

Privacyreglement 2018

Gemeente Oostzaan, Wormerland, GR OVER-gemeenten



Inhoudsopgave

1. Wetgeving en definities.....	2
2. Reikwijdte	3
3. Verantwoordelijke.....	3
4. Verwerkingen (Artikel 4, AVG).....	3
5. Transparantie en communicatie	4
6. Geautomatiseerde verwerkingen	5
7. Plichten van de organisatie.....	6
Afsluiting.....	7

In dit reglement laat de organisatie zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is. Dit beleid is gelijklopend voor de gemeente Oostzaan, Wormerland en GR OVER-gemeenten (verder aangeduid als 'de organisatie').

Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. De organisatie heeft de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief is. De organisatie is verplicht om zorgvuldig en veilig, proportioneel en vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt voor taken op het gebied van basisadministraties, openbare orde en veiligheid, en het sociaal domein. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van de organisatie. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen.

1. Wetgeving en definities

Vanaf 25 mei 2018 wordt het juridische kader voor de omgang met persoonsgegevens in Nederland, bepaald door de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet (UAVG). De AVG dient ter vervanging van de Wet bescherming persoonsgegevens (Wbp), welke gebaseerd was op de Europese richtlijn van 1995.

De inwerkingtreding van de AVG zorgt voor verandering in het privacyklimaat van Nederland. De AVG bouwt voort op de Wbp en zorgt onder andere voor versterking en uitbreiding van de privacyrechten met meer verantwoordelijkheden voor organisaties. Ook de organisatie zal deze extra verantwoordelijkheidseisen moeten naleven.

De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

Persoonsgegevens: alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn gegevens die betrekking hebben op etnische afkomst, politieke opvattingen, religieuze overtuigingen, het lidmaatschap van een vakbond, genetische gegevens/biometrische gegevens, gezondheid of seksuele aard. Verder kent de wet nog gevoelige persoonsgegevens, zoals het Burgerservicenummer (BSN) en strafrechtelijke gegevens, waar extra zorgvuldig mee om dient te worden gegaan.

Betrokkene: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

Verwerkingsverantwoordelijke: een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

Verwerker: de persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

Verwerking: als een verwerking geldt alles wat je met een persoonsgegeven doet. Voorbeelden zijn: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Gegevensbeschermingseffectbeoordeling: met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een Privacy Impact Assessment (PIA).¹

¹ <https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/14-0404-Toelichting-PIA-v1.0.pdf>

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de organisatie. Oftewel: voor alle verwerkingen die binnen de organisatie plaatsvinden.

3. Verantwoordelijke

De (bestuur)organen van de organisatie zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester en het college van burgemeesters en wethouders (college van B&W). De bestuursorganen bij OVER-gemeenten zijn onder andere het Algemeen en het Dagelijks Bestuur en de voorzitter.

4. Verwerkingen (Artikel 4, AVG)

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. Bij de verwerking van persoonsgegevens hanteert de organisatie de vereisten zoals genoemd in de AVG. Onderstaand worden de belangrijkste vereisten nader toegelicht.

Doelinden (Artikel 5, AVG)

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

Rechtmatige grondslag (Artikel 6, AVG)

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel van is;
- Om een verplichting na te komen die in de wet staat;
- Om een ernstige bedreiging voor de gezondheid van de betrokkene of een ander natuurlijk persoon te bestrijden (vitaal belang);
- Voor de goede vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
- Voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, voor zover belangenafweging dit rechtvaardigt.

Wijze van verwerking

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet en op een zorgvuldige wijze plaatsvindt. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

De organisatie zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligd de organisatie alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de organisatie dit doet, staat in het informatiebeveiligingsbeleid van de organisatie en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Doorgifte (Artikel 44 t/m 50, AVG)

De organisatie geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie indien er minimaal een adequaat beschermingsniveau wordt gewaarborgd.

