Gemeente Sittard-Geleen

GEMEENTEBLAD

Officiële uitgave van de gemeente Sittard-Geleen

Nr. 418280

22 november 2021

Privacybeleid Sittard-Geleen 2021-2024

Het college van burgemeester en wethouders van de gemeente Sittard-Geleen besluit:
1. Vaststellen van het privacybeleid Sittard-Geleen 2021-2024;
2. Kennisnemen en onderschrijven van de kernwaarden als omschreven in het privacybeleid Sittard-Geleen 2021-2024 op pagina 3 en 4;
3. Intrekken privacybeleid 2018.

1. Inleiding

De gemeente Sittard-Geleen behandelt mensen met respect. Privacy staat bij ons daarom hoog in het vaandel. Dit privacybeleid dient daarbij als een kapstok. Het doel van dit privacybeleid is om te beschrijven hoe wij aantoonbaar op een juiste wijze omgaan met persoonsgegevens. De Algemene Verordening Gegevensbescherming (hierna: AVG) is daarbij het centrale kader. Dit biedt ons een belangrijke houvast voor de wijze waarop wij omgaan met persoonsgegevens. Het beleid is geschreven voor alle burgers, partners en onze medewerkers. Het beleid heeft betrekking op de (onderdelen van de) gemeente Sittard-Geleen als bestuursorgaan en als werkgever. Dit stuk beschrijft de context van het beleid, de doelen en de uitgangspunten voor ons handelen. Daarmee maken we inhoudelijke keuzes binnen de kaders van de AVG en verwante sector wet- en regelgeving.

Digitalisering en de toepassing van nieuwe technologieën leiden tot veranderingen in de samenleving. Hierdoor verschuiven ook de verwachtingen die inwoners hebben van de gemeentelijke 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 een zorgvuldige verwerking van informatie, zeker als het gaat om persoonsgegevens. Persoonsgegevens dienen goed te worden beschermd door middel van de juiste maatregelen wat betreft Informatieveiligheid. In de Baseline Informatiebeveiliging Overheid (BIO), die van toepassing is op de gemeente Sittard-Geleen, zijn normen bepaald voor informatieveiligheid. Deze zijn nader uitgewerkt in informatiebeveiligingsbeleid.[1]

In dit privacybeleid wordt beschreven hoe de gemeente invulling geeft aan de centrale privacy uitgangspunten en de verplichtingen die de AVG met zich meebrengt. Dit beleid is vervolgens in de organisatie nader uitgewerkt in operationeel beleid en werkinstructies voor een juiste implementatie. In dit stuk wordt geschreven over “de gemeente”, “ons” of “wij”. Dit refereert altijd aan de gemeente Sittard-Geleen.

1.1 Kernwaarden en ambities

De gemeente Sittard-Geleen ziet het beschermen van de gegevens van de burgers als een van de belangrijkste prioriteiten. Daartoe hanteren we onderstaande kernwaarden.

De vijf kernwaarden

A. *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 verwacht de gemeente meer in die behoefte te voorzien. Zo werkt de gemeente in de basis digitaal, tenzij de context het niet toelaat.[2]

B. *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.

C. *Digitale veiligheid*: bij digitaal werken is digitale veiligheid en privacy van essentieel belang. Burgers moeten er op kunnen vertrouwen dat gegevens veilig zijn bij ons. Het privacybeleid steunt dan ook op de 3 algemene privacy uitgangspunten, lees hoofdstuk 3, en de 10 principes van informatiebeveiliging.[3]

1) Informatiebeveiligingsbeleid (tactisch en strategisch)

2) Visie document: Organisatie en manier van werken (mei 2020) inclusief bijlagen, zie p. 9

3) Strategisch Informatiebeveiligingsbeleid, zie p. 15

D. *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 (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 de rechtsgrond Toestemming.
E. *Openheid*: Wij hechten er veel waarde aan dat onze burgers vertrouwen hebben in ons als gemeente. Daarbij speelt transparantie een belangrijke rol. Dit betekent dat wij de burgers op passende manieren informeren over de privacy rechten. Hiervoor gebruiken wij diverse (niet-)digitale kanalen. Daarnaast informeren wij de burgers door een algemene privacyverklaring.[4]

Deze kernwaarden worden nader uitgewerkt in dit privacybeleid en de stukken waar naar wordt verwezen.

