Gemeente IJsselstein

GEMEENTEBLAD

Officiële uitgave van de gemeente IJsselstein

Nr. 567026

24 december 2025

Privacybeleid gemeente IJsselstein

1. Inleiding

Binnen de gemeente IJsselstein wordt veel gewerkt met persoonsgegevens van inwoners, ondernemers medewerkers en (keten)partners. Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. 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. Nieuwe technologische voorzieningen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij 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).

Geldigheidsduur
Dit beleid is besproken geaccordeerd op 30 april 2025 door het managementteam. Het beleid wordt tenminste een keer per vier jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld in het geval van grote organisatorische veranderingen, wetswijzigingen, uitkomsten van DPIA's, o.i.d.) kan het college besluiten tot een tussentijdse herziening.

2. Begripsbepalingen

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

3. Visie

De komende jaren zet de gemeente in op het verhogen van de privacy bewustwording en verdere professionalisering van privacy in de organisatie. Privacy bewustwording is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van inwoners, ondernemers, medewerkers en (keten)partners. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van medewerkers essentieel voor privacy binnen de gemeente.

4. Doel

De gemeente IJsselstein geeft door middel van dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Ook is dit beleid bedoeld om de belangen van betrokkenen, bijvoorbeeld inwoners en ondernemers, centraal te stellen. 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 de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet Maatschappelijke Ondersteuning.

Naast dit door het college vastgestelde privacybeleid is er ook informatiebeveiligingsbeleid. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoonsgegevens) te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

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

5. Wettelijk kader

Het privacybeleid van de gemeente IJsselstein is in lijn met de geldende wet- en regelgeving. De Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet politie gegevens (hierna: Wpg) zijn daarbij het centrale kader.

De AVG is sinds 25 mei 2018 van toepassing in de hele Europese Unie (EU). De AVG geldt voor iedereen die persoonsgegevens verwerkt. Elke EU-lidstaat moet op een aantal punten onder de AVG zelf nog wetgeving maken. In Nederland is dit voor een belangrijk deel gebeurd in de Uitvoeringwet Algemene Verordening Gegevensbescherming (hierna: de UAVG).

In het geval de gemeente strafbare feiten opspoort, valt de daarmee samenhangende verwerking van persoonsgegevens onder de reikwijdte van de Wpg. Voorbeeld hiervan is het verwerken van persoonsgegevens door de gemeentelijke Buitengewoon opsporingsambtenaar (hierna: BOA). Voor verwerkingen onder de Wpg is een addendum bij dit privacybeleid opgesteld.

Voor de omgang met persoonsgegevens gelden de volgende (overige) wettelijke kaders:
- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
- Specifieke wet- en regelgeving die invulling geven aan de bescherming van persoonsgegevens binnen een bepaald domein (bijvoorbeeld de Wet Maatschappelijke Ondersteuning, Jeugdwet, Wet politiegegevens, Participatiewet, Wet basisregistratie personen, Archiefwet, Wet open overheid).

6. Principes voor de verwerking van persoonsgegevens

De AVG kent een aantal basisprincipes, in de AVG 'beginselen' genoemd. Iedereen, dus ook de gemeente, die persoonsgegevens verwerkt, moet zich hieraan houden en dit kunnen aantonen.

A) Rechtmatige grondslag
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Voor de verwerking van een persoonsgegeven is altijd een wettelijke grondslag nodig. Daarnaast worden persoonsgegevens alleen verwerkt indien dit noodzakelijk is voor het doel waarvoor ze worden verwerkt. Aan de hand van het verwerkingsregister wordt per verwerking aangegeven wat hiervoor de grondslag is en wat het doel van de verwerking is. Bij de verwerking van persoonsgegevens worden de beginselen van proportionaliteit en subsidiariteit in acht genomen. Dit betekent dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot en met de verwerking te dienen doel en dat voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, de inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk moet worden beperkt.