Verwerkersovereenkomsten

Indien de organisatie gebruik maakt van een verwerker (derde partij) bij de verwerking van persoonsgegevens, sluit de organisatie een verwerkersovereenkomst af. In de verwerkersovereenkomst worden afspraken met de verwerker gemaakt over veilige verwerking van persoonsgegevens. Deze overeenkomst omvat in ieder geval: het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven. Tevens neemt de organisatie in haar verwerkersovereenkomst op dat de gemaakte afspraken/privacyrechtelijke verplichtingen worden doorgegeven aan eventuele sub-verwerkers. Hiermee waarborgt de organisatie dat eveneens bij gebruik van een sub-verwerker de privacy ten aanzien van de persoonsgegevens op gelijkelijk niveau wordt beschermd als bij verwerking door de organisatie.

5. Transparantie en communicatie

Wet openbaarheid van bestuur (Wob)

Via de Wob² (en straks wellicht de Wet Open Overheid) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de organisatie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt. Als de organisatie gegevens openbaart als gevolg van een Wob verzoek, worden persoonlijke gegevens in beginsel gepseudonimiseerd.

Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie³ regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de organisatie altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Informatieplicht (Artikel 13,14, AVG)

De organisatie informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de organisatie geven, worden zij op de hoogte gesteld van de manier waarop de organisatie met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de organisatie persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Verwijdering

De organisatie bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van (gemeentelijke) taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel, worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

Rechten van betrokkenen (Artikel 13 t/m 20, AVG)

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

- **Recht op informatie:** Betrokkenen hebben het recht om aan de organisatie te vragen of zijn/haar persoonsgegevens worden verwerkt.

² <http://wetten.overheid.nl/BWBR0005252/2016-10-01>

³ <http://wetten.overheid.nl/BWBR0036795/2016-10-01>

- Inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- Correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de organisatie om dit te corrigeren.
- Recht van verzet: Betrokkenen hebben het recht aan de organisatie te vragen om hun persoonsgegevens niet meer te gebruiken.
- Recht om vergeten te worden: In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De organisatie zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Indienen van verzoek

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De organisatie heeft een maand de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Indien nodig kan deze termijn met twee maanden worden verlengd. Binnen een maand zal de organisatie laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de organisatie, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de organisatie aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Communicatie met medewerkers, burger en partners

Medewerkers

Medewerkers moeten bewust worden van hun gedrag en werkwijze ten aanzien van het verwerken van privacygevoelige gegevens. Zij dienen de op de AVG-aangepaste werkprocessen en protocollen op te volgen. Ook is het belangrijk dat medewerkers in hun werk rekening houden met 'dataminimalisatie en transparantie'. Intern is bewustwording een belangrijke factor. Door middel van verschillende kanalen worden medewerkers bewust gemaakt van de manier waarop zij om dienen te gaan met het verwerken van persoonlijke gegevens.

Inwoners

Inwoners worden actief geïnformeerd over de nieuwe privacywet, hun rechten en hoe de organisatie daarmee omgaat. Burger moeten misschien wel vaker hun persoonsgegevens doorgeven voor verschillende aanvragen bij de organisatie. Door mensen actief te informeren over de manier waarop de organisatie omgaat met hun gegevens zal hier draagvlak voor worden gecreëerd.

De organisatie maakt van diverse kanalen en middelen gebruik om haar burgers actief te informeren over de nieuwe wet. Denk bijvoorbeeld aan artikelen in huis-aan-huisbladen, folders en de (gemeentelijke) website. Daarnaast worden burgers op het moment dat de organisatie gegevens van hen nodig heeft (nogmaals) geïnformeerd over de omgang van de organisatie met hun persoonsgegevens.

Partners/ bedrijven

Bedrijven waar de organisatie een opdracht aan geeft of een samenwerking mee aangaat krijgen een mail met het verzoek een samenwerkings- of een verwerkersovereenkomst af te sluiten.