Ambities
De afgelopen jaren heeft de gemeente Sittard-Geleen hard gewerkt om te voldoen aan de privacy wet- en regelgeving. Hierbij zijn externe experts ingehuurd en is intern meer budget vrij gekomen voor dit thema. Zo is aan de hand van het CIP model, nader omschreven in hoofdstuk 5, gekeken naar het privacy volwassenheidsniveau binnen de gemeente.[5] Begin 2021 was het volwassenheidsniveau overwegend niveau 3, maar nog niet organisatie breed.

Onze doelstelling is om te groeien naar een privacy volwassenheidsniveau 3 op alle privacy thema's in 2021 in de gehele organisatie. Daarnaast is het de ambitie om door te groeien naar overwegend niveau 4 in 2025. Dit privacybeleid vormt de basis voor de gemeente Sittard-Geleen om deze ambitie waar te maken. Aan de hand van dit beleid zal er een privacy compliance risicobeheersingsraamwerk opgezet worden. Op deze manier kan doorlopend worden bijgehouden waar de gemeente staat.

1.2 Scope van dit beleid
Het privacybeleid omvat de gehele datastroom van persoonsgegevens binnen de 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 de gehele organisatie van (de bestuursorganen van) de gemeente Sittard-Geleen.

Dit beleid is/wordt nader uitgewerkt in operationeel beleid, werkinstructies en richtlijnen. Wanneer sprake is van 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.

Het beleid strekt zich ook uit over de verwerkingen van persoonsgegevens op grond van de wet Basisregistratie Personen (BRP) en op de verwerkingen waarop de Archiefwet van toepassing is. Uiteraard voor zover deze specifieke wet- en regelgeving geen afwijkende eisen stellen.[6]

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)***

4) Privacyverklaring (website), zoekterm privacy
5) Grip op Privacy: de Privacy Baseline (versie 3.2)
6) Persoonsgegevens mogen alleen o.b.v. de Archiefwet worden bewaard als deze in overeenstemming met de AVG zijn verzameld. Voor het archiveren en bewaren wordt specifiek beleid opgesteld. Verwerkingen op basis van de wet BRP kennen een eigen regime dat minimaal gelijk is aan of strenger is dan de AVG-regels.

In het Nederlands vertaald naar gegevensbeschermingseffectbeoordeling, maar de gangbare term is DPIA. Dit 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 privacy risico 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 model om te beoordelen of een DPIA verplicht is of niet.
- ***Functionaris Gegevensbescherming (FG)***
  Een onafhankelijke en 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).
- ***Privacy Team***
- Binnen de gemeente zijn meerdere rollen belegd met controle en aanpassing van het privacybeleid. Onder het Privacy Team wordt onder meer verstaan de Privacy Officer(s), Adviseur privacy & security en de FG.
- ***Persoonsgegevens***
  Informatie uit data 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 bij verwerkingen in opdracht en ten behoeve van de verwerkingsverantwoordelijke.
- ***Verwerking***
  Alles wat je met persoonsgegevens kan 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 om een zorgvuldige afweging. Naast het belang van de individuele burger, is er het publieke (algemeen) belang en zijn er belangen van burgers ten opzichte van elkaar.

- **Belang van de burger**: een burger wil dat zijn 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 burger er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de inwoner efficiënte dienstverlening, waarbij wij niet naar de bekende weg vragen.
- **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 burgers ten opzichte van elkaar**: de bescherming van de rechten van de ene burger kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander.

Voordat persoonsgegevens worden verwerkt vindt er een belangenafweging plaats. Daarbij worden de privacy uitgangspunten als beschreven in hoofdstuk 3 meegewogen. De gemeente maakt een analyse, zodat de risico's van de verwerking vooraf inzichtelijk zijn. Na een onderbouwde belangenafweging wordt besloten of de gegevensverwerking kan plaatsvinden. Daarbij worden risico's zoveel mogelijk verkleind met de juiste maatregelen. Dit wordt nader uitgewerkt in paragraaf 4.2.

