Omgevingsdienst Rivierenland

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 846

14 augustus 2020

Officiële uitgave van de gemeenschappelijke regeling Omgevingsdienst Rivierenland

Privacybeleid Omgevingsdienst Rivierenland

Samenvatting
Dit privacybeleid beschrijft hoe de Omgevingsdienst Rivierenland (ODR) invulling geeft aan de wettelijke eisen uit de Algemene Verordening Gegevensbescherming (AVG) op het gebied van werken met persoonsgegevens. Dit geldt voor persoonsgegevens van klanten en medewerkers van de ODR. ODR geldt hierbij als verwerkingsverantwoordelijke in de zin van de Algemene verordening gegevensbescherming (AVG).

Het privacybeleid is onlosmakelijk verbonden met het informatieveiligheidsbeleid.

Dit beleid is van toepassing op de gehele organisatie, processen en systemen van de ODR.

De AVG regelt het algemene kader voor de omgang met persoonsgegevens binnen de landen van de Europese unie. De uitgangspunten van de AVG zijn:
- Rechtmatigheid, behoorlijkheid, transparantie
- Grondslag en doeleinden
- Dataminimalisatie
- Bewaartermijn
- Integriteit, vertrouwelijkheid en communicatie
- Delen met derden
- Rechten van betrokkenen

Het bestuur, het management en alle medewerkers hebben een cruciale rol bij het waarborgen van privacy. Dit beleid beschrijft de taken, rollen en verantwoordelijkheden van:
- Medewerkers
- MT
- Coördinatoren
- Functionaris gegevensbescherming
- Privacycoördinator
- Organisatiejurist
- Informatiemanager
- Adviseur informatiebeheer

Om privacy als integraal aspect te borgen binnen de taakuitvoering en naast de strategische kaders de AVG praktisch en laagdrempelig toe te kunnen passen door medewerkers in de dagelijkse werkzaamheden zijn naast dit beleid spelregels vastgesteld Deze spelregels zijn terug te vinden in het document “Spelregels ODR werken met persoonsgegevens”.

Inleiding
Binnen ODR worden persoonsgegevens verwerkt en gebruikt. Alle gegevens of informatie die naar een persoon te herleiden is, is een persoonsgegeven. Ook gegevens die indirect iets over een persoon zeggen, zijn persoonsgegevens.

Dit beleid geldt voor alle persoonsgegevens van klanten, ketenpartners en medewerkers van de ODR. Het uitgangspunt van het gebruik van persoonsgegevens is dat uitsluitend persoonsgegevens worden verwerkt en gebruikt die noodzakelijk zijn voor de uitvoering van de taken van de ODR. Dit zijn de taken die de ODR uitvoert in mandaat voor de deelnemende gemeenten en de Provincie Gelderland en de taken die de ODR uitvoert als openbaar lichaam in het kader van de Wet gemeenschappelijk regelingen (Wgr) en als werkgever. ODR geldt hierbij als verwerkingsverantwoordelijke in de zin van de Algemene verordening gegevensbescherming (AVG).

Dit beleid is van toepassing op de gehele organisatie, alle organisatieonderdelen, alle processen , informatiesystemen en persoonsgegevens van ODR. Het borgen van de privacy is onlosmakelijk verbonden met informatiebeveiliging. Dit privacybeleid is in lijn met het algemene beleid van de ODR, de relevante nationale en Europese wet- en regelgeving.

1. Doelstellingen van het beleid
Doelstelling van het beleid is dat op een verantwoordelijke wijze en binnen wettelijke kaders met privacygevoelige gegevens wordt omgegaan. Het wettelijk kader voor bescherming van persoonsgegevens

wordt - naast vele specifieke wetten - gegeven door de AVG. De eisen die de AVG stelt aan het verwerken van persoonsgegevens zijn dan ook zorgvuldig geïmplementeerd binnen ODR.

