

# Privacybeleid gemeente Ooststellingwerf



Februari 2023

## **Privacybeleid Gemeente Ooststellingwerf**

Binnen de gemeente Ooststellingwerf wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. In deze tijd gaat ook de gemeente mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Het bestuur en management spelen een cruciale rol bij het waarborgen van privacy. De gemeente Ooststellingwerf geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Dit privacybeleid van de gemeente Ooststellingwerf is in lijn met het algemene beleid van de gemeente en de relevante lokale, regionale, nationale en Europese wet- en regelgeving.

In dit privacybeleid laat de gemeente Ooststellingwerf zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy en wat er wettelijk wel en niet verantwoord is.

### **1. Reikwijdte**

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden.

### **2. Verantwoordelijke**

De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de bestuursorganen worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeesters en Wethouders (college van B&W) en de Raad.

### **3. Uitgangspunten**

De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. De gemeente houdt zich hierbij aan de volgende uitgangspunten:

#### *Rechtmatigheid, behoorlijkheid, transparantie*

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

#### *Grondslag en doelbinding*

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.

#### *Dataminimalisatie*

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

### *Bewaartermijn*

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

### *Integriteit en vertrouwelijkheid*

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

### *Delen met derden*

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken zijn vastgelegd in een (verwerkers)overeenkomst en voldoen aan de eisen van de Algemene Verordening Gegevensbescherming (AVG) en de Wet politiegegevens (Wpg).

### *Subsidiariteit*

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

### *Proportionaliteit*

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot en met de verwerking te dienen doel.

### *Rechten van betrokkenen*

De gemeente honoreert alle rechten van betrokkenen.

## **4. Wettelijke kaders voor de omgang met gegevens**

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:

- Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming
- Wet politiegegevens (Wpg)
- Besluit politiegegevens (Bpg)
- Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa)

De volgende begrippen worden in de AVG (artikel 4 AVG) en de Wpg gebruikt (artikel 1 Wpg):

### *Betrokkene*

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

### *Verwerker*

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

### *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. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

### *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 Data Privacy Impact Assessment (DPIA).

### *Verwerkingsverantwoordelijke*

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

### *Verwerking*

Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

## **5. Verwerken van persoonsgegevens**

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG en de Wpg valt onder een verwerking:

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

### *Doeleinden (artikel 5 AVG, artikel 3 Wpg)*

Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verwerkt. Persoonsgegevens mogen verder worden verwerkt voor andere doelen, als die doelen verenigbaar zijn met het oorspronkelijke verzameldoel. 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:

- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking

### *Uitvoering van de dagelijkse politietaak (artikel 8 Wpg)*

De Wpg kent geen grondslagen voor verwerking van persoonsgegevens zoals de AVG. De Wpg geeft aan dat politiegegevens verwerkt kunnen worden voor het uitvoeren van de dagelijkse politietaak.

### *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. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De AVG en de Wpg gaan uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de AVG en de Wpg 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. Voor wat betreft politiegegevens, zijn deze vereisten beschreven in de Aanwijzing Wet politiegegevens en de rol van de officier van justitie.

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

#### *Doorgifte (artikel 44 t/m 50 AVG)*

De gemeente geeft geen persoonsgegevens door aan een land buiten de Europese Unie (EU), Europese Economische Ruimte (EER) of een internationale organisatie.

#### *Doorgifte (artikel 15 t/m 20 Wpg)*

Politiegegevens kunnen aan andere landen of internationale organisaties worden doorgegeven. Bij het verstrekken van de politiegegevens moet sprake zijn van een zwaarwegend belang.

## **6. Transparantie en communicatie**

#### *Wet open overheid (Woo)*

Via de Wet open overheid kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt. Politiegegevens vallen niet onder de Woo.

#### *Wet hergebruik van overheidsinformatie*

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

#### *Informatieplicht (artikel 13,14 AVG, artikel 24a, 24b Wpg)*

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente 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 gemeente 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 en vernietiging*

De AVG maakt geen onderscheid tussen verwijderen en vernietigen. De gemeente 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.