3. Privacy uitgangspunten

De AVG omschrijft een aantal uitgangspunten die centraal staan in dit beleid. De gemeente Sittard-Geleen 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 en de wijze waarop wij deze concreet invulling geven binnen onze organisatie.

3.1 Rechtmatigheid

- Wij gaan uit van de geldende wet- en regelgeving voor gegevensverwerking en hanteren de AVG als basis. Voor verwerking van persoonsgegevens moet er altijd een wettelijke grondslag bestaan.
- Het kan zijn dat wij persoonsgegevens vaker moeten gebruiken. Dit kan alleen als dat doel verenigbaar is met de oorspronkelijke verzameldoeleinden. Mocht blijken dat het niet verenigbaar is dan zal worden gekeken naar een rechtmatige grondslag. Dit wordt getoetst bij ons Privacy Team.
- 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.[7]
- Diverse gemeentelijke taken vereisen het gebruik van persoonsgegevens. In deze gevallen is het doel in de wet vastgelegd. Tevens wordt in het verwerkingsregister per verwerking bijgehouden op welke grondslag en met welk doel dit gerechtvaardigd is.
- Bij de gegevensverwerking wordt rekening gehouden met de beginselen van 'proportionaliteit' en 'subsidiariteit'. Wij vragen slechts die informatie die noodzakelijk is om het beoogde doel te bereiken. Daarbij gebruiken wij altijd de minst ingrijpende methode voor de betrokkenen.

3.2 Behoorlijkheid

- Wij hanteren het principe van 'minimale gegevensverwerking'. Dit wilt 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 teveel 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 slechts mogelijk als hier een wettelijke grondslag en verenigbaar doel voor is. De grondslag en verenigbaarheid wordt niet op werknemer niveau bepaald. Dit wordt op teamniveau vastgelegd middels werkinstructies en autorisaties om heldere kaders te schetsen voor onze medewerkers.[8]
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is. De noodzakelijkheid is voor ons altijd gerelateerd aan het doeleinde waarvoor de betreffende persoonsgegevens zijn verzameld. Vaak is dit op basis van wettelijke bewaartermijnen. Wanneer de wet hier niet in voorziet staan de bewaartermijnen beschreven in ons verwerkingsregister. De gemeente Sittard-Geleen bewaart persoonsgegevens in ieder geval in overeenstemming met de "Selectielijst gemeenten en intergemeentelijke organen 2020".[9] De interne organisatie heeft toegang tot het verwerkingsregister om de bewaartermijnen te raadplegen. Verder zijn er werkinstructies voor het gebruik van dit register.
- Alleen functionarissen (ambtenaren, externen, leveranciers, convenantpartners) waarvoor het voor de directe taakuitoefening noodzakelijk is, hebben inzage in persoonsgegevens. Deze gegevens worden vertrouwelijk behandeld. Verder hebben wij een autorisatiebeleid zodat slechts ambtenaren toegang hebben tot de gegevens die hier ook echt een doel voor hebben.[10]
- 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' wordt al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht aan privacy verhogende maatregelen geschonken.

7) Verwerkingsregister (iNavigator)

8) Tactisch informatiebeveiligingsbeleid onder 2.5, zie p. 11-12.

9) Selectielijst gemeenten en intergemeentelijke organen 2020, https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf

10)Tactisch informatiebeveiligingsbeleid onder 2.5, zie p. 11-12.

- Het is voor zowel ons als de burgers van belang dat persoonsgegevens actueel en correct zijn. Er worden diverse projecten en processen periodiek uitgevoerd om de basis registratie personen actueel en juist te houden. Dit is tevens een wettelijke verantwoordelijkheid.

