GEMEENTE Gulpen-Wittem

GEMEENTEBLAD

Officiële uitgave van de gemeente Gulpen-Wittem

Nr. 122354

21 maart

2025

Privacy beleid 2025

Burgemeester en wethouders besluiten
1. Het Privacy beleid 2025 vast te stellen.

Definities

Onderwerp	Betekenis
Algemene Verordening Gegevensbescherming (AVG). (Engelse term: 'GDPR').	Algemene Verordening Gegevensbescherming, vastgesteld door het Europees Parlement.
Betrokkene(n)	De geïdentificeerde of identificeerbare natuurlijk persoon op wie de verwerkte en/of de te verwerken persoonsgegevens betrekking hebben.
Bijzondere persoonsgegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden (artikel 9 AVG).
Datalek/inbreuk in verband met persoonsgegevens	Een inbreuk op de beveiliging die per ongeluk of 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 gegevens (artikel 4 onder 12 AVG).
Data Protection Impact Assessment (DPIA)	Vertaald in het Nederlands: gegevensbeschermings-effectbeoordeling. Het is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is een beoordeling over het effect van de (nieuwe of aangepaste) verwerking op de bescherming van de persoonsgegevens en is verplicht als een gegevensverwerking waarschijnlijk een hoog risico oplevert voor de betrokkenen.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken (artikel 10 onder 4 AVG).
Functionaris Gegevensbescherming (FG)	Een onafhankelijke deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de Algemene verordening gegevensbescherming (AVG).
Ontvanger	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn (artikel 4 onder 9 AVG).
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 onder 1 AVG).

Privacyteam	Onder het Privacyteam wordt onder meer verstaan de Privacy Officer (PO), de Chief Informatie en Security Officer (CISO), de Informatie en Security Officer (ISO) en de Functionaris Gegevensbescherming (FG)
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (artikel 4 onder 8 AVG).
Verwerkersovereenkomst	Een overeenkomst met daarin de afspraken hoe een verwerker persoonsgegevens verwerkt.
Verwerking	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, 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, aligneren of combineren, afschermen, wissen of vernietigen van gegevens (artikel 4 onder 2 AVG).
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4 onder 7 AVG).

1. Inleiding

Gemeenten verzamelen en gebruiken persoonsgegevens om hun taken uit te voeren. Hierbij is een zorgvuldige en veilige verwerking van deze persoonsgegevens van belang.

De gemeente Gulpen-Wittem is zich hiervan bewust en zorgt ervoor dat de privacy behouden blijft. Het bestuur en het management spelen een essentiële rol bij het beschermen van de privacy van de inwoners van de gemeente.

1.1 Missie

De gemeente heeft als missie om een 5 sterren kwaliteit te leveren aan de inwoners. Daaruit vloeit voort dat we een solide basis leggen voor een effectief Informatiebeveiliging en privacy beleid en een actieve privacybeschermingscultuur.

1.2 Visie

De gemeente wil dat iedereen erop kan vertrouwen dat zorgvuldig en veilig persoonsgegevens worden verwerkt en dat de privacy van de inwoners wordt gewaarborgd.

De komende jaren zal de gemeente zich richten op het vergroten van het bewustzijn rondom privacy. Een gedegen organisatiestructuur is cruciaal voor het functioneren van de gemeente en vormt onder andere de basis voor de privacybescherming. Een integrale aanpak, eigenaarschap en risico gericht werken is aangewezen. Verantwoord en bewust gedrag van medewerkers, ketenpartners en leveranciers zijn daarbij essentieel voor een rechtmatige, veilige en gedegen verwerking van persoonsgegevens.

1.3 Ambitie/Strategie

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).

Naast dit vastgestelde privacybeleid, is een informatiebeveiligingsbeleid vastgesteld. 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 niet los worden gezien van het vigerende gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer
Iedereen die werkzaam is 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.