De ODR wil hiermee bereiken dat:
- Dit beleid de basis vormt op het gebied van privacy en dat alle medewerkers zich bewust zijn van de noodzakelijkheid van een zorgvuldige omgang met persoonsgegevens;
- De rechten van betrokkenen worden gerespecteerd en in procedures zijn verankerd;
- Het vertrouwen van betrokkenen in de overheid niet wordt beschaamd;
- Uitvoering van het privacybeleid binnen de ODR gezamenlijk en integraal wordt opgepakt, zodat de wettelijke eisten goed geïmplementeerd zijn;

- Het onderwerp zowel bestuurlijk als ambtelijk breed wordt gedragen, als onderdeel van zowel uitvoering van de wettelijke opgave, goed werkgeverschap, opdrachtnemerschap en opdrachtgeverschap;
- De kans op financiële schade door het oplopen van boetes en reputatieschade wordt geminimaliseerd;
- Iedere medewerker en bestuurders helpen bij het vergroten van bewustwording op het gebied van privacy.

1.1 Begrippenkader

Begrippen die voor een goede uitvoering van het privacybeleid van groot belang zijn en worden gehanteerd binnen de AVG zijn:
- Betrokkene: de natuurlijke persoon van wie de gegevens worden gebruikt (verwerkt).
- DB: het dagelijks bestuur van de ODR.
- Functionaris Gegevensbescherming (FG): de FG is de interne toezichthouder op de verwerking van persoonsgegevens. De FG moet in alle onafhankelijkheid zijn werkzaamheden uit kunnen voeren en ontvangt daarbij geen instructies van opdrachtgevers of verwerkers. Hij is aangemeld bij de AP als contactpersoon en aanspreekpunt voor de meldingen van datalekken. Hij functioneert als tussenpersoon tussen verschillende belanghebbenden en is daarmee ook een verlengstuk van de AP. De FG van de ODR is ook FG van de overige Gelderse Omgevingsdiensten.
- Governance ; de wijze waarop de daadwerkelijke implementatie van richtlijnen en strategie is gegarandeerd, zodat vereiste processen op de juiste manier worden gevolgd om te kunnen voldoen aan de wet- en regelgeving. Governance bevat het definiëren van rollen en verantwoordelijkheden, meten en rapporteren, nemen van acties om kwesties op te lossen.
- Inbreuk op persoonsgegevens (datalek):een inbreuk op de beveiliging die al dan niet per ongeluk op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
- Persoonsgegevens: alle informatie over een persoon of informatie die naar een persoon te herleiden is. Ook gegevens die indirect iets over iemand zeggen, zijn persoonsgegevens. Er zijn veel soorten persoonsgegevens. Voor de hand liggende gegevens, minder voor de hand liggende gegevens en gevoelige gegevens. Voorbeelden van persoonsgegevens:
  ° burgerservicenummer (BSN)
  ° naam
  ° adres
  ° woonplaats
  ° postcode / postbusnummer
  ° huisnummer
  ° geboortedatum
  ° geslacht
  ° burgerlijke staat
  ° telefoonnummer / faxnummer
  ° e-mailadres
  ° IP-adres
  ° IBAN bankrekeningnummer
  ° gegevens over inkomen, bezittingen en schulden
  ° gegevens over ras / etnische afkomst
  ° gegevens over godsdienst of levensovertuiging
  ° gegevens over gezondheid
  ° politieke voorkeur
  ° lidmaatschap vakbond
  ° seksuele voorkeur
  ° strafrechtelijke veroordelingen en daarmee verband houdende veiligheidsmaatregelen
- Privacybescherming: het omgaan met persoonsgegevens volgens de eisen in de AVG.

- Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, standaardiseren of combineren, afschermen, wissen of vernietigen van gegevens. Ook het publiceren van informatie op het internet kan zo'n verwerking zijn.
- Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die of dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. ODR heeft in de praktijd te maken met meerdere verwerkers waarmee verwerkersovereenkomsten zijn afgesloten.
- Verwerkingsverantwoordelijke: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst die of een ander orgaan dat, allen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In de relatie met de deelnemers in de gemeenschappelijke regeling van de ODR moet de ODR worden beschouwd al verwerkingsverantwoordelijke. Dat betekent dat ODR zelf verantwoordelijk is voor de naleving van de AVG en daarop aanspreekbaar is.

