Gemeente Sittard-Geleen Born

GEMEENTEBLAD

Officiële uitgave van de gemeente Sittard-Geleen

Nr. 159991

3 april 2026

Privacy beleid gemeente Sittard-Geleen 2025-2028

Het college besluit:
1. Het Privacybeleid Gemeente Sittard-Geleen 2025-2028 vast te stellen.

1. Inleiding

Digitalisering en de toepassing van nieuwe technologieën leiden tot veranderingen in de samenleving. Hierdoor verschuiven ook de verwachtingen die inwoners hebben van onze dienstverlening. Denk aan het beheer van de openbare ruimte, het toezicht en de handhaving. Het gebruik van gegevens speelt een belangrijke rol bij het waarmaken van die verwachtingen. Wij hechten veel waarde aan het met respect behandelen van onze inwoners, het zorgvuldig verwerken van informatie en het beschermen van hun privacy.

De AVG (Algemene Verordening Gegevensbescherming) en de WPG (Wet politiegegevens) zijn daarbij de centrale kaders. Deze bieden ons een belangrijke norm voor de wijze waarop wij omgaan met persoonsgegevens. Dit privacybeleid beschrijft hoe wij dat doen. Persoonsgegevens dienen daarnaast goed te worden beschermd met de juiste maatregelen. In de Baseline Informatiebeveiliging Overheid (BIO) zijn voor ons de concrete normen vermeld. Deze zijn nader uitgewerkt in ons strategisch en tactisch informatiebeveiligingsbeleid.

Het privacybeleid is geschreven voor onze inwoners, onze medewerkers en voor onze organisatie. Het privacybeleid heeft betrekking op de (onderdelen van de) gemeente Sittard-Geleen als bestuursorgaan, openbaar lichaam en als werkgever. Het beschrijft de context van het beleid, de doelen, de uitgangspunten en de keuzes voor ons handelen binnen de kaders van de AVG, de WPG, en verwante sectorregelgeving. Daar waar in dit privacybeleid wordt gesproken over “de gemeente”, “ons” of “wij” refereert dit naar de gemeente Sittard-Geleen en over ‘inwoners’ naar inwoners en in voorkomende gevallen naar medewerkers van de gemeente Sittard-Geleen.

1.1 Kernwaarden en ambitie

Wij zien het beschermen van persoonsgegevens als een prioriteit. Daarbij hanteren we onderstaande kernwaarden die in dit privacybeleid verder zijn uitgewerkt.

De vijf kernwaarden

I. *De mens staat centraal:* wij organiseren ons op een klantgerichte manier, waarbij de behoefte van de mens centraal staat. Door het steeds meer digitaal werken verwachten wij meer in die behoefte te voorzien. Zo werken wij in de basis digitaal, tenzij de context het niet toelaat.[1]
II. *Een heldere belangenafweging:* de uitvoering van onze wettelijke taken, optimale dienstverlening en privacybescherming betekenen het constant zoeken naar de juiste balans. Er wordt zorgvuldig gekeken naar het belang van het individu en het algemeen belang. Hierbij wordt gekeken naar het wettelijke kader, een correcte risicoafweging en ons moreel kompas. We geloven dat een goede privacybescherming, dienstverlening en werkbaarheid samen kunnen gaan.
III. *Digitale veiligheid:* bij digitaal werken is digitale veiligheid en privacy van essentieel belang. Inwoners en medewerkers moeten erop kunnen vertrouwen dat persoonsgegevens veilig zijn bij ons. Het privacybeleid steunt dan ook op de 3 algemene privacy uitgangspunten, lees hoofdstuk 3, en de 10 principes van informatiebeveiliging.[2]
IV. *Eenmalige vastlegging, meervoudig gebruik:* we willen niet opnieuw gegevens opvragen die al bekend zijn. Uiteraard kan dit alleen met een wettelijke grondslag. Bij onze rol als overheid horen de volgende wettelijke grondslagen: wettelijke verplichting, taak van algemeen belang en/ of in het kader van een taak van openbaar gezag. Wij verwerken bij voorkeur niet op basis van toestemming als verwerkingsgrondslag.
V. *Openheid:* Wij hechten er veel waarde aan dat onze inwoners en medewerkers vertrouwen hebben in ons als gemeente. Daarbij speelt transparantie een belangrijke rol. Dit betekent dat wij inwoners en medewerkers op passende manieren informeren over hun privacy rechten. Hiervoor gebruiken wij verschillende (digitale) kanalen en de algemene privacyverklaring.[3]

1) Visie document: Organisatie en manier van werken (mei 2020) inclusief bijlagen, zie p. 9
2) Strategisch Informatiebeveiligingsbeleid, zie p. 15
3) Privacyverklaring (website)

Ambitie
Wij hebben de ambitie om organisatiebreed op een volwassenheidsniveau van 4 te opereren. Wij willen dit bereiken en in stand houden door elk kwartaal onze processen te toetsen en te verbeteren waar nodig.

