ernaar vraagt.
- *Gebruik expertise*
  Gebruik de aanwezige expertise in uw organisatie om tot een goed gegevensbeschermingsbeleid te komen. De FG kan hier als adviseur en intern toezichthouder een belangrijke rol in spelen. Het beleid moet voldoen aan de AVG en werkbaar zijn in de praktijk. Wanneer uw organisatie problemen ondervindt met het invullen van dit beleid, kunt u altijd een externe expert raadplegen voor advies over de normen uit de AVG en over de specifieke uitwerking binnen uw organisatie.
- *Leg het vast in één document*
  Uit de ontvangen documentatie blijkt dat de informatie met betrekking tot het gegevensbeschermingsbeleid wel voorhanden is, maar soms versnipperd is. Informatie is soms te vinden in het verwerkingsregister, in de privacyverklaring op de website en het komt voor dat er daarnaast nog een gegevensbeschermingsbeleid is ingericht. Op zich is dat mogelijk, maar het is overzichtelijker als het gegevensbeschermingsbeleid een compleet beeld geeft. Op die manier is

immers makkelijker te achterhalen welk beleid uw organisatie heeft voor het beschermen van persoonsgegevens.

- *Wees concreet*
  Een professioneel gegevensbeschermingsbeleid vormt een concrete vertaalslag van de AVG-normen naar de gegevensverwerkingen van uw organisatie. Het is dus niet toereikend om de normen uit de AVG te herhalen.
- *Maak het bekend*
  De AVG vereist niet dat u het gegevensbeschermingsbeleid publiceert, maar het is wel aan te bevelen. Ook voor betrokkenen wordt dan inzichtelijk hoe uw organisatie met hun persoonsgegevens omgaat. Let bij de publicatie wel op dat er geen informatie in het beleid staat waarmee kwaadwillenden hun voordeel kunnen doen. Zoals informatie over de beveiliging.
- *Niet verplicht? Toch raadzaam*
  Het kan zijn dat uw organisatie niet verplicht is om een gegevensbeschermingsbeleid te hebben. Ook dan is het raadzaam om een dergelijk beleid in te richten, omdat u daarmee aantoont dat u de persoonsgegevens van betrokkenen wilt beschermen.

Achtergrond gegevensbeschermingsbeleid

Organisaties zijn zelf verantwoordelijk voor het voldoen aan de privacyregels van de Algemene verordening gegevensbescherming (AVG). Uit dit 'accountability' principe volgt de verantwoordingsplicht. Deze plicht houdt in dat organisaties moeten kunnen aantonen dat hun verwerkingen van persoonsgegevens in overeenstemming zijn met de regels. In de AVG staan de maatregelen die verwerkingsverantwoordelijken moeten nemen om aan deze verantwoordingsplicht te kunnen voldoen.

Gegevensbeschermingsbeleid

Verwerkingsverantwoordelijken moeten op grond van artikel 24 AVG passende technische en organisatorische maatregelen treffen om te waarborgen en te kunnen aantonen dat een verwerking in overeenstemming met de AVG wordt uitgevoerd. Afhankelijk van de soort verwerkingsactiviteiten moet een organisatie een gegevensbeschermingsbeleid uitvoeren. Dit staat in het tweede lid van dit artikel. Hieruit volgt dat een gegevensbeschermingsbeleid niet voor alle verwerkingsverantwoordelijken een verplicht onderdeel uitmaakt van de passende technische en organisatorische maatregelen die een verwerkingsverantwoordelijke moet treffen. Dat hangt af van de aard, de omvang, de context en het doel van de gegevensverwerking. Een gegevensbeschermingsbeleid helpt een organisatie om alle verwerkingen van persoonsgegevens in kaart te brengen en hiervoor verantwoordelijkheid te nemen. Het geeft personen wiens persoonsgegevens verwerkt worden inzicht in de organisatie en de mogelijkheden voor het uitoefenen van zijn of haar rechten.

Het opstellen, borgen en periodiek bijwerken van een gegevensbeschermingsbeleid stimuleert organisaties om vooraf na te denken over een zorgvuldige omgang met persoonsgegevens. Het vermindert daarmee risico's zoals een datalek.