1.4 Reikwijdte beleid

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens die door of namens de gemeente worden verricht. Ketenpartners en leveranciers dienen zich te committeren aan dit beleid. Dit beleid zal nader worden uitgewerkt in operationeel beleid, zoals werkinstructies en richtlijnen.

Op verwerkingen die voortvloeien uit de Wet politiegegevens (Wpg), is het vigerende Wpg-beleid van toepassing.

2. Belangenafweging

Bij verwerking van persoonsgegevens kunnen diverse belangen spelen, namelijk het belang van de burger, het publieke belang en de belangen van burgers ten opzichte van elkaar (deze opsomming is niet limitatief). Een belangenafweging kan dan aan de orde zijn. Deze belangenafweging vindt zorgvuldig plaats door middel van een analyse van de verwerking en de bijbehorende risico's en te nemen maatregelen.

3. Privacy uitgangspunten

De AVG omschrijft een aantal uitgangspunten die centraal staan in dit beleid. De gemeente hanteert hierbij de centrale uitgangspunten van Rechtmatigheid, Behoorlijkheid en Transparantie om invulling te geven aan alle uitgangspunten die de AVG stelt. Hieronder worden deze uitgangspunten omschreven.

3.1 Rechtmatigheid

- De geldende wet- en regelgeving voor gegevensverwerking wordt gehandhaafd, waarbij de AVG als basis geldt. Verwerking van persoonsgegevens is enkel toegestaan indien sprake is van een wettelijke grondslag.
- Hergebruik van persoonsgegevens is enkel toegestaan indien het verenigbaar is met het initiële doel (doelbinding). Indien dit niet het geval is dan zal worden gekeken naar een rechtmatige grondslag met behulp van het privacy team.
- Enkel de persoonsgegevens die uitsluitend noodzakelijk zijn voor een specifiek doel van de verwerking worden verwerkt.
- Bij gegevensverwerking wordt rekening gehouden met de beginselen van proportionaliteit en subsidiariteit. De gemeente vraagt slecht die informatie die noodzakelijk is om het beoogde doel te bereiken. Daarbij gebruikt de gemeente altijd de minst ingrijpende methode voor de betrokkene.

3.2 Behoorlijkheid

- De gemeente hanteert het principe van minimale gegevensverwerking om dataminimalisatie te waarborgen.
- De gemeente hanteert het beginsel van éénmalige vastlegging en meervoudig gebruik, met inachtneming van noodzakelijke werkinstructies en autorisaties.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk en worden vertrouwelijk behandeld.
- Alleen functionarissen die dit voor hun taakuitoefening nodig hebben, hebben inzage in persoonsgegevens.
- De gemeente neemt maatregelen om de juistheid en actualiteit van de persoonsgegevens te waarborgen.
- De gemeente geeft betrokkene de mogelijkheid om haar persoonsgegevens te corrigeren.

3.3 Transparantie

- Betrokkenen hebben recht op informatie over de persoonsgegevens die de gemeente verwerkt.
- Belanghebbenden en burgers kunnen op basis van de procedure Rechten van
- Betrokkenen verzoeken indienen voor inzage, correctie of verwijdering van hun gegevens.
- De gemeente is transparant over het delen van persoonsgegevens met derden, tenzij de wet dit verbiedt.
- De gemeente is open en transparant over hoe met persoonsgegevens wordt omgegaan.
- Afwijkingen van dit beleid worden beargumenteerd voorgelegd aan het privacy team. Indien nodig zal worden geëscaleerd naar het College en/of de burgemeester.

4. Rechtsgrondslagen

De AVG (artikel 6) definieert de rechtsgrondslagen voor het rechtmatig verwerken van persoonsgegevens. De rechtsgrondslagen zijn wettelijke taak, algemeen belang, gerechtvaardigd belang, uitvoering van een overeenkomst, toestemming of vitaal belang. De rechtsgrondslag vitaal belang is bij de verwerking van persoonsgegevens binnen de gemeente niet van toepassing. De rechtsgrondslag gerechtvaardigd

belang wordt door de gemeente enkel en alleen gebruikt voor bedrijfsvoeringszaken en de rechtsgrondslag toestemming wordt zeer terughoudend gebruikt.

