

Privacybeleid gemeente Venlo 2024

De raad van de gemeente Venlo;
gelezen het voorstel van het college van 18 februari 2025, registratienummer 180935;
gelet op artikel 24 lid 2 van de Algemene verordening gegevensbescherming en artikel 4 lid 1 van de Wet politiegegevens;
overwegende dat de drie bestuursorganen van de gemeente Venlo een gelijkkluidend kader willen vaststellen voor het juist en conform de wet- en regelgeving verwerken van persoonsgegevens;
besluit:

Tot vaststelling van onderstaand Privacybeleid gemeente Venlo 2024.

1 KERNPUNTEN

1.1 Inleiding

Binnen de gemeente Venlo wordt gewerkt met een aanzienlijk aantal persoonsgegevens van inwoners, medewerkers en (keten)partners. Er worden veel persoonsgegevens verzameld voor het goed uitvoeren van de gemeentelijke taken en om te voldoen aan wettelijke verplichtingen. De gemeente gebruikt persoonsgegevens voor bijvoorbeeld haar salarisadministratie en om beleid te kunnen verbeteren wordt statistisch onderzoek uitgevoerd. Voor buitengewoon opsporingsambtenaren (boa's) geldt dat zij in het kader van hun opsporingstaak politiegegevens verwerken. Dit zijn persoonsgegevens die zij verwerken in het kader van hun opsporingstaak.

Alle betrokkenen moeten er op kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente Venlo is zich hiervan bewust en zorgt dat privacy, door middel van een continu verbeterproces, gewaarborgd wordt, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole. De gemeente Venlo geeft middels dit privacybeleid een duidelijke richting aan en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Er wordt getracht met dit beleid aan te geven hoe zij in algemene zin invulling geeft aan de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens, waaronder de Algemene verordening gegevensbescherming (hierna: AVG), de Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG), de Wet politiegegevens (hierna: Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (hierna: Bpg boa).

De definities uit de AVG, de UAVG, de Wpg en het Bpg boa worden in dit beleid gevolgd.

1.2 Voor wie?

Het Privacybeleid gemeente Venlo 2024 bevat afspraken tussen de bestuursorganen van de gemeente Venlo (bestaande uit het college van burgemeester en wethouders (hierna: "het college"), de gemeenteraad (hierna: "de raad") en de burgemeester (hierna gezamenlijk te noemen: "de bestuursorganen")) en vormt daarnaast een kader waarbinnen medewerkers die persoonsgegevens verwerken dienen te opereren.

1.3 Doel

Met de vaststelling van dit privacybeleid willen de bestuursorganen drie doelen bereiken:

1. De visie van de gemeente Venlo op het onderwerp privacy vastleggen.
2. Verantwoordelijkheden in dit kader beleggen.
3. Kaders stellen om te borgen dat de gemeente Venlo op een behoorlijke en zorgvuldige wijze persoonsgegevens verwerkt in overeenstemming met de wet.

1.4 Visie

Privacy is een grondrecht en een voorwaarde om vrij te zijn in wie je bent en wat je doet. Privacy omvat naast de persoonlijke levenssfeer en ontwikkeling ook de bescherming van persoonsgegevens, vertrouwelijke communicatie en integriteit van persoon en lichaam. De gemeente Venlo ziet privacy en de bescherming van persoonsgegevens als een zaak van behoorlijk bestuur. Inwoners en medewerkers moeten erop kunnen vertrouwen dat persoonsgegevens rechtmatig, zorgvuldig en veilig worden verwerkt. De bestuursorganen zorgen daarom voor de randvoorwaarden van een privacybewuste organisatiecultuur en voeren in dat kader een adequaat privacybeleid. Zij zijn transparant over hun gegevensverwerkingen en de manier waarop deze gegevens worden beschermd. Zij zorgen voor een goede balans tussen adequate bescherming van persoonsgegevens en processen om betrokkenen te bedienen. Met behulp van dit privacybeleid wil de gemeente richting maatschappij en betrokkenen kunnen verantwoorden en aantonen dat persoonsgegevens bij haar in goede handen zijn.

