

Privacybeleid Gemeente Dronten

Inleiding

De gemeente Dronten werkt met persoonsgegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheid of voor bijvoorbeeld burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en het in toenemende mate digitaliseren van de overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Dronten 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)

Begripsbepalingen

De definities in dit privacybeleid hebben dezelfde betekenis als de definities in artikel 4 van de AVG

Visie

De komende jaren zet de gemeente in op het verhogen van de privacy bewustwording en verdere professionalisering van het onderwerp 'privacy' in de organisatie. Een goed privacy beleid is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers 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 de gemeente. Het zorgvuldig omgaan met persoonsgegevens draagt daar mee bij aan een onderdeel van de gemeenschappelijke visie van de gemeente Dronten: de V van vertrouwen.

Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen. Dit algemene privacybeleid werkt de gemeente verder uit op zowel tactisch als operationeel niveau door middel van handreikingen, concrete werkprocedures of werkafspraken voor zowel algemene onderwerpen als voor domeinspecifieke onderwerpen.

Naast dit vastgestelde privacybeleid is er ook een strategisch informatiebeveiligingsbeleid, het P&IB-beleid. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom dan ook niet los worden gezien van het gemeente informatiebeveiligingsbeleid.

Iedereen die werkzaam is binnen de gemeente Dronten 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.

Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers, medewerkers en andere natuurlijke personen (hierna: betrokkenen).

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

- De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;

- De verwerking van persoonsgegevens die zijn uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
- De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Principes voor de verwerking van persoonsgegevens

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

Rechtmatige grondslag

Persoonsgegevens worden door de gemeente 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. Vaak vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet of een publiekrechtelijke taak. Deze grondslagen staan in artikel 6 van de AVG.

Welbepaalde doeleinden

De gemeente 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 de gemeente alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken. De gemeente ziet af van de verwerking als het doel op een andere – minder ingrijpende – wijze kan worden bereikt, door bijvoorbeeld minder persoonsgegevens te verwerken (subsidiariteit).

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 geen nadelige effecten voor betrokkenen zijn, 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 de wet- en regelgeving. Dit wordt ook wel de doelbindingstoets genoemd.

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, dan kiest de gemeente bij voorkeur voor die mogelijkheid. 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 kiest de gemeente bij voorkeur voor die mogelijkheid. De verwerkingen die plaatsvinden binnen de gemeente worden opgenomen in het verwerkingsregister.

Juiste en actuele gegevens

De gemeente zorgt er voor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen. Eén van de belangrijkste bronnen van persoonsgegevens voor de gemeente is de Basisregistratie Personen (BRP).

Gegevens worden op tijd vernietigd

De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en selectielijsten. Gemeenten 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. De meest voorkomende selectielijst is de Selectielijst archiefbescheiden gemeenten en intergemeentelijke organen 2020 van de VNG.

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. Het uitgangspunt is in dat geval dan ook: niet langer bewaren dan **noodzakelijk**. De gemeente bewaart alleen geanonimiseerde gegevens langer, waarbij (in)directe identificatie van een persoon niet meer mogelijk is.

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 ongeau-

toriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het geldende informatie-beveiligingsbeleid

Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk ofwel 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 wordt ook wel Privacy by Design genoemd. Tijdens de ontwikkeling of het ontwerp worden de standaardinstellingen altijd zo privacy-vriendelijk mogelijk gehouden. Dit wordt Privacy by Default genoemd. Dit betekent dat vanaf het begin van een proces eisen worden meegegeven vanuit privacy en dat er controles worden uitgevoerd om te kijken of deze twee principes worden toegepast.

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.

Inbreuk in verband met persoonsgegevens

Een inbreuk in verband met persoonsgegevens wordt ook wel een 'datalek' genoemd. Hierbij worden er per ongeluk of onrechtmatig persoonsgegevens verloren, gewijzigd of wordt er onbedoeld toegang verleend tot deze persoonsgegevens. Afhankelijk van het risico moet een datalek gemeld worden bij de Autoriteit Persoonsgegevens (hierna: AP) en soms ook bij de betrokkene(n). De gemeente houdt een datalekkenregister bij. Nadere regels over het aanpakken van datalekken is geregeld in het interne datalekkenproces.

Externe partijen

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 en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, dit zijn de zogenaamde verwerkersovereenkomsten. De gemeente maakt gebruik van de (landelijke) standaard verwerkersovereenkomst van de VNG (Vereniging Nederlandse Gemeenten).

