

Privacybeleid Omgevingsdienst Zuid-Holland Zuid 2025

Vastgesteld door het dagelijks bestuur op 10 april 2025

Inhoud

1. Inleiding
2. Begripsbepalingen
3. Visie
4. Doel
5. Reikwijdte
6. Principes voor de verwerking van persoonsgegevens
7. Rollen en Verantwoordelijken

1. Inleiding

De Omgevingsdienst Zuid-Holland Zuid (OZHZ) werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. OZHZ verzamelt deze gegevens om zowel de eigen taken als de taken in opdracht van gemeenten en provincie goed uit te kunnen voeren. Bij de eigen taken gaat het bijvoorbeeld om het voeren van het personeelsbeleid en contractenbeheer. Voor gemeenten en provincie voert OZHZ taken uit op het gebied van vergunningverlening, toezicht, handhaving en advisering in de fysieke leefomgeving, en is in die zin te kwalificeren als 'verwerker' als bedoeld in de AVG. Om deze taken goed te kunnen uitvoeren is het noodzakelijk dat OZHZ persoonsgegevens verwerkt. Inwoners moeten erop kunnen vertrouwen dat OZHZ zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. OZHZ is zich hiervan bewust en wil daarom met dit beleid aangeven hoe hij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Wet politiegegevens (Wpg)

OZHZ heeft ook te maken krijgen met verwerkingen van persoonsgegevens op grond van de Wpg. Dan gaat het om politiegegevens. Hierbij kan men denken aan de verwerkingen die de buitengewone opsporingsambtenaren (BOA's) verrichten bij hun onderzoek naar en opsporing van strafbare feiten. Het beleid over het verwerken van politiegegevens staat in het Addendum Privacybeleid OZHZ vanwege de Wet politiegegevens van 11 november 2021 (<https://lokaleregelgeving.overheid.nl/CVDR663912/1>). Met uitzondering van de verwijzingen naar het privacy- en informatiebeveiligingsbeleid, die in 2025 zijn geactualiseerd, is dat document nog steeds actueel. In het kader van de Wpg geldt OZHZ niet als verwerker, maar als verwerkingsverantwoordelijke.

Geldigheidsduur

Het voorliggende privacybeleid is vastgesteld door het dagelijks bestuur op 10 april 2025, met terugwerking naar 1 januari 2025. Het wordt tenminste eens per drie jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is, bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van bepaalde risicoanalyses, kan besloten worden tot een tussentijdse herziening. Ook als de samenwerking van de omgevingsdiensten in Zuid-Holland op het terrein van informatiebeveiliging en privacy verder gevorderd is kan dat aanleiding zijn om het beleid of de uitvoering ervan te herzien.

Het Privacybeleid Omgevingsdienst Zuid-Holland Zuid, geactualiseerde versie 2020, van 17 september 2020 is ingetrokken.

2. Begripsbepalingen

De definities van artikel 4 van de AVG hebben in dit beleidsdocument dezelfde betekenis.

3. Visie

Privacy gaat over het recht van alle inwoners en medewerkers op de bescherming van hun persoonlijke levenssfeer. Voor het realiseren van onze maatschappelijke doelen en de uitvoering van onze wettelijke taken is gegevensverzameling en -uitwisseling van groot belang. Het beschermen van persoonsgegevens en een rechtmatige en veilige gegevensverwerking is een essentieel onderdeel van die gegevensuitwisseling. Daarom verwerken wij persoonsgegevens op een rechtmatige, behoorlijke en transparante manier, conform wet- en regelgeving. Wij willen de gegevens van anderen alleen verwerken als het echt nodig is.

OZHZ wil zich actief inzetten om het gebruik van persoonsgegevens tot een noodzakelijk minimum te beperken. De komende jaren zet OZHZ in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Hiertoe werkt OZHZ samen met de andere omgevingsdiensten in Zuid-Holland. Een goede privacy 'boekhouding' is noodzakelijk voor het goed functioneren van OZHZ en de basis voor het beschermen van rechten van inwoners en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen OZHZ.

4. Doel

Met dit privacybeleid geeft OZHZ een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan OZHZ persoonsgegevens verwerkt of laat verwerken. Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen OZHZ, zoals handreikingen, werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken en inzageverzoeken.