1.2 Reikwijdte privacybeleid
Het privacybeleid is van toepassing op al het gebruik van persoonsgegevens binnen onze gemeente. Van het genereren of verzamelen van persoonsgegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging van persoonsgegevens. Dit privacybeleid is bindend voor het openbare lichaam, de gehele bedrijfsorganisatie en de bestuursorganen van de gemeente Sittard-Geleen.

Dit beleid is op onderdelen nader uitgewerkt in operationeel beleid, werkinstructies en richtlijnen. Wanneer sprake is van gegevensuitwisselingen met externe partijen gelden dezelfde uitgangspunten en ambitie. Bij verwerkers of samenwerking gelden dezelfde uitgangspunten. Diezelfde uitgangspunten vormen het kader bij de selectie van leveranciers c.q. verwerkers. Hiervoor maken wij contractuele afspraken die we ook kunnen toetsen bij de uitvoering van de werkzaamheden. Het beleid is ook van toepassing in geval van uitwisseling van informatie met andere gemeenten en organisaties bij de uitbesteding van publieke taken aan externe partijen.

Hoewel de AVG de belangrijkste wet is op het gebied van de verwerking van persoonsgegevens zijn er ook andere wetten waar in dit privacybeleid naar kan worden verwezen of die van toepassing op ons zijn. Dit zijn onder andere, maar niet beperkt tot:

- Wet politiegegevens.
- Telecommunicatiewet.
- AI-verordening.
- Archiefwet.
- Basisregistratie Personen (BRP).
- Wet maatschappelijke ondersteuning.
- Wet gemeentelijke schuldhulpverlening.
- Participatiewet.

1.3 Definities
In het privacybeleid worden de volgende definities gehanteerd:

- **Algemene Verordening Gegevensbescherming (AVG)**
  Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).
- **Betrokkene(n)**
  De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt. Dit kan gaan om een inwoner, ondernemer, ambtenaar of contactpersoon van een (keten)partner.
- **Datalek**
  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.
- **Data Protection Impact Assessment (DPIA)**
  In het Nederlands vertaald naar gegevensbeschermingseffectbeoordeling, maar de gangbare term is DPIA. Dit is een instrument om vooraf de privacyrisico'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 privacyrisico oplevert voor de betrokkenen. De beoordeling bevat tenminste een inschatting van de risico's van de verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen.
- **DPIA-Toets**
  Een DPIA-toets is een methode om te beoordelen of een DPIA wettelijk verplicht is om uit te voeren.
- **Functionaris Gegevensbescherming (FG)**
  Een onafhankelijke en deskundige toezichthouder met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de naleving van alle privacy wet- en regelgeving waaronder

de AVG en de WPG. Wij hebben een externe specialist benoemd als FG om de onafhankelijkheid van de FG nog beter te kunnen waarborgen.

- **Privacy Team**
  Binnen onze gemeente zijn vakspecialisten benoemd die ons adviseren over het naleven van privacy wet- en regelgeving en helpen bij de inrichting van de organisatieprocessen. Tot het Privacy Team behoren onder meer de Privacy Officer(s) en de Adviseur Security en Privacy.
- **Persoonsgegevens**
  (Digitale) informatie die direct of indirect betrekking heeft op een levend persoon.
  Denk hierbij aan naam, adres, geboortedatum. Naast deze “gewone” persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Deze gegevens gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeur of gezondheid.
- **Verwerker**
  De organisatie, of persoon, die in opdracht en ten behoeve van de verwerkingsverantwoordelijke bepaalde onderdelen van of de gehele verwerking voor zijn rekening neemt.
- **Verwerkersovereenkomst**
  Een overeenkomst waarin de afspraken staan hoe een verwerker met de persoonsgegevens moet omgaan.
- **Verwerking**
  Alles wat je met persoonsgegevens kunt doen; “het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van gegevens.”
- **Verwerkingsverantwoordelijke**
  De organisatie, of persoon, die bepaalt waarom de verwerking van persoonsgegevens plaatsvindt en vaststelt met welke middelen dat gebeurt.

2. Belangenafweging

Bij verwerking van persoonsgegevens zijn vaak diverse belangen gemoeid. Dat vraagt in sommige situaties om een zorgvuldige afweging. Naast het belang van de individuele inwoner is er het publieke (algemeen) belang en zijn er belangen van inwoners ten opzichte van elkaar.

- **Belang van de inwoner**: een inwoner wil dat persoonsgegevens veilig en betrouwbaar worden verwerkt. Daarnaast moeten wij transparant zijn wat wij met die informatie doen. De wensen kunnen wel van verschillend karakter zijn. Aan de ene kant heeft de inwoner er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht een inwoner efficiënte dienstverlening.
- **Publiek belang**: wij voeren op diverse gebieden wettelijke- en bestuurlijke taken uit. Denk hierbij aan onder andere in het sociaal domein, openbare orde en veiligheid of burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat er persoonsgegevens worden verwerkt.
- **Belangen van inwoners ten opzichte van elkaar**: de bescherming van de rechten van de ene inwoner kan ingrijpende gevolgen hebben voor de belangen en de rechten van een ander.