Bijzondere persoonsgegevens

Alle organisaties waarvan de AP in dit verkennend onderzoek het gegevensbeschermingsbeleid heeft opgevraagd verwerken bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens over iemands:

- ras of etnische afkomst;
- politieke opvattingen;
- godsdienst of levensovertuiging;
- lidmaatschap van een vakbond;
- genetische of biometrische gegevens met oog op unieke identificatie;
- gezondheid;
- seksuele leven.

Daarnaast zijn er nog gevoelige gegevens, zoals financiële gegevens en strafrechtelijke gegevens. Juist voor de organisaties die bijzondere en gevoelige gegevens verwerken is het van belang om een goed gegevensbeschermingsbeleid op te stellen en te hanteren.

Functionaris voor de gegevensbescherming

Organisaties zijn in bepaalde situaties verplicht een functionaris gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Organisaties die bijzondere persoonsgegevens verwerken, zoals de onderzochte partijen, zijn verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is.

Een belangrijke taak van de FG is intern toezicht houden op het naleven van de AVG. Om dit te kunnen doen kan de FG:

- informatie verzamelen over gegevensverwerkingen binnen de organisatie;
- deze verwerkingen analyseren en beoordelen of ze aan de wet voldoen en
- informatie, adviezen en aanbevelingen geven aan de organisatie.

Drie onderdelen van een gegevensbeschermingsbeleid

Omschrijving van de categorieën persoonsgegevens

De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Er zijn veel soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en bankrekeningnummers zijn persoonsgegevens. Gegevens die betrekking hebben op iemands ras, godsdienst of gezondheid worden bijzondere persoonsgegevens genoemd. Uit een gegevensbeschermingsbeleid dient te blijken welke gegevens worden verwerkt en tot welke categorie deze gegevens behoren. Politieke partijen verwerken bijvoorbeeld veelal gegevens waaruit de politieke opvatting van een persoon kan worden herleid. Een politieke partij die deze gegevens verwerkt dient dan ook te vermelden dat bijzondere persoonsgegevens worden verwerkt. Vervolgens dient uit het gegevensbeschermingsbeleid te blijken welke specifieke gegevens worden verwerkt. Dan kan het bijvoorbeeld gaan om naam en adres, maar ook om een telefoonnummer of bankrekeningnummer. Door deze categorieën te beschrijven geeft de organisatie specifiek inzicht in de verwerkingen.

Beschrijving van de doeleinden van de verwerkingen

Op basis van de persoonsgegevens die verwerkt worden dient de organisatie vervolgens te beschrijven met welk doel die gegevens verwerkt worden. Een politieke partij kan de adresgegevens bijvoorbeeld gebruiken voor correspondentie over het lidmaatschap, of het rekeningnummer om contributie te innen. Van belang is om te motiveren op basis van welke juridische grondslag deze verwerkingen plaatsvinden.

Rechten van betrokkenen

De AVG geeft iedereen sterke en uitgebreide privacyrechten. Organisaties moeten bijvoorbeeld in een aantal gevallen iemands persoonsgegevens wissen als diegene daarom vraagt. En mensen hebben het recht om organisaties te vragen hun persoonsgegevens te verbeteren, aan te vullen of af te schermen. Een goed gegevensbeschermingsbeleid beschrijft hoe privacyrechten in de organisatie geborgd zijn en op welke wijze een betrokkene zijn of haar rechten kan uitoefenen. Een goed uitgeschreven en helder overzicht van de rechten van betrokkenen kan, mits deze rechten in de praktijk ook daadwerkelijk zo uitgeoefend kunnen worden, vertrouwen geven dat deze (bijzondere) persoonsgegevens in goede handen zijn.

Het onderzoek

Onderzochte partijen

De AP heeft ervoor gekozen om dit onderzoek te richten op twee soorten zorginstellingen en op gemeentelijke/lokale afdelingen van politieke partijen.

De zorginstellingen betreffen IVF-klinieken (tien in totaal) en bloedbanken (acht in totaal). Deze zorginstellingen verwerken bijzondere persoonsgegevens en/of gevoelige gegevens. Zoals gegevens over de gezondheid en genetische gegevens. Vanwege deze verwerking vallen deze zorginstellingen onder de verplichting van artikel 24, eerste lid, AVG.