De Wpg maakt wel onderscheid tussen verwijderen en vernietigen van gegevens. Als de gegevens verwijderd worden, zijn zij nog niet definitief weg. Ze komen als het ware achter een digitaal schot te staan en zijn niet meer in te zien. Alleen als mocht blijken dat we de gegevens nodig hebben voor een klachtenprocedure of omdat er verantwoording over moet worden afgelegd, dan kunnen de gegevens opgevraagd worden.

Als er een groot opsporingsonderzoek moet worden verricht wat een grote impact heeft op de rechtsorde, dan mogen deze gegevens opnieuw verwerkt en dus ook geraadpleegd worden. Dit kan alleen als de officier van justitie daar opdracht voor geeft. Vernietigen is een definitieve handeling. De gegevens zijn niet meer terug te halen.

### *Rechten van betrokkenen (artikel 13 t/m 20 AVG, artikel 24 t/m 28 Wpg)*

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:

1. Recht op informatie: betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
2. Inzagerecht: betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
3. Correctierecht: als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
4. Recht van verzet: betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
5. 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.
6. Recht op bezwaar: betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.
7. Recht op overdraagbaarheid van gegevens: Dit recht is alleen in de AVG opgenomen. Betrokkenen hebben het recht om persoonsgegevens in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen.

### *Indienen van verzoek*

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan schriftelijk of via DigiD ingediend worden. De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de gemeente 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 gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

## **7. Geautomatiseerde verwerkingen**

### *Profiling (artikel 22 AVG, artikel 7a Wpg)*

Profiling 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 profiling wat duidelijker te maken gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten 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 profiling.

- De gemeente Ooststellingwerf maakt geen gebruik van profiling.

### *Big data onderzoek en tracking*

Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente 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.

- De gemeente Ooststellingwerf maakt geen gebruik van Big data en tracking.

### *Inzet van camera's*

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht. 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. Het gebruik van cameratoezicht in het gemeentehuis en op de gemeentewerf is met stickers en borden kenbaar gemaakt op het terrein en in de gebouwen.

## **8. Plichten van de gemeente**

### *Register van verwerkingen (artikel 30 AVG, artikel 31d Wpg)*

De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente 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.

Aanvullend op de AVG wordt voor politiegegevens de volgende informatie opgenomen in het register:

- Categorieën van gegevens die worden doorgegeven buiten de EU;
- Toekenning van autorisaties;
- Rechtsgrondslag voor werking van de gegevens.

### *Gegevensbeschermingseffectbeoordeling (artikel 35 AVG, artikel 4c Wpg)*

Met een gegevensbeschermingseffectbeoordeling worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

### *Aanstellen van een Functionaris voor gegevensbescherming (artikel 37 t/m 39 AVG, artikel 36 Wpg)*

De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de Autoriteit Persoonsgegevens (AP).

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de Functionaris voor Gegevensbescherming van de gemeente Ooststellingwerf via: [privacy@ooststellingwerf.nl](mailto:privacy@ooststellingwerf.nl)

### *Datalekken (artikel 33,34 AVG, artikel 33a Wpg)*

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Een datalek die nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van betrokke(nen), meldt de gemeente zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de 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 gemeente dit aan de betrokkenen in eenvoudige en duidelijke taal. Als politiegegevens betrokken zijn bij het datalek wordt de betrokkene niet altijd geïnformeerd. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

## **9. Afsluiting**

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenprocedure van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

## **10. Inwerkingtreding**

Dit privacybeleid treedt in werking na vaststelling door het college van burgemeesters en wethouders. Het beleid wordt ieder jaar geëvalueerd en indien nodig herzien. Bij wijziging wordt het geactualiseerde beleid ter vaststelling aangeboden aan het college. Aanpassingen van dit beleid worden aangekondigd via het digitale gemeenteblad van de gemeente Ooststellingwerf.

*Disclaimer:*

*Dit product is een eenvoudige en begrijpbare vertaling van de huidige privacywetgeving en gebaseerd op de AVG en de Wpg. Vanzelfsprekend is de toepasbare wet-en regelgeving altijd leidend en kunnen er geen rechten ontleend worden aan dit document.*