Naast dit privacybeleid stelde het DB op 6 maart 2025 het Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025 – 2029 vast (<https://lokaleregelgeving.overheid.nl/CVDR736226/1>). Hierin zijn richtinggevend kaders opgenomen voor maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het privacybeleid kan daarom niet los worden gezien van het informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer

Iedereen werkzaam binnen OZHZ is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. OZHZ verlangt van al zijn medewerkers en alle personen die werkzaam zijn voor OZHZ dat de voorschriften van dit privacybeleid worden opgevolgd en actief worden uitgedragen.

5. Reikwijdte

OZHZ verzamelt en gebruikt persoonsgegevens van inwoners, van medewerkers van bedrijven en instellingen en andere natuurlijke personen (hierna te noemen: betrokkenen).

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens OZHZ, waaronder:

1. De verwerking van persoonsgegevens binnen de eigen bedrijfsprocessen.
2. De verwerking van persoonsgegevens die is uitbesteed of op een andere manier is georganiseerd, zoals een externe verwerker die voor OZHZ bepaalde diensten verricht.
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

6. Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. OZHZ onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag

Persoonsgegevens worden door OZHZ slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien

hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij OZHZ voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

Welbepaalde doeleinden

OZHZ verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat OZHZ alleen die persoonsgegevens verwerkt die noodzakelijk zijn om een specifiek doel te bereiken en ze mogen dan niet gebruikt worden om een ander doel te bereiken. Dit mag alleen in geval van een verdere rechtmatige verwerking.

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. OZHZ voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, voert OZHZ het op die manier uit. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan zal OZHZ het op die manier verwerken.

Juiste en actuele gegevens

OZHZ zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn, gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. OZHZ neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Gegevens worden op tijd vernietigd

OZHZ stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en selectielijsten. Gemeenten en provincie hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard. OZHZ hanteert deze selectielijsten.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt OZHZ de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. OZHZ bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

OZHZ neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. OZHZ handelt hierbij in overeenstemming met het vastgestelde informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht OZHZ om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Default en Privacy by Design

OZHZ houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt Privacy by Design genoemd. OZHZ draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt OZHZ Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens, voor zover aan hen hiervoor bevoegdheden zijn toegerekend. Deze bevoegdheden worden verleend op grond van het binnen OZHZ geldende beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. OZHZ hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij OZHZ, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de externe toezichthouder, de Autoriteit Persoonsgegevens, en soms bij de getroffen betrokkenen. OZHZ registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in de procedure meldplicht datalekken.

Samenwerking

OZHZ schakelt soms derden in om in zijn opdracht persoonsgegevens te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van OZHZ. De AVG verplicht OZHZ tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten, waarin het zorgvuldig omgaan met persoonsgegevens wordt geborgd.

Samenwerkingsverbanden

Verder werken gemeenten samen met andere (overheids-)organisaties om een taak van algemeen belang uit te voeren. Een voorbeeld daarvan is OZHZ. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel) of van een relatie verwerkingsverantwoordelijke – verwerker. Dit laatste is het geval bij de taken die OZHZ uitvoert in opdracht van gemeenten en provincie. Met de gemeenten en provincie is dan ook een verwerkersovereenkomst aangegaan op basis van het landelijke model van de Informatiebeveiligingsdienst van de VNG.

Daarnaast schakelt OZHZ ook zelf externe verwerkers in. Een speciale samenwerking betreft die met de gemeente Dordrecht, i.c. de Servicegemeente (SGD). Deze verricht in opdracht van OZHZ diverse bedrijfsvoeringstaken, waarbij zij voor OZHZ persoonsgegevens verwerkt. SGD kwalificeert in die relatie als verwerker. Daarom is tussen OZHZ en SGD een verwerkersovereenkomst gesloten.

Doorgifte buiten de EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie

OZHZ informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat hij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. OZHZ heeft daarom een privacyverklaring op zijn website opgenomen. Alleen indien de wet anders bepaalt, wijkt OZHZ van deze informatieplicht af. Ook het register van verwerkingen staat op de website van OZHZ. Zie <https://www.ozhz.nl/privacybeleid/>.