Soms botsen de verschillende wettelijke taken die wij uitvoeren. In die gevallen worden de privacy uitgangspunten als beschreven in hoofdstuk 3 meegenomen in de belangenafweging die wij soms noodgedwongen en onderbouwd moeten maken. Op basis van de belangenafweging wordt besloten of en op welke wijze persoonsgegevens worden gebruikt. De risico’s die hierbij aanwezig kunnen zijn worden zo beperkt mogelijk gehouden door het nemen van passende beheersmaatregelen. Dit is nader uitgewerkt in paragraaf 4.2.

3. Privacy uitgangspunten

De AVG en WPG omschrijven een aantal uitgangspunten die centraal staan in dit privacybeleid. Wij hanteren hierbij de centrale uitgangspunten van *Rechtmatigheid, Behoorlijkheid en Transparantie* om invulling te geven aan alle uitgangspunten die de AVG en WPG stellen. Hieronder worden deze uitgangspunten omschreven en de wijze waarop wij deze concreet invulling geven binnen onze organisatie.

3.1 Rechtmatigheid

- Wij hanteren de geldende wet- en regelgeving voor gegevensverwerking, waaronder de AVG en andere relevante wetgeving zoals de WPG. Voor de verwerking van persoonsgegevens moet altijd een verwerkingsgrondslag bestaan.

- Wij leggen alleen persoonsgegevens vast als dit noodzakelijk is voor het specifieke doel van de verwerking. Het kan zijn dat de wet het ons verplicht of om de belangen van betrokkenen te beschermen. Dit wordt voor de verwerking concreet gemaakt en vastgelegd in het verwerkingsregister.[4] Daarbij gebruiken wij altijd de minst ingrijpende methode voor de betrokkenen door rekening te houden met de beginselen van 'proportionaliteit' en 'subsidiariteit'. Verschillende gemeentelijke taken verplichten het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd.
- Het kan zijn dat wij persoonsgegevens vaker moeten gebruiken. Dit kan alleen als dat doel verenigbaar is met de oorspronkelijke verzameldoeleinden. Dit wordt getoetst door het Privacy Team.
- In het verwerkingsregister wordt per verwerking bijgehouden wat de verwerkingsgrondslag is en het doel van de verwerking.

3.2 Behoorlijkheid

- Wij hanteren het principe van 'minimale gegevensverwerking'. Dit wil zeggen dat er geen overbodige gegevens worden gevraagd die niet nodig zijn voor het vastgestelde doel. Hiermee geven wij invulling aan het principe van 'dataminimalisatie'. Zo richten wij onze systemen op een wijze in zodat niet te veel informatie wordt gevraagd. Denk aan online formulieren die geen overbodige invulvakjes hanteren. Verder zijn er werkinstructies en periodieke data "opschoonacties" om het dataminimalisatie principe te waarborgen.
- Wij hanteren het beginsel van 'éénmalige vastlegging, meervoudig gebruik': gegevens die bekend zijn worden niet nodeloos opnieuw gevraagd. Dit betekent ook zo veel mogelijk gebruik maken van zogenoemde brongegevens, zoals die zijn opgenomen in het stelsel van basisregistraties. Dit is alleen mogelijk als dit rechtmatig kan plaatsvinden. Op afdelingsniveau zijn werkinstructies vastgelegd en autorisaties ingericht om heldere kaders te schetsen voor onze medewerkers.[5]
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. Vaak is dit op basis van wettelijke bewaartermijnen. Wanneer de wet hier niet in voorziet staan de bewaartermijnen beschreven in ons verwerkingsregister. Wij bewaren persoonsgegevens in ieder geval in overeenstemming met de "Selectielijst gemeenten en intergemeentelijke organen 2020"[6] en de "Selectielijst e-mailbewaring gemeentelijke en intergemeentelijke organen 2024".[7] De interne organisatie heeft toegang tot het verwerkingsregister om de bewaartermijnen te raadplegen. Verder zijn er werkinstructies voor het gebruik van dit verwerkingsregister.
- Alleen functionarissen (ambtenaren, externen, leveranciers, convenantpartners) waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. Functionarissen (ambtenaren, externen, leveranciers, convenantpartners) hebben alleen toegang tot persoonsgegevens wanneer dit noodzakelijk is voor de directe taakuitoefening. Deze gegevens worden strikt vertrouwelijk behandeld en de toegang is geregeld volgens ons autorisatiebeleid. Medewerkers hebben alleen toegang tot gegevens waarvoor zij een legitiem doel hebben. Bovendien is binnen de organisatie de Gedragscode Ambtelijke Integriteit van kracht, waaraan iedereen zich dient te houden om te garanderen dat persoonsgegevens altijd met zorgvuldigheid en integriteit worden behandeld.[8]
- Er wordt gewerkt met geheimhoudingsverklaringen voor externen en leveranciers. Met externe (keten)partners worden overeenkomsten (convenanten) afgesloten.
- Persoonsgegevens worden goed beveiligd opgeslagen zodat ze adequaat zijn beschermd tegen misbruik, verlies, onbevoegde toegang en bewerking. Door gebruik te maken van 'privacy by design' of 'privacy by default' worden al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht aan privacy verhogende maatregelen geschonken.
- Persoonsgegevens zullen nooit voor commercieel gewin van externen worden gebruikt.
- Het is voor zowel ons als de inwoners van belang dat persoonsgegevens actueel en correct zijn. Er worden diverse projecten en processen periodiek uitgevoerd om de basisregistratie personen actueel en juist te houden. Dit is tevens een wettelijke verantwoordelijkheid.
- Wij hanteren het PeGREC (Privacy-en gebruikersreglement voor elektronische communicatiemiddelen), waarin richtlijnen zijn vastgelegd voor het gebruik en de controle van bedrijfsmiddelen binnen de gemeente. Dit draagt bij aan het waarborgen van de informatiebeveiliging en de privacy van onze inwoners en werknemers. Het PeGREC is van toepassing op alle medewerkers die gebruik