6. Geautomatiseerde verwerkingen

Profilering (Artikel 22, AVG)

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de (gemeentelijke) website naar een bepaalde dienst kijkt, mag de organisatie geen actie ondernemen om de dienst aan te bieden. Organisaties mogen wel bekijken hoe vaak een

bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.

De organisatie maakt geen gebruik van profilering.

Big data en tracking

Door middel van Big data en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon (anonymiseren). Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de organisatie wordt uitgevoerd. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon.

Inzet van camera's

Binnen de organisatie wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet (art 151c GW).⁴ Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's.

7. Plichten van de organisatie

Register van verwerkingen (Artikel 30, AVG)

De organisatie is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de organisatie de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

In aanvulling op de bovenstaande elementen, neemt de organisatie nog enkele aanvullende aspecten mee in het register van verwerkingen, omdat ook deze aspecten per verwerking moeten worden bepaald om de legitimiteit te borgen. Deze aanvullende elementen zijn:

- de rechtsgrondslag op basis waarvan de persoonsgegevens worden verwerkt;
- als de rechtsgrondslag is dat het noodzakelijk is voor het voldoen aan een wettelijke verplichting of als het noodzakelijk is voor het uitvoeren van een taak in het algemeen belang of voor de uitoefening van het openbaar gezag, moet de betreffende wet die dit bepaalt worden vermeld;
- of het geven van de persoonsgegevens wettelijk verplicht is of noodzakelijk is voor het aangaan van een overeenkomst.

Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De organisatie voert deze uit wanneer een verwerking, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

⁴ <http://wetten.overheid.nl/BWBR0005416/2017-01-01>

Een gegevensbeschermingseffectbeoordeling is met name vereist in de volgende gevallen:

- a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;
- b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten; of
- c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

De Autoriteit Persoonsgegevens stelt een lijst op van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling verplicht dan wel uitgesloten is.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)
De organisatie heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de FG zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van het Autoriteit Persoonsgegevens. Het is niet de bedoeling dat de FG de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de (gemeentelijke) richtlijnen op het gebied van privacy.

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van de organisatie. Dit kan via het algemene telefoonnummer van de organisatie, als genoemd op de (gemeentelijke) website.

Datalekken (Artikel 33, 34, AVG)

We spreken van een datalek wanneer persoonsgegevens verloren raken of onrechtmatig verwerkt worden. Onder onrechtmatige verwerking valt onder andere ongeautoriseerde toegang tot persoonsgegevens door derden. Wanneer er een datalek heeft plaatsgevonden meldt de organisatie dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan het AP. 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 meldt de organisatie dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

Afsluiting

Als de organisatie een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de organisatie worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke (bestuurs)orgaan van de organisatie. Bij de Autoriteit Persoonsgegevens bestaat de voorkeur de klachtafhandeling tussen de organisatie en betrokkenen te doen plaatsvinden.⁵ Echter, mochten partijen er samen niet uitkomen, dan kan de betrokkene haar klacht in het kader van dit onderwerp eveneens rechtstreeks melden bij de Autoriteit Persoonsgegevens. Dit ongeacht de gebruikelijke opties ten aanzien van beroep en bezwaar.

⁵ <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruik-persoonsgegevens>

Dit privacyreglement treedt in werking na vaststelling door het college van burgemeesters en wethouders. Het reglement wordt ieder jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit reglement worden aangekondigd via de (gemeentelijke) kanalen. De meest actuele versie van het reglement is te vinden op www.overheid.nl.

Aldus vastgesteld door burgemeester en wethouders van gemeente Oostzaan op __-__-__,

R. Meerhof
Burgemeester

Aldus vastgesteld door burgemeester en wethouders van gemeente Wormerland op __-__-__,

P. C. Tange
Burgemeester

Aldus vastgesteld door het algemeen bestuur van OVER-gemeenten op __-__-__,

E. van Watteringen
Algemeen Directeur