In de AVG (artikel 6 lid 1 sub a t/m f) staan de volgende zes grondslagen voor het verwerken van persoonsgegevens opgenomen:
a. De gemeente heeft toestemming van de persoon om wie het gaat.
b. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
c. Het is noodzakelijk om gegevens te verwerken omdat de gemeente hiertoe wettelijk verplicht is.
d. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
e. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang uit te voeren/openbaar gezag uit te oefenen.
f. Verwerking voor de uitoefening door de gemeente in het kader van de uitoefening van haar taken.

Veelal vloeit de grondslag voor een verwerking bij de gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

B) Welbepaalde doeleinden
De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. De gemeente mag dus niet alvast persoonsgegevens verzamelen omdat deze misschien in de toekomst van pas gaan komen.

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Verdere verwerking van persoonsgegevens is toegestaan als die verwerking verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld, er zich geen nadelige effecten voordoen voor de betrokken dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van wet- en regelgeving.

C) Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor deze persoonsgegevens 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. De gemeente voert, voordat de verwerking start, een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van wet- en regelgeving.

D) Minimale gegevensverwerking
De gemeente streeft zodoende naar 'minimale gegevensverwerking'. Dit betekent dat waar mogelijk minder of geen persoonsgegevens worden verwerkt. Dit betekent ook dat de gemeente alleen de gegevens mag verwerken passend bij het (vooraf bepaalde) doel. De gemeente verwerkt niet meer gegevens dan noodzakelijk om het doel te bereiken.

E) Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die accuraat, toereikend, ter zake dienend en niet bovenmatig zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, rectificeren en/of te wissen.

F) Gegevens worden op tijd vernietigd
Zodra de persoonsgegevens niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld, zal de gemeente deze persoonsgegevens moeten verwijderen. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie documenten hoelang deze moeten worden bewaard. Deze selectielijsten zijn vastgesteld door de Vereniging van Nederlandse Gemeenten (hierna: "de VNG") en worden door de gemeente gehanteerd.

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

G) Integriteit en vertrouwelijkheid
De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid. Dit beleid verplicht de gemeente 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
De gemeente 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 uitganspunt wordt privacy by design (PbD) genoemd. De gemeente draagt er zorg voor dat de concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacyvriendelijk 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 toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldend beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente 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.

Datalekken
De gemeente houdt zich aan de AVG-vereisten met betrekking tot datalekken en beveiligingsincidenten door een register bij te houden van alle datalekken. Hierin is vastgelegd of een beveiligingsincident heeft geleid tot een datalek en, indien dat het geval is, of het datalek is gemeld en welke corrigerende maatregelen er zijn getroffen om de risico's ten gevolge van het datalek te mitigeren.

Wanneer sprake is van een (mogelijk) datalek, en de inbreuk waarschijnlijk een (hoog) risico vormt voor de rechten en vrijheden van degenen wiens persoonsgegevens bij de inbreuk betrokken waren, zal een melding moeten worden gemaakt bij de Autoriteit Persoonsgegevens. De melding aan de Autoriteit Persoonsgegevens dient onmiddellijk, maar uiterlijk 72 uur nadat er kennis is genomen van het datalek, te worden gemeld bij de Autoriteit Persoonsgegevens. Bij het niet halen van deze termijn, dient er een motivering van de vertraging bij de melding worden gevoegd. Op het moment dat vaststaat dat het datalek een hoog risico met zich meebrengt voor betrokkenen, dan meldt de gemeente het datalek ook aan betrokkenen.

H) Samenwerking
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.
Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

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.

I) Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij 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. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

Rechten van betrokkenen
De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar 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:

- **Recht op informatie (artikelen 13 en 14 AVG):**
  Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.
- **Inzagerecht (artikel 15 AVG):**
  Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.
- **Correctierecht (artikel 16 AVG):**
  Als gegevens duidelijk niet kloppen, kan betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.
- **Recht om vergeten te worden/recht op vergetelheid (artikel 17 AVG):**
  Heeft betrokkene toestemming gegeven om gegevens te verwerken, dan heeft betrokkene het recht om die gegevens te laten verwijderen. Bijvoorbeeld ook als de verwerking onrechtmatig gebeurt.
- **Recht op beperking van verwerking (artikel 18 AVG):**
  In bepaalde situaties hebben betrokkenen er recht op dat hun persoons gegevens (tijdelijk) niet gebruikt worden
- **Recht op overdraagbaarheid/ dataportabiliteit (artikel 20 AVG):**
  Dit recht houdt in dat een betrokkene de gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machine leesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hemzelf verstrekte gegevens.
- **Recht van bezwaar (artikel 21 AVG):**
  Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.
- **Recht op een menselijke blik bij besluiten/non profiling (artikel 22 AVG):**