4) Verwerkingsregister (iNavigator)
5) Tactisch informatiebeveiligingsbeleid onder 2.5, zie p. 11-12.
6) Selectielijst gemeenten en intergemeentelijke organen 2020, https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf
7) Selectielijst e-mailbewaring gemeentelijke en intergemeentelijke organen 2024, https://vng.nl/sites/default/files/2023-07/selectielijst-e-mailbewaring-gemeentelijke-en-intergemeentelijke-organen-2024-van-de-adviescommissie-archieven.pdf
8) Tactisch informatiebeveiligingsbeleid onder 2.5, zie p. 11-12.

maken van bedrijfsmiddelen, zoals laptops, telefoons, bodycams en kantoorsoftware, en waarborgt een verantwoord en veilig gebruik van deze middelen.

3.3 Transparantie

- Wij zijn open en transparant over hoe wij met persoonsgegevens omgaan. Iedereen heeft het recht om te vernemen welke persoonsgegevens wij over hem/haar hebben verzameld en waarvoor die worden gebruikt. Dit gebeurt onder meer door onze privacyverklaring op de website.[9] Verder is per afdeling bepaald hoe betrokkenen op een passende wijze worden geïnformeerd. Dit is waar nodig ook vastgelegd in werkinstructies.
- Inwoners hebben de mogelijkheid om te vragen waarom en welke persoonsgegevens wij van hen verwerken. In de basis verstrekken wij de gevraagde informatie tenzij er sprake is van een weigeringsgrond op grond van de wet. Verder kunnen inwoners om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken. Dit verzoek wordt gehonoreerd, tenzij ook hier weer de wet anders heeft bepaald (bijvoorbeeld opsporingsbelang).

3.4 Rechten van betrokkenen

Onder de AVG en WPG hebben betrokkenen verschillende rechten met betrekking tot hun persoonsgegevens. Wij hechten veel waarde aan het naleven van deze rechten. Wij hebben procedures ingericht om verzoeken van betrokkenen correct en tijdig af te handelen. Betrokkenen kunnen via een online formulier op onze website een verzoek indienen. Wij zullen altijd binnen een maand de verzoeker informeren. Wij houden hierbij zo veel mogelijk rekening met de adviezen van de Autoriteit Persoonsgegevens, Europese privacy toezichthouders en de ontwikkelingen in de rechtspraak.

- **Recht op inzage**
  Betrokkenen hebben het recht om te weten welke persoonsgegevens wij van hen verwerken, voor welke doeleinden, en met wie deze gegevens worden gedeeld. Dit kan door een inzageverzoek in te dienen. Betrokkenen kunnen op basis hiervan inzicht krijgen in de categorieën van gegevens die worden verwerkt en de bijbehorende grondslag.
- **Recht op rectificatie**
  Als de persoonsgegevens die wij van een betrokkene verwerken onjuist of onvolledig zijn, heeft de betrokkene het recht om correctie van deze gegevens te verzoeken. Wij zijn verplicht om onjuiste gegevens zo snel mogelijk te corrigeren.
- **Recht op vergetelheid**
  Betrokkenen hebben onder bepaalde omstandigheden het recht om te verzoeken dat hun persoonsgegevens worden verwijderd. Dit recht is van toepassing wanneer de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld, of wanneer de betrokkene zijn toestemming voor de verwerking intrekt en er geen andere grondslag voor verwerking is.
- **Recht op beperking van de verwerking**
  Betrokkenen kunnen verzoeken om de verwerking van hun persoonsgegevens te beperken, bijvoorbeeld wanneer de juistheid van de gegevens wordt betwist, of wanneer de verwerking onrechtmatig is maar de betrokkene de gegevens wil behouden voor een juridische procedure.
- **Recht op overdraagbaarheid van gegevens (dataportabiliteit)**
  Betrokkenen hebben het recht om hun persoonsgegevens in een gestructureerd, gangbaar en machineleesbaar formaat te ontvangen, en deze gegevens door te geven aan een andere verwerkingsverantwoordelijke, indien de verwerking is gebaseerd op toestemming of een overeenkomst en de verwerking op geautomatiseerde wijze plaatsvindt.
- **Recht van bezwaar**
  Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens, bijvoorbeeld wanneer de verwerking plaatsvindt op basis van het gerechtvaardigd belang van de gemeente. Bij bezwaar tegen verwerking voor direct marketing wordt de verwerking direct stopgezet.
- **Recht met betrekking tot geautomatiseerde besluitvorming en profilering**
  Betrokkenen hebben het recht om niet te worden onderworpen aan een beslissing die uitsluitend is gebaseerd op geautomatiseerde verwerking, inclusief profilering, die rechtsgevolgen voor hen heeft of hen anderszins significant beïnvloedt.
- **Recht op informatie**
  Wij hebben de plicht om betrokkenen duidelijk te informeren over de verwerking van hun persoonsgegevens. Dit omvat onder andere de doeleinden van de verwerking, de grondslagen waarop de verwerking is gebaseerd, en de rechten van de betrokkenen. Deze informatie wordt verstrekt via onze privacyverklaring en kan op verzoek worden aangevuld.