Ook kan het voorkomen dat de gemeente samenwerkt met een andere partij, die niet aan te merken is als een verwerker, zoals een andere gemeente of overheidsorganisatie. In zulke gevallen kan er sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt, door bijvoorbeeld een gegevens-uitwisselingsovereenkomst. Derde partijen waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

Opslag data en doorgifte

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

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. Nadere informatie over transparantie is opgenomen in de Privacyverklaring van de gemeente Dronten.

Volledig geautomatiseerde besluitvorming

Bij het verwerken van persoonsgegevens zonder (enige) menselijke tussenkomst is er sprake van geautomatiseerde besluitvorming. De gemeente maakt geen gebruik van volledig geautomatiseerde besluitvorming. Dit betekent dat er bij de totstandkoming van een besluit altijd sprake is van menselijke tussenkomst.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar 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 op inzage
- Het recht op rectificatie
- Het recht op verwijdering / vergetelheid
- Het recht op bezwaar
- Het recht op beperking van de verwerking
- Het recht op overdraagbaarheid

Nadere regels over deze rechten zijn opgenomen in de Privacyverklaring van de gemeente Dronten. Om een verzoek op grond van hoofdstuk III van de AVG in behandeling te nemen, moet de gemeente de identiteit van de verzoeker vaststellen. Zo weet de gemeente zeker dat de gegevens aan de juiste persoon wordt verstrekt. Een verzoek kan worden ingediend via het digitale webformulier (DigiD) of fysiek bij de balie / receptie van het gemeentehuis.

Geschillenbeslechting

Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals opgenomen in de privacyverklaring op de website van de gemeente Dronten of door contact op te nemen via fg@dronten.nl. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

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 AP houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (hierna: FG). De FG ziet erop 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 beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Functionaris Gegevensbescherming

De gemeente is verplicht een FG aan te stellen, omdat zij structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De FG is een onafhankelijke interne 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.

Gegevensbeschermingseffectenbeoordeling (GEB/DPIA)

Als een verwerking een mogelijk hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente moet in dat geval een gegevensbeschermingseffectenbeoordeling (hierna: GEB) uitvoeren. Dit wordt in de praktijk ook wel een Data Protection Impact Assessment genoemd. Als uit de GEB blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om deze risico's te verminderen. Als dat niet lukt, moet de gemeente met de AP overleggen voordat zij met de verwerking beginnen. Dit heet 'voorafgaande raadpleging'. In de werkinstructie 'uitvoeren DPIA's' is uitgewerkt welke verwerkingen de gemeente kwalificeert als 'een verwerking met een hoog risico.'

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. De gemeente geeft hier onder andere invulling aan door het geven van trainingen, het beschikbaar stellen van e-learning modules en het geven van presentaties aan nieuwe collega's.

Rollen en verantwoordelijkheden

Het governancemodel van de gemeente biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het College van B&W, het managementteam en medewerkers, de Functionaris Gegevensbescherming en de Privacy Officer.

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	Teammanagers en Directeuren De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	Het college van B&W
C	Consulted/ Adviserend	Privacy Officer CISO (Chief Information Security Officer) Functionaris Gegevensbescherming
I	Informerend/ Geïnformeerd	Gemeenteraad (privacy rechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) Functionaris Gegevensbescherming Belanghebbende(n)/Betrokkene(n)

Toelichting governancemodel

College van B&W

Het college is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de de privacywetgeving binnen de gemeente;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

Teammanagers en directeuren

De teammanagers en directeuren zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen de afdeling, alsmede voor de uitvoering van het privacybeleid.

De teammanagers en directeuren hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de eigen afdeling;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen de eigen afdeling;

- Informeert de FG op welke manier de eigen afdeling compliant is aan de privacywetgeving; verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen de eigen afdeling;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op de eigen afdeling;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de Privacy Officer voor zover benoemd binnen de eigen afdeling;
- Bevordert duurzame privacycultuur;
- Betreft PO en/of FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezicht houdende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:

- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingenregister;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het College van B&W.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor de gemeente rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van geveenseffectbeoordeling (GEB) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Het college van Dronten, 7 januari 2025

R. Hammenga, MA
secretaris

drs. J.P. Gebben
burgemeester