Daarnaast is de keuze gemaakt om van drie gemeenten de politieke partijen te kiezen die zitting hebben in de gemeenteraad. Politieke partijen verwerken naar de aard van hun organisatie bijzondere persoonsgegevens, namelijk gegevens over de politieke voorkeur van mensen. Daarom vallen zij onder de norm van artikel 24, tweede lid, AVG. De gemeenten zijn gekozen op basis van hun gelijke omvang (boven de 100.000 inwoners), zodat de gemeenten onderling goed vergeleken kunnen worden. Daarnaast betreffen het vanuit sociaaleconomisch en demografisch oogpunt gemiddelde gemeenten binnen Nederland. De keuze voor drie gemeenten zorgt voor een breder beeld van de naleving van deze specifieke norm door lokale politieke partijen.

Alle bloedbanken en IVF-klinieken hebben een gegevensbeschermingsbeleid en hebben deze ook toegestuurd. Twee politieke partijen hebben aangegeven geen beschermingsbeleid te hebben, omdat zij geen leden hebben.

Beeld van de ontvangen documentatie

De AVG stelt geen eisen aan de vorm van een gegevensbeschermingsbeleid. Dit heeft tot gevolg dat de aangeleverde documentatie zeer verschilt van aard en omvang. Sommige documentatie bevat een privacyverklaring en/of het verwerkingsregister. Het houden van zo'n register is op basis van artikel 30 AVG voor alle verwerkingsverantwoordelijken verplicht. De inhoud van dit register overlapt voor een groot deel met de vereisten van een gegevensbeschermingsbeleid, waaronder een beschrijving van de verwerkingsdoeleinden en een beschrijving van de categorieën van persoonsgegevens.

Verder hebben de lokale afdelingen van landelijke politieke partijen veelal het landelijke beleid van hun partij toegestuurd. Het ligt in de rede om een landelijk gegevensbeschermingsbeleid vast te stellen waaraan de lokale afdelingen zich committeren.

Het verkennend onderzoek richtte zich op drie verplichte onderdelen van het gegevensbeschermingsbeleid. Dit betreft een omschrijving van de (categorieën van) persoonsgegevens, een beschrijving van de doeleinden van de gegevensverwerking en de rechten van betrokkenen, zoals bedoeld in artikel 15 ev. AVG. Daarnaast is bij de beoordeling gekeken of specifieke onderdelen de aandacht trokken en welke aanbevelingen uit de documenten zijn af te leiden.
In deze rapportage maakt de AP onderscheid tussen de beoordeling van de documentatie van de zorginstellingen en de beoordeling van de documentatie van de politieke partijen. Hoewel het vereiste van het hebben van een gegevensbeschermingsbeleid voor beide groepen hetzelfde is, maakt deze rapportage inzichtelijk hoe beide groepen afzonderlijk invulling geven aan de verplichting om een

gegevensbeschermingsbeleid te hanteren.

Beoordeling gegevensbeschermingsbeleid bloedbanken en IVF-klinieken

In totaal is aan acht bloedbanken en tien IVF-klinieken gevraagd hun gegevensbeschermingsbeleid naar de AP te sturen. De bloedbanken vallen allemaal onder dezelfde organisatie die een landelijk beleid hanteert. Dit betekent dat de AP in totaal elf documenten met een gegevensbeschermingsbeleid heeft ontvangen. Hieronder volgt een beoordeling en toelichting per getoetst onderdeel van het beleid: beschrijving van de categorieën van persoonsgegevens, beschrijving van de doeleinden en een beschrijving van de rechten van betrokkenen.