Als op basis van automatisch verwerkte gegevens een besluit over iemand is genomen, kan iemand een nieuw besluit verlangen waar de gegevensdoor een mens worden beoordeeld.

Indienen van verzoek/geschillenbeslechting
Om gebruik te maken van deze rechten kan de betrokkene een verzoek indienen. De gemeente heeft vanaf ontvangst van het verzoek vier weken de tijd om een besluit te nemen op het verzoek. Wordt deze termijn overschreden, dan kan betrokkene de gemeente in gebreke stellen of een klacht indienen bij de FG. Voordat een verzoek in behandeling kan worden genomen, dient de identiteit van betrokkene vastgesteld te worden. Dit om fraude te voorkomen.

De gemeente voldoet aan het verzoek, tenzij er gerechtvaardigde gronden zijn om een verzoek af te wijzen. Een betrokkene heeft het recht om bezwaar te maken tegen de beslissing.

J) Verantwoording
Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad 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 de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister
De gemeente is als verwerkingsverantwoordelijke verplicht om een register van de verwerkingsactiviteiten bij te houden conform artikel 30 AVG. Dat register bevat de volgende gegevens:
- Naam en contactgegevens van de gemeente en FG;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers;
- Indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie
- Indien van toepassing, de beoogde bewaartermijnen
- Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De proceseigenaar is verantwoordelijk voor verwerkingen en relevante wijzigingen in het bestaande verwerkingenregister. De Privacy Office heeft daarbij een ondersteunende en adviserende rol. Daarnaast draagt de Privacy Office er zorg voor dat deze nieuwe verwerkingen en relevante wijzigingen in het register opgenomen worden.

Data protection impact assessment (DPIA)
De gemeente is verplicht om een 'data protection impact assessment' (hierna: DPIA) uit te voeren in het geval zij van plan is persoonsgegevens te verwerken die waarschijnlijk een hoog privacyrisico oplevert. Door middel van het uitvoeren van een DPIA kunnen vooraf de privacyrisico's in kaart worden gebracht. Het gevolg is dat de gemeente maatregelen kan treffen om deze risico's te verkleinen.

De gemeente moet dus zelf bepalen of er een DPIA moet worden uitgevoerd. De verplichting om een DPIA uit te voeren staat in de Wet justitiële en strafvorderlijke gegevens (Wjsg), Wpg en AVG. In deze wetten wordt de DPIA een 'gegevensbeschermingseffectbeoordeling' (GEB) genoemd.

Voor de gemeente geldt dat voor iedere nieuwe verwerking of een wijziging in een bestaande verwerking een DPIA zal worden uitgevoerd indien er gebruik wordt gemaakt van nieuwe technologieën en, gelet op de aard, omvang en context, sprake is van een hoog risico. De gemeente hanteert voor het opstellen van een DPIA de handreiking "*Samen naar een kwalitatief goede DPIA – handreiking & sjabloon*" . In deze handreiking staat uitgeschreven welke partijen betrokken moeten worden bij het opstellen van de DPIA, waar welke verantwoordelijkheid ligt en aan welke verplichtingen moet worden voldaan.

Ook zal de gemeente ten aanzien van bestaande processen een DPIA uitvoeren indien uit een risicoinventarisatie blijkt dat er gelet op de aard, omvang en context, sprake is van een hoog risico voor het betreffende proces. Op basis daarvan kunnen dan passende maatregelen worden getroffen.

Functionaris gegevensbescherming (FG)
De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente 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 de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus
De gemeente 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 de gemeente 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 gemeentelijke organisatie 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. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

Vastgesteld door het college van B&W op 11 november 2025.