9) Privacyverklaring (website), footer ‘privacy’

- **Recht op klacht bij de toezichthouder**
  Betrokkenen hebben het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP) of een andere relevante toezichthouder als zij van mening zijn dat hun rechten op het gebied van gegevensbescherming zijn geschonden.

Om recht te doen aan verzoeken van betrokkenen hebben wij een Procedure rechten van betrokkenen vastgesteld.[10] Hierin is beschreven op welke wijze verzoeken van betrokkenen door ons worden afgehandeld. Hier wordt ook omschreven wie daarbij welke taken en verantwoordelijkheden heeft. In nadere interne beleidsstukken is uitgewerkt hoe betrokkenen tijdig geïnformeerd worden over deze procedure.

4. Risicobeheersingsraamwerk

Aan de AVG moeten wij aantoonbaar voldoen. Dit doen wij door de inrichting van een risicobeheersingsraamwerk waarbij we voortdurend monitoren of we onszelf kunnen verbeteren in het beheersen van onze processen en de daaraan gekoppelde privacy risico's. Het risicobeheersingsraamwerk hebben wij vormgegeven aan de hand van de Privacy Baseline en het Privacy Volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP). De Privacy Baseline en het Privacy Volwassenheidsmodel geven themagewijs invulling aan de open normen van de AVG en helpen ons bij het treffen van de noodzakelijke beheersmaatregelen en het in kaart brengen van privacy risico's. Hierbij sluiten wij zoveel mogelijk aan bij modellen die specifiek zijn opgesteld voor gemeenten zoals het borgingsproduct van de Vereniging van Nederlandse Gemeenten.

Op basis van de Privacy Baseline en het Privacy Volwassenheidsmodel hebben wij kerncontrolepunten en bijbehorende werkprogramma's vastgesteld. Op deze wijze borgen wij in onze dagelijkse processen de implementatie van onze kernwaarden, onze ambitie, de manier waarop wij alle betrokken belangen afwegen en hoe we de privacy uitgangspunten toepassen.

De AVG en de WPG leggen diverse verplichtingen op aan gemeenten. Hieronder worden de belangrijkste verplichtingen omschreven, inclusief de feitelijke uitwerking daarvan binnen onze organisatie. Dit geeft ook weer hoe wij operationeel invulling geven aan de privacy-uitgangspunten zoals beschreven in hoofdstuk 3.

4.1 Het register van verwerkingsactiviteiten

Binnen onze gemeente werken wij met zeer veel processen en dus ook diverse verwerkingen van persoonsgegevens. In de applicatie 'i-Navigator' wordt door ons precies bijgehouden waar welke verwerkingen plaats vinden. In i-Navigator staat de volgende informatie vermeld:

- De naam en contactgegevens van de vertegenwoordiger namens de gemeente, de FG en eventuele andere organisaties waarmee wij gezamenlijk verwerkingsverantwoordelijke zijn.
- De doelen en grondslagen van de verwerkingen.
- Een beschrijving van de categorieën van betrokkenen en de categorieën persoonsgegevens.
- Een beschrijving van de ontvangers van de persoonsgegevens.
- Indien van toepassing, een beschrijving van het delen van persoonsgegevens aan derde landen.
- De bewaartermijnen.
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Het Privacy Team beheert de registratie van de verwerkingen. Proceseigenaren binnen de domeinen zijn verantwoordelijk voor het melden van nieuwe of gewijzigde verwerkingen. Zij worden hierbij geadviseerd door het Privacy Team. De FG controleert periodiek of het inzicht in de verwerkingen volledig en up-to-date is. Intern zijn de rollen en verantwoordelijkheden ten aanzien van het beheer van de registraties schriftelijk vastgelegd.

4.2 Data Protection Impact Assessment (DPIA)

Onze organisatie staat niet stil en is altijd in ontwikkeling. Zo worden processen en systemen doorlopend aangepast. Om privacy risico's voor verwerkingen in kaart te kunnen brengen voeren wij steeds een DPIA-Toets uit op nieuwe verwerkingen of wijzigingen van bestaande verwerkingen. De uitkomst van de DPIA-Toets bepaalt of wij verplicht zijn een DPIA op de verwerking uit te voeren. Een DPIA geeft inzicht in mogelijke privacy risico's en welke maatregelen we kunnen treffen om die risico's te beheersen.

Wij hanteren hiervoor vaste modellen en interne werkinstructies. De uitvoering van de DPIA-Toets en de DPIA is de verantwoordelijkheid van de betrokken teammanager of proceseigenaar. Het Privacy Team ondersteunt en adviseert bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA.