2. Juridisch kader – basiseisen uit de AVG
Bij de verwerking van persoonsgegevens staat bescherming van de persoonlijke levenssfeer van de betrokkenen voorop. Er moet immers worden voorkomen dat er op de persoonlijke levenssfeer van betrokkene wordt ingebroken.

De AVG is het algemene kader voor de omgang met persoonsgegevens binnen de Europese Unie. De AVG is de hoogste wetgeving voor privacybescherming en fungeert als een parapluwet die van toepassing is op alle verwerkingen van persoonsgegevens door zowel bedrijven als overheden.

2.1 De uitgangspunten van de AVG
De uitgangspunten van de AVG zijn:

<u>Rechtmatigheid, behoorlijkheid, transparantie</u>
Verwerking op rechtmatige, behoorlijke en transparante wijze (artikel 5 lid 1 sub a AVG). (accountability).

<u>Grondslag en doeleinden</u>
- Verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5 lid 1 sub b AVG);
- Alleen verwerking op één van de in de AVG opgenomen grondslagen (artikel 6 AVG).

<u>Dataminimalisatie</u>
ODR verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor een voorafgaand bepaald doel. ODR streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

<u>Bewaartermijn</u>
De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waar ze voor nodig zijn. Dit doel wordt beschreven in verschillende wetten, waardoor de bewaartermijnen van persoonsgegevens uiteen lopen.

<u>Integriteit, vertrouwelijkheid en communicatie</u>
ODR gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. ODR zorgt voor passende beveiliging van persoonsgegevens Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. ODR maakt daarom inzichtelijk op welke wijze persoonsgegevens worden verwerkt en beheerd. Dit is vastgelegd in het verwerkingsregister en de privacyverklaring.

<u>Delen met derden</u>
Een rechtstreeks gevolg van het uitvoeren van wettelijke taken en regelingen is het verwerken van persoonsgegevens. ODR deelt alleen persoonsgegevens als zij hiervoor een wettelijke grondslag heeft. In andere gevallen vragen wij hiervoor toestemming. Een betrokkene moet weten dat zijn of haar gegevens worden verwerkt worden wanneer een melding of aanvraag wordt gedaan. Het is hierom van belang dat ODR de betrokkene informeert hoe zijn of haar gegevens worden verwerkt.
Als wij informatie laten verwerken door derden dan maken wij hierover afspraken.

<u>Rechten van betrokkenen</u>

Verzoeken van betrokkenen op het gebied van rechten zoals 'het recht om vergeten te worden', 'het recht op inzage' en ' het recht op rectificatie' kunnen zonder belemmeringen worden gedaan bij ODR. De wijze waarop betrokkenen een beroep kunnen doen op hun rechten, staat beschreven in de privacyverklaring. De privacyverklaring is gepubliceerd op de website van de ODR.

3. Organisatie, taken en verantwoordelijkheden
In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot het onderwerp 'privacy' op welke plaatsen belegd zijn binnen de organisatie. Het dagelijks bestuur, het managementteam, de coördinatoren en alle medewerkers hebben een cruciale rol bij het waarborgen van privacy. Bewustwording is essentieel voor het borgen van privacy in de organisatie. Het is belangrijk dat iedereen die werkt met privacygevoelige informatie zich bewust is van het belang om hier zorgvuldig mee om te gaan. Op basis hiervan zet het MT dit beleid voor privacy op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het MT geeft een duidelijke richting aan het onderwerp 'privacy' en demonstreert dat zij bewust omgaan met privacy en bescherming van persoonsgegevens ondersteunt en zich hierbij betrokken voelt. Zij draagt het belang van 'privacy' uit, handhaaft het privacybeleid van en voor de hele ODR.

De tweede lijn (FG, privacycoördinator, organisatiejurist en informatiemanager ondersteunt, adviseert, coördineert en bewaakt of het MT zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

De rollen, taken en verantwoordelijkheden zijn samengevat in bijlage 1, governance gegevensbescherming. De inrichting van de governance op de gebieden van privacy (AVG) en informatieveiligheid overlapt zodanig dat hiervoor één governancedocument is opgesteld.