3.3 Transparantie

- Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente Sittard-Geleen over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Dit gebeurt onder meer door onze privacyverklaring op de website.[11] Verder wordt per team bekeken hoe betrokkenen op een passende wijze worden geïnformeerd. Dit is vastgelegd in werkinstructies om te voldoen aan de informatieplicht onder de AVG.
- Burgers hebben de mogelijkheid om te vragen waarom en welke persoonsgegevens wij van hen verwerken. In de basis verstrekken wij de gevraagde informatie tenzij de wet anders aangeeft. Verder kunnen burgers om verbetering, aanvulling of verwijdering van persoonsgegevens verzoeken. Dit verzoek wordt gehonoreerd, tenzij ook hier weer de wet anders heeft bepaald (bijvoorbeeld opsporingsbelang).
- Om recht te doen aan verzoeken van betrokkenen hebben wij een Procedure rechten van betrokkenen vastgesteld.[12] 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.
- Wij zijn transparant over het type persoonsgegevens dat wij voor een specifiek doel met derden delen. Daarbij kan het zijn dat er een uitzondering is wanneer er belangen zijn, genoemd in wet- of regelgeving, die zich daartegen verzetten. Type persoonsgegevens worden bijgehouden in het verwerkingsregister en zijn opvraagbaar.
- Wij zijn open en transparant over hoe wij met persoonsgegevens omgaan. Door de waarborg dat afwijkingen van dit beleidskader beargumenteerd worden voorgelegd aan het Privacy Team. Indien nodig zal de interne toezichthouder (de FG) escaleren naar het college en/of de burgemeester. Zo wordt maximaal invulling gegeven aan transparantie richting inwoners en de raad.

4. Algemene Verordening Gegevensbescherming

De AVG legt diverse verplichtingen op aan gemeenten. Hieronder worden deze verplichtingen omschreven inclusief de feitelijke uitwerking daarvan binnen onze organisatie. Dit geeft tevens weer hoe wij verdere invulling geven aan de privacy uitgangspunten als omschreven in het vorige hoofdstuk.

4.1 Het verwerkingsregister

Binnen de gemeente werken wij met zeer veel processen en dus ook diverse verwerkingen van persoonsgegevens. Middels een verwerkingsregister wordt precies bijgehouden waar welke verwerkingen plaats vinden. In dit register staat de volgende informatie vermeld:

- De naam en contactgegevens van de vertegenwoordiger namens de gemeente Sittard-Geleen, de FG en eventuele andere organisaties waarmee de gemeente Sittard-Geleen gezamenlijk verwerkingsverantwoordelijke is;
- 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 het verwerkingsregister. Proceseigenaren binnen de teams zijn verantwoordelijk voor het opnemen van nieuwe verwerkingen in het verwerkingsregister. Zij worden hierbij geadviseerd door de Privacy Officer(s). De FG controleert of het register volledig en up-to-date is. Middels een memo zijn de rollen en verantwoordelijkheden ten aanzien van het beheer van het register van verwerkingsactiviteiten vastgelegd.[13]

11) Privacyverklaring (website), zoekterm privacy

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

13) 20210127 SG Memo Actiepunten

4.2 Data Protection Impact Assessment (DPIA)

De gemeente staat niet stil en wij zijn altijd in ontwikkeling. Zo worden processen en systemen periodiek aangepast. Daardoor kan er sprake zijn van een nieuwe verwerking of wijziging van een bestaande verwerking. Om de privacy risico's in kaart te brengen voor een juiste belangenafweging voeren wij vooraf een DPIA-Toets uit.[14] De uitvoering van de DPIA-Toets valt onder de verantwoordelijkheid van de teammanager. Deze kan een DPIA verantwoordelijke binnen het proces aanwijzen. Aan de hand van de uitgevoerde DPIA-Toets worden voor zowel informatiebeveiliging als privacy, een risico-inventarisatie uitgevoerd.

Op basis van de uitgevoerde DPIA-Toets wordt bepaald of voor een afzonderlijke verwerking een hoog risico bestaat. Is dit niet het geval dan kan een privacy advies van het Privacy Team volstaan. Wanneer een verwerking wel een hoog privacy risico voor betrokkenen met zich meebrengt wordt er eerst een DPIA uitgevoerd. Een DPIA geeft inzicht in welke maatregelen getroffen moeten worden om het risico te verkleinen naar een minimaal en acceptabel niveau. Hiermee wordt invulling gegeven aan een juiste belangenafweging.