5. AVG-verplichtingen

De AVG verplicht gemeenten tot een aantal concrete handelingen. In dit hoofdstuk staan deze verplichtingen beschreven. De gemeente dient deze handelingen aantoonbaar deel uit te laten maken van haar processen en activiteiten.

5.1 Privacy by Design & Privacy by Default

De gemeente hanteert de principes van 'Privacy by Design' en 'Privacy by Default' op haar verwerkingen.

Privacy by Design: houdt in dat er bij het ontwerpen (de voorfase) van producten en diensten wordt gezorgd dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of bouw van het systeem wordt onder andere gekeken naar de benodigde organisatorische en technische maatregelen. De PO is in deze ontwikkelfase betrokken. De FG ziet er op toe dat dit ook plaatsvindt.

Privacy by Default: houdt in dat de standaardinstellingen van een programma ingesteld dienen te worden op de meest privacy vriendelijke manier.

5.2 Data protection impact assessment (DPIA)

Een Data Protection Impact Assessment (DPIA), ook wel gegevensbeschermingseffectbeoordeling genoemd, is een instrument dat de gemeente gebruikt om de privacy risico's van een gegevensverwerking in kaart te brengen voordat er begonnen wordt met een verwerking. Het doel van een DPIA is om mogelijke risico's voor de privacy van betrokkenen te identificeren en maatregelen te nemen om deze risico's te verkleinen.

Per gegevensverwerking dient de gemeente te bepalen of de verwerking mogelijk een hoog privacy risico oplevert voor betrokkenen. Bij het vermoeden van een hoog privacy risico voert de gemeente een DPIA uit. Van een vermoeden van een hoog privacy risico is bijvoorbeeld sprake indien de verwerking op grootschalige basis plaatsvindt, de verwerking van bijzondere categorieën van persoonsgegevens aan de orde is of er sprake is van stelselmatige monitoring. De verwerkingen waarvoor het uitvoeren van een DPIA minimaal verplicht is, worden benoemd in artikel 35 derde lid AVG. Deze worden nader gespecificeerd in het besluit dat is genomen door de Autoriteit Persoonsgegevens (AP) (Staatscourant 2019 nr. 64418).

5.3 Register van verwerkingsactiviteiten/Verwerkingsregister

De gemeente is verplicht om een register van verwerkingen bij te houden. Het register is een overzicht waarin de gemeente alle verwerkingen van persoonsgegevens documenteert. In het register staat onder andere de volgende informatie vermeld:

- Naam en contactgegevens
  - De naam en contactgegevens van de verwerkingsverantwoordelijke, de verwerker en, indien van toepassing, de Functionaris voor Gegevensbescherming (FG).
- Verwerkingsdoeleinden
  - Een beschrijving van de doeleinden waarvoor de persoonsgegevens worden verwerkt.
- Categorieën van betrokkenen en persoonsgegevens
  - Een beschrijving van de categorieën van betrokkenen en de categorieën van persoonsgegevens die worden verwerkt .
- Ontvangers van persoonsgegevens
  - De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt.
- Doorgifte van gegevens
  - Informatie over de doorgifte van persoonsgegevens aan derde landen (buiten de EU) of internationale organisaties, indien van toepassing.
- Bewaartermijnen
  - De beoogde termijnen waarvoor de persoonsgegevens zullen worden opgeslagen.
- Beveiligingsmaatregelen
  - Een algemene beschrijving van de technische en organisatorische maatregelen die zijn genomen om de persoonsgegevens te beveiligen.

5.4 Datalekken
Een datalek heeft potentieel een grote impact op betrokkenen en de gemeentelijke organisatie. Volledig uitsluiten van een datalek is onmogelijk, maar de gemeente zet zich in om een cultuur te creëren waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Bij een datalek kan het voorkomen dat het datalek verplicht binnen 72 uur bij de AP. Tevens kan het voorkomen dat betrokkenen spoedig moeten worden geïnformeerd. Daarvoor is een datalek procedure opgesteld.