3.1 Governance
De governance is ingericht volgens de onderstaande uitgangspunten:

3.1.1 Dagelijks Bestuur
- Het dagelijks bestuur is eindverantwoordelijke voor de privacy en stelt als eindverantwoordelijke het privacybeleid vast.

3.1.2 Managementteam
- Het DB stelt het privacybeleid vast;
- Het MT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid;
- Het MT stelt onderliggend tactisch beleid en protocollen vast;
- Het MT is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en ziet erop toe dat de afdelingshoofden adequate maatregelen genomen hebben voor de bescherming van persoonsgegevens die onder hun verantwoordelijkheid valt.
- Het MT draagt zorg voor de rechtmatige verwerking van persoonsgegevens door de organisatie;
- Het MT bewaakt en draagt een integrale benadering van privacybewust handelen uit binnen de gehele organisatie;
- Het MT geeft sturing geven op het gebied van privacy.

3.1.3 Lijnmanagement
- De uitvoering van privacybeleid is een verantwoordelijkheid van de coördinatoren ;
- De afdelingshoofden zijn verantwoordelijk voor de uitvoering van het onderwerp 'privacy' voor de processen waarvoor zij verantwoordelijk zijn;
- De afdelingshoofden zien erop toe dat de coördinatoren adequate maatregelen genomen hebben voor het borgen van de privacy en bescherming van persoonsgegevens die onder hun verantwoordelijkheid valt;
- De afdelingshoofden zijn verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid;
- De afdelingshoofden/coördinatoren bewaken een zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar afdeling/team plaatsvindt;
- De coördinatoren monitoren of persoonsgegevens zorgvuldig worden verwerkt;
- De coördinatoren sturen bij wanneer nodig.

3.1.4 Medewerkers

Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht zorgvuldig en bewust met persoonsgegevens en privacy om te gaan. Daarnaast moet iedere medewerker, zowel vast als tijdelijk, intern of extern bekend zijn met de protocollen rondom incidenten en datalekken, ook zijn zij bekend met de spelregels "werken met persoonsgegevens". Bij vermeende incidenten of inbreuken maken zij hier direct melding van.

Bij privacybewust werken is de mens de zwakste schakel, alle medewerkers hebben onder ander de volgende verantwoordelijkheden:
- Privacybewust handelen en gedrag;
- Werken volgens de spelregels (spelregels ODR werken met persoonsgegevens);
- Op de hoogte zijn van de geldende werkprocessen (o.a. procedure meldplicht datalekken) op gebied van privacy;
- Bekend zijn met de locatie van de informatie over privacy, AVG en het werken met persoonsgegevens (intranet).

3.1.5 Functionaris Gegevensbescherming
Voor onafhankelijk advies, toezicht en controle op de kwaliteit van de uitvoering van het privacybeleid hebben de omgevingsdiensten Gelderland een FG aangesteld. De FG heeft een onafhankelijke positie in de organisatie. De werkzaamheden die een FG uitvoert staan genoemd in artikel 39 AVG. De FG van de omgevingsdiensten Gelderland is door de directeuren van de Gelderse omgevingsdiensten aangewezen.

De FG heeft een adviserende en toezichthoudende rol op de uitvoering van de AVG en is de contactpersoon van de Autoriteit Persoonsgegevens (AP).

3.2 Controle en verantwoording
Dit Strategisch Beleid is een verantwoordelijkheid van het dagelijks bestuur van de ODR. Het MT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over het onderwerp privacy aan respectievelijke portefeuillehouders. Het MT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

De controle en verantwoording van informatieveiligheid valt uiteen in twee onderdelen:
- Informatiebeveiliging
  De informatiemanager rapporteert over de uitvoering van het informatieveiligheidsbeleid en het naleven van uitvoeringsrichtlijnen aan de directeur/MT.
- Privacy
  Over naleving van de AVG rapporteert de FG jaarlijks aan het dagelijks bestuur. De rapportage bevat elementen waaruit duidelijk wordt op welke onderwerpen aan de AVG wordt voldaan en waar verbetering nodig is. Hieruit volgen aanbevelingen waarbij de prioriteit is weergegeven. Door onderdelen die verbetering vereisen uit te voeren neemt de Omgevingsdienst verantwoordelijkheid om aan de AVG te voldoen.