De gemeente Sittard-Geleen hanteert hiervoor een standaard DPIA model.[15] Proceseigenaren zijn verantwoordelijk voor de uitvoering van een DPIA voor een verwerking met een hoog privacy risico. De gemeente hanteert hierbij een handreiking ter verduidelijking voor de DPIA verantwoordelijke.[16] Het Privacy Team ondersteunt en adviseert bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde DPIA en ondertekent de DPIA.

Het Privacy Team houdt een register bij van uitgevoerde DPIA´s en monitort de voortgang van het DPIA proces. Er wordt gekeken naar de geïmplementeerde beheersmaatregelen en gerapporteerd aan de FG.[17]

Processen kunnen regelmatig worden aangepast met mogelijke effecten op de verwerking. Als er een wijziging in het proces wordt doorgevoerd is het noodzakelijk om een eerder uitgevoerde DPIA te herzien en te kijken of de wijziging ook nieuwe risico's met zich meebrengt. Kleine risico's kunnen groter worden, maar grote risico's kunnen ook kleiner worden. Dit wordt meegenomen bij een herijking van een DPIA.

4.3 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 van producten en diensten 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 wordt aan het begin voor de uitvoer van projecten meegenomen. Dit wordt gewaarborgd door een Privacy Officer mee te laten kijken in de voorfase van een project. De FG ziet er op toe dat dit ook gebeurt.

Privacy by Default: houdt in dat de standaardinstellingen van een programma ingesteld dienen te worden op de meest privacy vriendelijke manier. Zoals beschreven in paragraaf 4.2 geldt voor de gemeente Sittard-Geleen dat voor een nieuwe verwerking of een wijziging in een bestaande verwerking een DPIA-Toets uitgevoerd dient te worden. Door deze toets wordt aan de voorkant helder of een uitgebreidere 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. Zo worden in formulieren geen gegevens gevraagd die overbodig zijn. Dit helpt tevens mee aan het principe van dataminimalisatie. Op deze manier wordt geborgd dat nieuwe verwerkingen conform de normen van *Privacy by Design* en *Privacy by Default* worden ingericht.

4.4 Datalekken

Een datalek heeft potentieel een grote impact op betrokkenen en ons als organisatie. Er worden daarom meerdere processen, systemen en acties ingezet om datalekken te voorkomen. Volledig uitsluiten is onmogelijk, maar wij zetten ons in om een cultuur te creëren waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Het kan namelijk zo zijn dat een datalek gemeld moet worden bij de

14) DPIA toets document – versie 15-01-2021
15) Template L2P DPIA model versie 3.1 – versie 15-01-2021
16) DPIA Handreiking versie 3.1 – versie 15-01-2021
17) DPIA planning is onder beheer van het Privacy Team

Autoriteit Persoonsgegevens (hierna: "AP") en/of betrokkenen binnen 72 uur. Indien wij niet of niet tijdig melden lopen wij een risico op een boete van de AP. Deze kan oplopen tot een maximum van 20 miljoen euro of 4% van een jaaromzet. Los van een morele verplichting is er dus ook een financieel risico wanneer niet wordt voldaan aan de meldplicht.

Om te voldoen aan bovengenoemde verplichtingen is er een *procedure datalekken* opgesteld.[18] Hier staat beschreven op welke wijze datalekken worden afgehandeld en wie daarbij welke taken en verantwoordelijkheden heeft. In deze procedure staat ook beschreven hoe en wanneer een datalek dient te worden gemeld bij de AP en/of betrokkenen. Daarnaast ontvangen onze medewerkers meerdere malen per jaar informatie over dit thema om de bewustwording op peil te houden. Tevens staat de gemeente Sittard-Geleen voor een open en veilige cultuur zodat medewerkers zich veilig voelen om datalekken te melden. Dit wordt bevordert door de bestuurders.[19] Tot slot staat op het interne portaal van de gemeente Sittard-Geleen diverse aanvullende bronnen ten aanzien van het melden van datalekken.