Aantal documenten dat een goede omschrijving geeft per onderdeel

Categorieën	Doeleinden	Rechten betrokkenen
5 van 11 documenten voldoen	6 van 11 documenten voldoen	7 van 11 documenten voldoen

Toelichting

a) Omschrijving van de categorieën persoonsgegevens

Van de elf ontvangen documenten bevatten vijf een goede omschrijving van de categorieën persoonsgegevens die worden verwerkt, zoals contactgegevens, financiële gegevens (bijv. rekeningnummer), BSN, en bijzondere persoonsgegevens (bijv. specifieke gezondheidsgegevens). Voor de overige beleidsstukken geldt dat in het geheel geen omschrijving was opgenomen of alleen een zeer algemene beschrijving. Zo beschrijft één beleid slechts dat de partij beschikt over "*een groot aantal persoonsgegevens van zeer uiteenlopende betrokkenen*". Zo'n omschrijving geeft de betrokkenen en de toezichthouder onvoldoende informatie over welk soort informatie de organisatie verwerkt.

b) Beschrijving van de doeleinden van de verwerkingen

Van de elf ontvangen documenten is in zes een beschrijving opgenomen van de doeleinden waarvoor zij persoonsgegevens verwerken. Dit betrof overigens dezelfde vijf beleidsdocumenten die ook een goede omschrijving van de categorieën persoonsgegevens bevatten.
De zes overige gegevensbeschermingsbeleidsstukken geven geen beschrijving van de doeleinden van verwerking van de specifieke organisatie.

c) Rechten van betrokkenen

Van de elf documenten bevatten zeven een duidelijke omschrijving van de rechten die mensen kunnen uitoefenen en van de wijze waarop zij dat kunnen doen. In de overige documenten is slechts de tekst van de AVG over 'de rechten van betrokkenen' overgenomen en is niet opgenomen op welke wijze betrokkenen die rechten kunnen uitoefenen.

Beoordeling gegevensbeschermingsbeleid lokale politieke partijen

De AP heeft in drie gemeenten alle politieke partijen die zitting hebben in de gemeenteraad aangeschreven. Twee partijen hebben in hun reactie aangegeven geen leden te hebben en daarom geen gegevensbeschermingsbeleid te hanteren. Negen lokale afdelingen die hebben gereageerd hanteren een landelijk gegevensbeschermingsbeleid. Hiervan hebben drie lokale afdelingen een lokale toevoeging aan het landelijk beleid toegestuurd, hetgeen voor de AP reden was deze wel individueel te beoordelen. De AP heeft in totaal 21 beleidsstukken met gegevensbeschermingsbeleid van lokale politieke partijen beoordeeld. Een aantal kleinere politieke partijen bleek een zeer goed uitgewerkt gegevensbeschermingsbeleid te hebben. Hieruit kan worden opgemaakt dat het ter beschikking hebben van minder middelen geen belemmering voor een goed beleid hoeft te zijn. Hieronder volgt een beoordeling en toelichting per getoetst onderdeel van het beleid.

Aantal documenten dat een goede omschrijving geeft per onderdeel

Categorieën	Doeleinden	Rechten betrokkenen
20 van 21 documenten voldoen	20 van 21 documenten voldoen	18 van 21 documenten voldoen

Toelichting

a) Omschrijving van de categorieën persoonsgegevens

Van de 21 stukken met gegevensbeschermingsbeleid die de AP heeft ontvangen, bevat slechts één geen omschrijving van de categorieën persoonsgegevens die de betreffende organisatie verwerkt. Wel is het zo dat soms de categorieën niet limitatief zijn omschreven. Uit het verkennend onderzoek blijkt dat ook de zeer kleine lokale politieke partijen een omschrijving van de categorieën persoonsgegevens hebben opgenomen.

b) Beschrijving van de doeleinden van de verwerkingen

Slechts één document met gegevensbeschermingsbeleid bevat geen beschrijving van de doeleinden van de verwerkingen. Dit betreft hetzelfde beleid als waarin de omschrijving van de categorieën persoonsgegevens ontbreekt. De overige documenten bevatten dus wel een adequate beschrijving, waaruit mensen kunnen afleiden voor welke doeleinden de organisatie hun persoonsgegevens verwerkt.

c) Rechten van betrokkenen

Drie toegestuurde gegevensbeschermingsbeleidsdocumenten bevatten geen beschrijving van de rechten die betrokkenen kunnen uitoefenen. De overige documenten bevatten wel een goede beschrijving met daarbij vaak ook aangegeven op welke wijze zij die rechten kunnen uitoefenen. In de meeste gevallen is dat via een e-mailadres.

AUTORITEIT
PERSOONSGEGEVENS

Vragen over de AVG

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.