Bijlage bij:
- Strategisch privacybeleid
- Strategisch informatieveiligheidsbeleid 2020-2023

Wie	Rollen en Taken	PB	IB
Dagelijks Bestuur	Eindverantwoordelijke	X	X
	Politiek verantwoordelijk voor een passend niveau gegevensbescherming	X	X
	Stelt beleid vast	X	X
MT	Verantwoordelijk voor uitvoering van organisatiebrede vraagstukken ten aanzien van gegevensbescherming	X	X
	Verantwoordelijk voor de inrichting en werking van beveiligingsorganisatie.	X	X
	Voert regie en houdt toezicht op zijn processen inzake Gegevensbescherming	X	X
	Aantoonbaar compliant aan wetten en kaders	X	X
	Dataclassificatie van systemen en gegevens (-verzamelingen)		X
	Risicoafweging en treffen maatregelen	X	X
	Medewerkers meenemen in hun verantwoordelijkheid	X	X
	Vaststellen gewenste niveau van gegevensbescherming en uitgangspunten (zoals bijv gebruik standaard VNG)		X
	Stelt uitvoeringsrichtlijnen vast (gedragsregels, Toepassingsregels)	X	X
Afdelingshoofd / Coördinatoren / Proceseigenaren / Procesverantwoordelijke	Operationele verantwoordelijkheid voor systemen en processen		X
	Voert regie en houdt toezicht op zijn processen inzake gegevensbescherming	X	X
	Stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesysteem vast.		X
	Het treffen van maatregelen op basis van risicomanagement		X
	Zorgen voor bewustwording onder personeel	X	X
	Beheersen van en rapporteren over incidenten	X	X
	Verantwoordelijke voor implementatie juiste beveiligingsniveau		X
	Manager kan taken opdragen aan medewerker blijft echter verantwoordelijk	X	X
Medewerkers	Zijn verantwoordelijk ten aanzien van de veiligheid van gegevens in hun dagelijkse werkprocessen	X	X

	Werken volgens en binnen richtlijnen, kaders en gedragsregels	X	X
Functionaris Gegevensbescherming	Intern toezichthouder verwerking persoonsgegevens / naleving van de AVG	X	X
	Verantwoordelijk voor het toezicht op de naleving van de privacywetten en –regels	X	X
	Adviseert en informeert de organisatie en medewerkers over allerlei privacy gerelateerde zaken	X	X
	Verantwoordelijk voor het afhandelen van vragen en klachten	X	X
	Adviseert en ondersteunt bij privacy impact assessments (PIA's)	X	X
	Contactpersoon AP	X	X
	Rapporteert aan het Dagelijks Bestuur (DB) / directeuren	X	X
Informatiemanager	Verantwoordelijk voor het implementeren van, adviseren over en toezicht houden op het informatiebeveiligingsbeleid		x
	Formuleert IB beleid		X
	t Formuleert het informatiebeveiligingsplan (IBP)		X
	Controle op uitvoering beveiligingsplan		X
Privacycoördinator	Interne contactpersoon voor privacygerelateerde zaken	X	
	Bewaakt en beheert het register van incidenten en datalekken	X	
	Contactpersoon FG bij mogelijke inbreuken, incidenten, datalekken	X	X
Organisatiejurist	Adviseert over juridische vraagstukken rondom privacy en het verwerken en beschermen van persoonsgegevens	X	
	Adviseert over het register van verwerkingen	X	
	Adviseert over en sluit verwerkersovereenkomsten af	X	
	Handelt verzoeken met betrekking tot rechten van betrokkenen af	X	
	Vormt dossiers van de achterliggende stukken	X	
	Bewaakt het inzageproces en schaalt indien van toepassing op naar de klachtenprocedure	X	X
Adviseur informatiebeheer	Verantwoordelijk voor het bewaken en beheren van het verwerkingsregister	X	X
Controller	Sparring partner voor FG, informatiemanager, privacy coordinator bewaakt koppeling privacy- en informatiebeveiligings-doelen aan organisatiebrede inspanning om 'in control' te worden	X	X