Om te blijven anticiperen op mogelijke risico's wordt er een intern datalekregister bijgehouden waarin alle geconstateerde beveiligings-incidenten worden geregistreerd. Hierin wordt vastgelegd of het beveiligingsincident heeft geleid tot een datalek en indien dat het geval is, het datalek ook is gemeld bij de toezichthouder en/of de betrokkenen. Jaarlijks wordt het datalekregister geëvalueerd om trends bij te houden en structurele verbeteringen intern door te voeren. Tevens worden gevoelige datalekken direct geëvalueerd om zo dringende aanpassingen gelijk door te voeren in de organisatie.

4.5 Functionaris Gegevensbescherming (FG)

De gemeente Sittard-Geleen is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Het is in dit geval een wettelijke verplichting een FG aan te stellen.

De FG is als interne toezichthouder betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De rol kan door een interne medewerker worden uitgevoerd of door een externe partij. De gemeente heeft er voor gekozen om de rol van FG bij een externe partij te beleggen. Hij wordt hierin ondersteunt door ons interne Privacy Team.

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 toezichtplan. De FG rapporteert jaarlijks over de naleving van privacy wet- en regelgeving aan het college van B&W. De FG heeft onder meer de volgende wettelijke taken:

- Informatievoorziening;
- Toezicht op de implementatie van de privacy wet- en regelgeving;
- Contactpersoon voor de Autoriteit Persoonsgegevens;
- Periodieke verslaglegging aan college van B&W over de uitvoering van zijn taken;
- Het zorg dragen voor een juiste afwikkeling van de vragen of klachten van Betrokkenen;
- Adviseren en beoordelen van uitgevoerde DPIA's.

4.6 Beveiliging

Op grond van de AVG dienen organisaties passende technische en organisatorische maatregelen te nemen om de persoonsgegevens die zij verwerkt, te beveiligen. De gemeente Sittard-Geleen heeft een Strategisch en Tactisch Informatiebeveiligingsbeleid opgesteld waarin is beschreven op welke wijze invulling is gegeven aan de passende beveiliging van persoonsgegevens. Tevens is er een Adviseur Security & Privacy en een Security Officer aangesteld. Wij maken geen gebruik van verwijderbare media. Dit wordt ook uitgedragen door de managers in de organisatie.

4.7 Gegevens delen met derden

Wanneer er 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.

Er is een model verwerkersovereenkomst aanwezig dat inhoudelijk voldoet aan de eisen die de AVG daaraan stelt.[20] Verwerkers worden bijgehouden in het verwerkingsregister van de gemeente Sittard-

18) Procedure datalekken (intranet gemeente), zoekterm "melden datalek"
19) Strategisch Informatiebeveiligingsbeleid, zie p. 9
20) Standaardmodel Verwerkersovereenkomst Sittard-Geleen 01062021 (versie 2.4)

Geleen. De ondertekende versies van de verwerkersovereenkomsten behoren bij de proceseigenaren te zijn gearchiveerd. De gemeente Sittard-Geleen gebruikt zoveel mogelijk landelijke standaarden en richtlijnen om de contractuele verplichtingen te regelen met derden. Dit is uitgewerkt in werkinstructies en gewaarborgd in het inkooptraject.[21]

Met betrekking tot doorgifte 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. Rechtmatigheid wordt aangetoond in een van de volgende vier gevallen:

- Een adequaatheidsbesluit;
- Passende waarborgen middels een modelcontract (Standard Contractual Clauses);
- Binding corporate rules (BCR);
- Specifieke uitzonderingen.[22]

5. Risico's

Het privacy control framework van de gemeente Sittard-Geleen is vormgegeven door de Privacy baseline en het Privacy volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Dit dient als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. De Privacy baseline en het Privacy volwassenheidsmodel van het CIP geven invulling aan het normenkader voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente Sittard-Geleen. Hierbij houden wij nauwlettend nieuwe methodieken en modellen in de gaten wanneer deze specifiek zijn opgesteld voor gemeenten, zoals het borgingsproduct van de VNG.[23] In de basis zal de essentie gelijk blijven, maar kan de vorm en benaming tussentijds wijzigen mits dit geen wezenlijke impact heeft op de praktijk.