10)Procedure – rechten van betrokkenen (Privacy - Rechten van inwoners - Gemeente Sittard-Geleen (sittard-geleen.nl))

Het Privacy Team houdt een overzicht bij van uitgevoerde DPIA´s en DPIA-Toetsen en monitort de voortgang bij het treffen van maatregelen.

4.3 Privacy by Design & Privacy by Default
Wij hanteren de principes van 'Privacy by Design' en 'Privacy by Default' op haar verwerkingen. Zoals beschreven in paragraaf 4.2 geldt voor onze organisatie dat voor een nieuwe verwerking of een wijziging in een bestaande verwerking een DPIA-Toets uitgevoerd dient te worden. Door deze toets wordt het helder of een DPIA noodzakelijk is. Bij het uitvoeren van een DPIA worden de voor Privacy by Design en Privacy by Default noodzakelijke aspecten (bijvoorbeeld dataminimalisatie en bewaartermijnen) meegenomen in de voorgenomen verwerking. Dit wordt gewaarborgd door altijd het Privacy Team te betrekken bij de voorfase van een project of de inrichting van een verwerking.

Privacy by Design: houdt in dat er bij het ontwerpen van producten en diensten er voor wordt gezorgd dat persoonsgegevens goed worden beschermd. Bij de inrichting van het proces en/of bouw van het systeem wordt bijvoorbeeld gekeken naar de benodigde technische en organisatorische maatregelen.

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

4.4 Meldplicht inbreuken in verband met persoonsgegevens
In de AVG en de WPG is een meldplicht opgenomen voor 'inbreuken in verband met persoonsgegevens' waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van persoonsgegevens is of kan worden aangetast. In spreektaal noemen we dit 'datalekken'. Een datalek kan een grote impact op inwoners en onze bedrijfsvoering hebben. Wij proberen dit dan ook te allen tijde te voorkomen en richten ons ook op het creëren en in stand houden van een open en veilige organisatiecultuur waarbij (mogelijke) datalekken zo snel mogelijk worden gemeld via onze procedure datalekken.[11] In de procedure datalekken staat beschreven op welke wijze datalekken worden afgehandeld en wie daarbij welke taken, bevoegdheden en verantwoordelijkheden heeft.

Daarnaast ontvangen onze medewerkers meerdere malen per jaar informatie over dit thema om het bewustzijn op peil te houden en zij worden hierin actief gestimuleerd door de politiek bestuurders.[12] Tot slot staan op het Intranet van de gemeente Sittard-Geleen diverse aanvullende bronnen ten aanzien van het melden van datalekken.

Intern houden wij een datalekregister bij waarin alle geconstateerde beveiligings-incidenten worden geregistreerd. Hierin wordt vastgelegd of het beveiligingsincident heeft geleid tot een datalek en indien dat het geval is, of het datalek al dan niet is gemeld bij de Autoriteit Persoonsgegevens en/of de betrokkenen. Jaarlijks wordt de procedure datalekken geëvalueerd om te bepalen of structurele verbeteringen noodzakelijk zijn.

4.5 Functionaris Gegevensbescherming (FG) en Bevoegd Functionaris
Wij zijn op grond van de AVG en de WPG verplicht een Functionaris Gegevensbescherming (FG) aan te stellen.

- **De FG** is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en heeft een onafhankelijke toezichthoudende rol binnen de organisatie. Wij hebben hiervoor een externe vakspecialist ingehuurd, die wordt ondersteund door het Privacy Team. De FG ziet toe op naleving van zowel de AVG als de WPG.
- **De bevoegd functionaris** is verantwoordelijk voor het beheer van politiegegevens onder de WPG. Deze functionaris beslist wie toegang heeft tot de gegevens en zorgt ervoor dat de verwerking van politiegegevens voldoet aan de eisen van de WPG. De bevoegd functionaris speelt een belangrijke rol bij de naleving van de WPG binnen de gemeente.

De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG en WPG. De FG maakt jaarlijks een FG toezichtplan, voert dit uit en rapporteert jaarlijks over de naleving van privacy wet- en regelgeving aan het college via de verantwoordelijke wethouder. De FG heeft onder meer de volgende wettelijke taken:
- Toezicht op de naleving van privacy wet- en regelgeving en het privacybeleid van de gemeente.
- Contactpersoon voor de Autoriteit Persoonsgegevens.
- Periodieke verslaglegging aan het college over de uitvoering van zijn taken.

11)Procedure datalekken (intranet gemeente), zoekterm "melden datalek"
12)Strategisch Informatiebeveiligingsbeleid, zie p. 9

- Het zorg dragen voor een juiste afwikkeling van vragen of klachten.
- Gevraagd en ongevraagd informeren en adviseren over privacy wet- en regelgeving.
- Adviseren over DPIA's en toezien op de uitvoering ervan.

De reikwijdte van het FG-toezicht omvat alle verwerkingen van persoonsgegevens die onder de werking van de AVG en de WPG vallen (aangevuld door sectorspecifieke regelgeving), en waarvoor de gemeente als openbaar lichaam de verwerkingsverantwoordelijke is. Daarnaast valt onder de reikwijdte van het toezicht ook alle verwerkingen van persoonsgegevens van bestuursorganen van de gemeente.