Om te anticiperen op mogelijke risico's wordt een intern datalekregister bijgehouden, waarin alle geconstateerde beveiligingsincidenten worden geregistreerd. Jaarlijks wordt het datalekregister geëvalueerd om trends bij te houden en structurele verbeteringen intern door te voeren.

5.5 Gegevens delen met derden
Wanneer sprake is van structurele of gevoelige gegevensuitwisseling met derde partijen, worden er afspraken gemaakt over de gegevensuitwisseling. Deze afspraken voldoen tenminste aan de AVG en worden vastgelegd in een onderlinge regeling, samenwerkingsovereenkomst (convenant), een gegevensuitwisselingsovereenkomst of een verwerkersovereenkomst. Voor het vormgeven van de verwerkersovereenkomst maakt de gemeente gebruik van het model van de Informatiebeveiligingsdienst voor Gemeenten (IBD).

Ten aanzien van de doorgifte van persoonsgegevens hanteert de gemeente het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is (bijvoorbeeld door middel van een adequaatheidsbesluit van de AP).

5.6 Rechten van betrokkenen
Onder de AVG hebben betrokkenen, oftewel personen van wie persoonsgegevens worden verwerkt, verschillende rechten. Deze rechten geven hen meer controle over hun privacy en hoe hun gegevens worden gebruikt:

- Recht op informatie
  - Betrokkenen moeten geïnformeerd worden over het feit dat hun persoonsgegevens worden verwerkt, met welk doel, en door wie.

- Recht op inzage
  - Betrokkenen hebben het recht om te weten welke persoonsgegevens van hen worden verwerkt en om een kopie van deze gegevens te ontvangen.

- Recht op rectificatie
  - Betrokkenen kunnen verzoeken om onjuiste of onvolledige persoonsgegevens te laten corrigeren.

- Recht op gegevenswissing (recht om vergeten te worden)
  - In bepaalde gevallen kunnen betrokkenen verzoeken om hun persoonsgegevens te laten wissen.

- Recht op beperking van de verwerking
  - Betrokkenen kunnen onder bepaalde omstandigheden de verwerking van hun persoonsgegevens laten beperken.

- Recht op dataportabiliteit
  - Betrokkenen hebben het recht om hun persoonsgegevens in een gestructureerd, gangbaar en machineleesbaar formaat te ontvangen en deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke.

- Recht van bezwaar
  - Betrokkenen kunnen bezwaar maken tegen de verwerking van hun persoonsgegevens, bijvoorbeeld voor direct marketing.

- Recht met betrekking tot geautomatiseerde besluitvorming en profilering
  - Betrokkenen hebben het recht om niet te worden onderworpen aan een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking, inclusief profilering, tenzij bepaalde voorwaarden zijn vervuld.

De gemeente heeft haar website zo ingericht dat betrokkenen hun rechten kunnen inroepen.

5.7 Functionaris Gegevensbescherming (FG)
De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Daardoor is de gemeente wettelijke verplicht een FG aan te stellen. De gemeente heeft gekozen voor het aanwerven van een gezamenlijke FG voor gemeente Valkenburg, Vaals en Gulpen-Wittem.

De FG is onderdeel van het Privacyteam. De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG. De FG voert jaarlijks een interne audit uit en maakt daarbij een FG toezichtsplan. De FG rapporteert jaarlijks over de naleving van de privacy wet- en regelgeving aan het college van B&W. De FG vervult tenminste de taken zoals omschreven in artikel 39 AVG.