Op basis van de Privacy baseline en het Privacy volwassenheidsmodel zal de gemeente Sittard-Geleen kerncontrolepunten en bijbehorende werkprogramma's vaststellen.

Bij het niet voldoen aan de relevante wet- en regelgeving is het College van B&W wettelijk aansprakelijk. Niet voldoen kan leiden tot:

- Klachten van betrokkenen;
- Verlies van vertrouwen in de (lokale) overheid;
- Imagoschade voor de gemeentelijke organisatie;
- Datalekken;
- Schadevergoedingen;
- Onderzoeken, dwangmaatregelen en (hoge) bestuurlijke boetes.

De risico's van schending van de privacy voor betrokken personen variëren van ongemak, substantiële benadeling, ernstige sociale beschadiging of gevaren voor de gezondheid en de persoonlijke veiligheid. Dit beleid in combinatie met het informatiebeveiligingsbeleid en de stukken waarnaar wordt verwezen, hebben als doel deze risico's te verkleinen.

6. Taken & verantwoordelijken

Het College is verantwoordelijk voor het naleven van de uitgangspunten uit de privacy wet- en regelgeving en de kaders voor het verantwoord omgaan met persoonsgegevens. Dit is gelijk aan de 10 informatiebeveiligingsprincipes.[24] 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. Wij hanteren hiervoor het zogeheten 'Three Lines of Defense' model. Hieronder wordt dit principe kort toegelicht. De concrete interne taakverdeling om dit te borgen is vastgelegd in interne instructies.[25]

21) Handboek inkoop, nog in ontwikkeling
22) https://autoriteitpersoonsgegevens.nl, zoek op doorgifte-binnen-en-buiten-de-eu
23) Borgingsproduct 2.0 VNG
24) Strategisch Informatiebeveiligingsbeleid, zie p. 9
25) 20210127 SG Memo Actiepunten

De teammanagers dragen de eerstelijnsverantwoordelijkheid. Zij zijn daarmee een onmisbare en noodzakelijke schakel om namens het College (als interne eindverantwoordelijke), te voldoen aan privacy wet- en regelgeving. Deze interne verantwoordelijkheid dragen teammanagers voor de verwerkingsprocessen die binnen hun teams plaatsvinden. Deze interne verantwoordelijkheid heeft vooral betrekking op de uitvoering van de verplichtingen uit o.a. de AVG en sectorale wetgeving die op het team van toepassing is. Elk team zal een privacy ambassadeur aanwijzen. Deze ambtenaar zal fungeren als het eerste aanspreekpunt als het gaat om privacy vraagstukken. Bij complexe vraagstukken of escalatie zal het Privacy Team worden ingeschakeld.

Wij hebben een team van privacy professionals dat het College ondersteunt in de beleidsuitvoering van privacy. Dit team wordt het Privacy Team genoemd. Zij zorgen dat er centraal inzicht is in de naleving van privacy wet- en regelgeving binnen alle organisatieonderdelen en bestuursorganen van de gemeente. Daarnaast draagt het Privacy Team door middel van advisering en monitoring een tweedelijnsverantwoordelijkheid voor de naleving van de privacy wet- en regelgeving binnen de gemeente. Op deze wijze draagt het Privacy Team actief bij aan de door het College geambieerde privacy volwassenheidsniveau.

Ten slotte is er de FG die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert. Daarover velt hij 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. Wij verwachten dat elke medewerker een adequaat niveau van bewustwording heeft als het gaat om privacy en informatiebeveiliging. Er zijn diverse (online) middelen om de bewustwording van medewerkers te vergroten. Zo is gewaarborgd dat medewerkers weten wanneer er sprake is van (bijzondere) persoonsgegevens en gewone gegevens. Hier wordt aandacht aan besteed in o.a. een digitale leeromgeving en via berichtgeving op interne portalen. Zo komen periodiek onder meer de volgende thema's aan bod:

- Herkennen en melden van een datalek;
- Het kwalificeren van persoonsgegevens en overige informatie;
- Het informeren van de betrokkenen;
- Het uitvoeren van een DPIA;
- Et cetera.