4.6 Beveiliging
Op grond van de AVG en WPG dienen organisaties passende technische en organisatorische maatregelen te nemen om de persoonsgegevens die zij verwerkt, te beveiligen. Wij hebben een Strategisch en Tactisch Informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling is gegeven aan de passende beveiliging van persoonsgegevens.

4.7 Gegevens delen met derden
Wanneer er sprake is van gegevensuitwisseling met derde partijen, worden er schriftelijke afspraken gemaakt over de gegevensuitwisseling in de vorm van een onderlinge regeling, samenwerkingsovereenkomst (convenant), een gegevensuitwisselingsovereenkomst of een verwerkersovereenkomst.

Er is een model verwerkersovereenkomst aanwezig.[13] Een overzicht van Verwerkers wordt bijgehouden in ons register van verwerkingsactiviteiten. De proceseigenaren zijn verantwoordelijk voor het beheer en archivering van de originele ondertekende overeenkomsten. Wij gebruiken zoveel mogelijk landelijke standaarden en richtlijnen om de contractuele verplichtingen te regelen met derden. Dit is uitgewerkt in werkinstructies en gewaarborgd in het inkooptraject.[14]

Met betrekking tot doorgifte naar derde landen hanteren wij het uitgangspunt dat persoonsgegevens niet worden doorgegeven aan een bedrijf of vestiging in een land buiten de EU en de Europese Economische Ruimte (EER), tenzij deze doorgifte aantoonbaar rechtmatig is. Rechtmatigheid kan worden aangetoond in een van de volgende vier gevallen:
- Een adequaatheidsbesluit.
- Passende waarborgen middels een modelcontract (Standard Contractual Clauses).
- Binding corporate rules (BCR).
- Specifieke wettelijke uitzonderingen.[15]

5. Taken, bevoegdheden & verantwoordelijkheden

Het college is eindverantwoordelijk voor het naleven van de privacy wet- en regelgeving en de kaders voor het verantwoord omgaan met persoonsgegevens. Het college legt hiervoor verantwoording af aan de gemeenteraad. Dit is gelijk aan de 10 informatiebeveiligingsprincipes.[16] Wij hebben de verantwoordingsplicht om te kunnen aantonen dat deze uitgangspunten en kaders worden nageleefd. Elke ambtenaar binnen onze organisatie is intern verantwoordelijk voor de juiste implementatie en adoptie van dit privacybeleid. Wij hanteren hierbij het 'Three Lines' model. De concrete interne taakverdeling is vastgelegd in interne instructies.[17]

De teammanagers dragen de eerstelijnsverantwoordelijkheid. Zij zijn daarmee een onmisbare en noodzakelijke schakel om namens het college te voldoen aan privacy wet- en regelgeving. Deze interne verantwoordelijkheid dragen teammanagers voor de verwerkingsprocessen die binnen hun teams plaatsvinden. Elk team heeft hiervoor een privacy ambassadeur aangewezen. De privacy ambassadeur fungeert als het eerste aanspreekpunt als het gaat om privacyvraagstukken. Bij complexe vraagstukken of escalatie kan de privacy ambassadeur het Privacy Team inschakelen.

Het Privacy Team heeft een tweedelijnsverantwoordelijkheid voor advisering over en monitoring van de naleving van privacy wet- en regelgeving binnen het openbare lichaam, de bedrijfsvoering en de bestuursorganen van de gemeente.

13 Standaardmodel Verwerkersovereenkomst Sittard-Geleen
14 Handboek inkoop, v.1.9 14-09-2021
15 https://autoriteitpersoonsgegevens.nl, zoek op doorgifte-binnen-en-buiten-de-eu
16 Strategisch Informatiebeveiligingsbeleid, zie p. 9
17 20210127 SG Memo Actiepunten

De FG controleert als onafhankelijk toezichthouder of de naleving van privacy wet- en regelgeving voldoende aantoonbaar is en is bevoegd om gevraagd en ongevraagd te informeren en te adviseren. Adviezen van de FG dienen door de eerste en tweede lijn te worden opgevolgd door middel van het 'comply or explain' principe.

6. Kennisniveau

Kennis van de verplichtingen uit privacy wet- en regelgeving bij alle medewerkers is noodzakelijk om dit privacybeleid goed te kunnen uitvoeren. Wij verwachten dan ook dat elke medewerker voldoende kennis en bewustzijn heeft van de bescherming van persoonsgegevens en informatiebeveiliging.

Op verschillende wijzen werken wij aan voortdurende verbetering van onze kennis. Dit kan zijn via onze digitale leeromgeving en interne portalen. Zo borgen wij dat iedereen tenminste weet wanneer er sprake is van (bijzondere of gevoelige) persoonsgegevens en informatie. Periodiek vragen wij ook doorlopend aandacht voor het:
- Herkennen en melden van een datalek.
- Kwalificeren van persoonsgegevens en informatie.
- Zijn van transparant richting iedereen en het borgen van rechten van individuen.
- Het uitvoeren van een risicogebaseerd beleid waarbij aandacht is voor het op de juiste wijze afwegen van betrokken belangen.