6. Taken en verantwoordelijkheden

Het college van B&W is eindverantwoordelijk voor het naleven van de uitgangspunten uit de privacy wet- en regelgeving en de kaders voor het verantwoord omgaan met persoonsgegevens. De gemeente heeft de verantwoordingsplicht om te kunnen aantonen dat deze uitgangspunten en kaders worden nageleefd. Elke ambtenaar binnen onze organisatie is in diverse mate verantwoordelijk voor de juiste naleving en implementatie van dit privacybeleid. Hiervoor wordt het three-lines-of-defence model gehanteerd. Onderstaand een korte toelichting van dit model. De concrete interne taakverdeling wordt geborgd in instructies/werkprocessen/richtlijnen.

1e Lijn	2e Lijn	3e Lijn
Directie, managementteam en griffier	Privacyteam (exclusief FG) t.b.v. Privacy, informatiebeveiliging & Compliance	Functionaris Gegevensbescherming Toezichthouder/Adviseur/Signaleur
Primair verantwoordelijk voor de naleving van privacy uitgangspunten.	Ondersteunend aan de eerste lijn en verantwoordelijk voor methodiek en inrichting processen.	Toezichthoudend, toetsend, signalerend, adviserend, totaaloverzicht.

De eerste lijn, met name de afdelingshoofden, draagt de eerstelijnsverantwoordelijkheid. Deze verantwoordelijkheid dragen afdelingshoofden voor de verwerkingsprocessen die binnen hun teams plaatsvinden. Voor privacyvraagstukken kunnen de teams een beroep doen op het privacyteam. Een ambitie voor de toekomst is om per team een privacy ambassadeur aan te wijzen en het privacyteam in te schakelen bij complexe privacyvraagstukken.

De tweede lijn, het privacyteam, draagt de tweedelijnsverantwoordelijkheid. Deze verantwoordelijkheid heeft betrekking op het monitoren en adviseren ten aanzien van de naleving van de privacy wet- en regelgeving binnen de gemeente. Daarnaast ondersteunt het privacyteam de gemeentelijke organisatie in de beleidsuitvoering van privacy en informatiebeveiliging. Het privacyteam zorgt voor eenduidig inzicht in de naleving van de privacy wet- en regelgeving binnen alle organisatieonderdelen en bestuursorganen van de gemeente.

Het Privacyteam bestaat tenminste uit de CISO, Privacy Officer en de FG.
De CISO is verantwoordelijk voor het advies en toezicht op de toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van informatie. Daarnaast is de CISO betrokken bij beveiligingsincidenten.
De Privacy Officer is het eerste aanspreekpunt voor de gemeente rondom privacy gerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid. De Privacy Officer houdt zich onder meer bezig met verwerkersovereenkomsten, datalekken, het bijhouden van het verwerkingsregister en het uitvoeren van DPIA's.

De derde lijn, de FG, controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert. Daarover velt de FG een objectief en onafhankelijk oordeel met mogelijkheden tot verbetering. De FG speelt een rol in alle lijnen met de voornaamste focus op de derde lijn.

7. Bewustwording

Een hoge mate van bewustwording bij alle medewerkers is van essentieel belang om dit privacybeleid goed uit te voeren. De gemeente draagt ervoor zorg dat elke medewerker een adequaat niveau van bewustwording heeft/krijgt als het gaat om privacy en informatiebeveiliging.

In het kader van bewustwording is het aangewezen dat de leidinggevende zorg draagt voor informerende en voorlichtende activiteiten op het gebied van privacy binnen het team. Van belang is, dat de meldplicht datalekken en het gebruik van de online tool bewustwording op het gebied van informatie-

beveiliging en privacy een terugkerend onderwerp is. Daarnaast is het van belang om te bewerkstelligen dat nieuwe medewerkers worden verplicht om binnen drie (3) maanden na indiensttreding een digitale bewustwordingstraining te volgen.

8. Geldigheid en evaluatie volgens de PDCA-cyclus

Dit beleid is vastgesteld op 11 maart 2025 door het college van Burgemeester en Wethouders als eindverantwoordelijke voor de gegevensverwerking. Dit beleid wordt jaarlijks door het Privacyteam volgens de Plan-Do-Check-Act methodiek geëvalueerd en zo nodig geactualiseerd.