In het kader van bewustwording is de teammanager verantwoordelijk voor informerende en voorlichtende activiteiten op het gebied van privacy binnen zijn/haar team. Hierbij is in ieder geval de meldplicht datalekken een terugkerend onderwerp is. Verder worden nieuwe medewerkers gemotiveerd om binnen 3 maanden na indiensttreding een digitale training te volgen. Zo wordt de bewustwording gelijk tot het minimale vereiste niveau gebracht. Het Privacy Team in combinatie met de afdeling communicatie stellen ieder jaar een jaarplanning op om de bewustwording organisatie breed op peil te houden.

8. Uitwerking en evaluatie

Dit privacybeleid is opgesteld volgens de PDCA methodiek (Plan-Do-Check-Act). Dit betekent dat het beleid is vastgesteld volgens een cyclisch proces. De Privacy Officer heeft dit jaar het privacy beleid opnieuw opgesteld. Hierbij zijn uitgebreide voorbereidingen getroffen en is gekeken naar de huidige bedrijfsvoering van de gemeente. Hierbij is ook gekeken naar het informatiebeveiligingsbeleid. Op basis daarvan is dit privacybeleid uitgebreider opgesteld waarbij de kernwaarden, en de uitvoering daarvan van de gemeente beter naar voren komt. Dit privacybeleid is vervolgens voorgelegd bij de FG voor advies alvorens het is vastgesteld door het College. Dit is vervolgens door de gehele organisatie gecommuniceerd via diverse kanalen.

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 als adviseurs. Eens in de drie jaar, of eerder indien daar aanleiding toe is, wordt dit privacybeleid geëvalueerd en aangepast.

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

In 2024 zal dit proces wederom worden herhaald mocht eerdere herziening niet noodzakelijk zijn. Hierbij zal wederom dit cyclisch proces worden toegepast.

9. Inwerkingtreding

Het privacybeleid treedt in werking per 5 oktober 2021.

Vastgesteld door het college van burgemeester en wethouders op 5 oktober 2021.

Bijlage 1

- Template L2P DPIA model versie 3.1 – versie 15-01-2021
- DPIA Handreiking versie 3.1 – versie 15-01-2021
- DPIA toets document – versie 15-01-2021
- 20210127 SG Memo Actiepunten
- Strategisch Informatiebeveiligingsbeleid
- Tactisch Informatiebeveiligingsbeleid
- Visie document: Organisatie en manier van werken (mei 2020)

Bijlage 2

Operationeel privacybeleid, richtlijnen, werkinstructies
- Privacybeleid Sociaal domein;
- Mogelijk datalek melden procedure;
- Rechten van betrokkenen;
- DPIA procedure;
- Cameraprotocol;
- Algemene privacyverklaring.

Bijlage 3

De lijn is verantwoordelijk voor het juiste operationeel beleid, richtlijnen en werkinstructies actueel en kloppend te houden met de huidige wet- en regelgeving. Deze bijlage kan van tijd tot tijd worden aangevuld afhankelijk van nieuwe wet- en regelgeving:

- Algemene wet inzake rijksbelastingen;
- Algemene wet Bestuursrecht;
- Archiefwet;
- Auteurswet;
- Boek 1 Burgerlijk Wetboek;
- Drank- en Horecawet;
- Gemeentewet;
- Grondwet;
- Handelregisterwet;
- Jeugdwet;
- Kadasterwet;
- Kieswet;
- Leerplichtwet;
- Omgevingswet;
- Participatiewet;
- Telecommunicatiewet;
- Wet algemene bepalingen Burgerservicenummer;
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
- Wet basisregistratie personen;
- Wet bijzondere maatregelen grootstedelijke problematiek;
- Wet maatschappelijke ondersteuning;
- Wet op de geneeskundige behandelingsovereenkomst;
- Wet Politiegegevens;
- Wet publieke gezondheid;
- Wet structuur uitvoeringsorganisatie werk en inkomen;
- Wet Verplichte GGZ;
- Wet WOZ.