Elke teammanager is verantwoordelijk voor informerende en voorlichtende activiteiten op het gebied van privacy en informatiebeveiliging binnen het team. Het Privacy Team stelt samen met het team HR ieder jaar een planning op ter verbetering van het kennisniveau binnen onze organisatie.

7. Baseline Informatiebeveiliging Overheid

Wij conformeren ons aan de Baseline Informatiebeveiliging Overheid (BIO), de norm voor informatiebeveiliging binnen de gehele publieke sector. De BIO is doorontwikkeld naar de nieuwe BIO2 die is gebaseerd op de internationale ISO 27001-norm en ISO 27002-norm en beschrijft de minimale maatregelen die wij moeten nemen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen.

Wij zorgen ervoor dat informatiebeveiliging integraal onderdeel is van onze bedrijfsprocessen en dat deze maatregelen voortdurend worden geëvalueerd en verbeterd.
Dit houdt onder meer in:
- Risicomanagement: Wij voeren regelmatig risicoanalyses uit om potentiële beveiligingsrisico's te identificeren en passende maatregelen te treffen om deze risico's te beperken.
- Beveiligingsmaatregelen: Wij nemen passende technische en organisatorische maatregelen, zoals encryptie, toegangscontrole en logging, om de beveiliging van systemen en gegevens te waarborgen.
- Bewustwording en training: Wij trainen en informeren onze medewerkers en politiek bestuurders regelmatig over de eisen en verantwoordelijkheden op het gebied van informatiebeveiliging.
- Incidentmanagement: Wij beschikken over een incidentmanagementproces voor het tijdig detecteren, melden en afhandelen van beveiligingsincidenten en datalekken.

Met het naleven van de BIO zorgen wij ervoor dat de verwerking van persoonsgegevens veilig verloopt en dat de bescherming van persoonsgegevens in overeenstemming is met de AVG.

8. Wet politiegegevens

Voor buitengewoon opsporingsambtenaren (boa's) van de gemeente zijn naast de AVG de WPG en enkele andere regelingen van toepassing op de verwerking van politiegegevens, zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens. De WPG bevat enkele specifieke bepalingen die anders zijn dan de AVG.

De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van politiegegevens te maken met de AVG. De WPG gaat voor op de AVG voor zover het gaat om de verwerking van politiegegevens door de boa in zijn rol als opsporingsambtenaar.

Bij de verwerking van persoonsgegevens moet steeds duidelijk zijn wanneer een verwerking onder de AVG of onder de WPG valt. Dit is nodig om specifieke verplichtingen uit de WPG te kunnen borgen zoals de wettelijke plicht tot het ter beschikking stellen van politiegegevens aan iedere andere opsporingsambtenaar die deze gegevens nodig heeft voor de uitoefening van zijn taken.

In onze informatiesystemen hanteren we de volgende uitgangspunten:

- Politiegegevens die gebaseerd zijn op feiten worden gescheiden van politiegegevens die gebaseerd zijn op persoonlijke oordelen.
- Er is onderscheid gemaakt tussen de verschillende betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden.
- De doelen van de onderzoeken, de verstrekking of doorgifte, afwijzing van verzoeken om inzage, een inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvangers, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de AP zijn gedocumenteerd.
- Er vindt logging plaats van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er wordt voldaan aan de specifieke eisen voor de informatiebeveiliging die gesteld zijn vanuit het Bpg.

Het ter beschikking stellen en verstrekken van politiegegevens
De WPG maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit ‘need to know’-principe dient altijd een proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het WPG-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het WPG-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de WPG en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag als dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.

Bewustwording
Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Elke boa moet daarom verplicht een WPG-training doorlopen. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek WPG-onderwerp of in de vorm van een toets. Ook van deelname aan deze initiatieven wordt een notitie in het personeelsdossier gemaakt.

Open communicatie
Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. Wij creëren dat vertrouwen door via verschillende communicatiekanalen inzichtelijk te maken op welke wijze wij persoonsgegevens verwerken en beheren. Informatie hierover is onder meer terug te vinden in onze privacyverklaring op onze website.

9. Uitwerking en evaluatie

Dit privacybeleid is opgesteld op basis van de Plan-Do-Check-Act cyclus en voor advies voorgelegd aan de FG.

Dit privacybeleid dient door het lijnmanagement uitgewerkt te worden in specifiek uitvoeringsbeleid, nadere richtlijnen en/of werkinstructies. Het Privacy Team biedt hierbij ondersteuning waar nodig. Uiterlijk drie jaar na vaststelling, of eerder als daar aanleiding toe is, wordt dit privacybeleid geëvalueerd en waar nodig geactualiseerd.

Specifiek uitvoeringsbeleid, richtlijnen en werkinstructies worden jaarlijks door het verantwoordelijke lijnmanagement geëvalueerd. Hierover dient door het lijnmanagement te worden gerapporteerd aan de FG.

10. Inwerkingtreding

Het privacybeleid treedt in werking per 1 februari 2026.