Rechten van betrokkenen

Betrokken hebben het recht om te vernemen welke persoonsgegevens OZHZ over hen heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Zij kunnen hun recht uitoefenen onder andere via een webformulier dat te vinden is op de website van OZHZ. Daar is ook nadere informatie over de rechten van betrokkenen opgenomen.

Geschillenbeslechting

Indien de betrokkene van mening is dat OZHZ niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij/zij contact opnemen met de Privacy Officer (PC). De betrokkene heeft ook het recht een klacht in te dienen bij de Functionaris Gegevensbescherming (fg@rechtsteden.nl). Indien de betrokkene dit wenst kan hij/zij daarna nog een klacht bij de Autoriteit Persoonsgegevens indienen, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

Onder de verantwoordelijkheid van het dagelijks bestuur vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt OZHZ, samen met de gemeenten in de Drechtsteden, over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. OZHZ stelt voldoende middelen ter beschikking opdat de FG adequaat toezicht kan uitvoeren.

Register van verwerkingen

OZHZ beschikt over een register van verwerkingen, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt. Het register staat op de website van OZHZ.

Data Protection Impact Assessment (DPIA)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet OZHZ een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. OZHZ voert in dat geval een risico analyse (DPIA) uit. Als uit de DPIA blijkt dat er inderdaad risico's zijn verbonden aan de verwerking, dan moet OZHZ voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet OZHZ met de AP overleggen, voordat hij met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd.

Functionaris gegevensbescherming (FG)

OZHZ is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt. OZHZ is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan het DB van zijn werkzaamheden, bevindingen en aanbevelingen.

Plan-Do-Check-Act (PDCA) Cyclus

OZHZ streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat OZHZ weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de organisatie en bij bestuur voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd.

Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies en interne berichtgeving. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt. Daarnaast worden er verplichte informatieveiligheids- en privacy-trainingen gehouden voor nieuwe medewerkers. Ook wordt een e-learningmodule aangeboden op het gebied van informatiebeveiliging en privacy.

7. Rollen en Verantwoordelijken

Hieronder is op hoofdlijnen aangegeven hoe de bescherming van persoonsgegevens is georganiseerd binnen OZHZ.

	Verantwoordelijk	
R	Feitelijk verantwoordelijk	Managers: proceseigenaren. Medewerkers: verwerken van persoonsgegevens.
C	Eindverantwoordelijk	Dagelijks bestuur.
A	Adviserend	PC. Adviseur informatieveiligheid en CISO. FG.
I	Geïnformeerd Toezicht	Algemeen bestuur. FG. Belanghebbenden en betrokkenen.

Het DB

Het DB is bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving binnen OZHZ en stelt het privacybeleid en informatiebeveiligingsbeleid vast.

Het management

Het management is operationeel eindverantwoordelijk voor de naleving van de privacywetgeving voor processen binnen de eigen units en de hele organisatie, alsmede voor de uitvoering van het privacybeleid, waaronder het doen uitvoeren van een DPIA indien nodig. De managers zijn verantwoordelijk voor het doen volgen van trainingen door werknemers binnen de eigen unit en zorgen voor het registreren van hun gegevensverwerkingen in het register van verwerkingen. Zij bevorderen een duurzame privacycultuur.

De FG

De FG is verantwoordelijk voor het toezicht op de naleving van de AVG en heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG monitort veranderingen in privacywetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan. De FG adviseert bij privacy-klachten, verzoeken van betrokkenen, datalekken en DPIA's. Voor de uitvoering van zijn taken beschikt de FG over controle- en monitoringbevoegdheden met toegang tot informatie. De FG brengt jaarlijks verslag uit van zijn werkzaamheden en bevindingen en doet aanbevelingen.

De PC

De PC is het eerste aanspreekpunt rondom privacy-gerelateerde vraagstukken en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. Deze ondersteuning ziet onder andere op het opstellen van privacybeleid, formats en procedures, verwerkersovereenkomsten, het bijhouden van het register van verwerkingen, advisering bij DPIA's, het behandelen van verzoeken van betrokkenen, het afhandelen van datalekken en training en bewustwording van medewerkers.