1.5 Reikwijdte

Dit privacybeleid is van toepassing op:

- De gehele organisatie.

- Alle mogelijke groepen betrokkenen waarvan de gemeente persoonsgegevens verwerkt, dus onder meer op inwoners en medewerkers.
- Alle processen waarbinnen persoonsgegevens worden verwerkt, waaronder processen die de gemeente Venlo uitbesteedt, inkoopt of op een andere manier organiseert.
- Alle ruimten en middelen die door gemeenteambtenaren intern en extern worden gebruikt bij de uitoefening van hun taak waar(op) persoonsgegevens worden verwerkt.
- Alle onderdelen, objecten en gegevensverzamelingen van de gemeente waarin de verwerking van persoonsgegevens een rol speelt.
- De hele verwerkingscyclus van persoonsgegevens, van het ontvangen, verzamelen en genereren, het dagelijks gebruik en de opslag/archivering tot en met de vernietiging daarvan.
- Informatiesystemen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is.
- Verwerkingen via alle soorten gegevensdragers, zowel digitaal als op papier.

1.6 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap. In dit verband worden met name genoemd:

Informatiebeveiliging

Privacy en informatiebeveiliging staan naast elkaar en zijn van elkaar afhankelijk. Informatieveiligheid is een randvoorwaarde voor eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. In het informatiebeveiligingsbeleid van de gemeente Venlo zijn uitgangspunten beschreven om de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatievoorzieningen en persoonsgegevens te waarborgen.

Archiefbeleid, managementinformatie, gegevensvernietiging

De verantwoordelijkheid voor de archivering binnen de gemeente Venlo is vastgelegd in de Archiefverordening gemeente Venlo 2017 en de Beheerregeling informatiehuishouding gemeente Venlo 2024. Deze voorschriften zijn gebaseerd op de Archiefwet. Hierin zijn tevens bepalingen opgenomen over vernietiging van gegevens en documenten. Privacywetgeving en – beleid en de Archiefwet en – beleid moeten in onderlinge samenhang bekeken worden. Bij de overbrenging conform de Archiefwet van gegevens en bescheiden naar de gemeentelijke archiefbewaarplaats dienen de privacywet- en regelgeving in acht te worden genomen.

Integriteit

Privacybewust werken en integer zijn raken elkaar. Integer zijn is niet voldoende om te voldoen aan privacywetgeving, maar veilig omgaan met persoonsgegevens vereist een integere houding. In het kader van integriteit leggen (nieuwe) medewerkers de eed of belofte af en hebben zij een geheimhoudingsplicht op grond van de Ambtenarenwet.

2 PRIVACYMANAGEMENT

In dit hoofdstuk wordt de wijze waarop privacymanagement is ingericht met de bijbehorende rollen en verantwoordelijkheden beschreven.

2.1 Context

De bescherming van persoonsgegevens is een breed werkterrein: het gaat hierbij bijvoorbeeld om het nemen van technische en organisatorische maatregelen, het maken van afspraken met partijen met wie informatie wordt gedeeld en om voorlichting aan betrokkenen over de verwerking van hun persoonsgegevens. De gehele organisatie is betrokken bij de verwerking van persoonsgegevens. Privacy dient geborgd te worden middels een vaste plek binnen het verantwoordelijke bestuursorgaan. Een goed privacymanagement vergt goede werkwijzen, geboden en verboden. Het vergt overzicht over de totale keten waarbinnen data van de organisatie rond gaan en het maken van afspraken waarbinnen dit gebeurt. De verwerking van persoonsgegevens moet worden gemonitord en er moet worden ingegrepen als contractpartners aan wie de verwerking is uitbesteed hun afspraken niet nakomen. Goed privacymanagement is geen absolute garantie dat er nooit een datalek of andere calamiteit zal ontstaan. Maar als het gebeurt, kan in ieder geval niemand het verwijt van onbehoorlijk en onrechtmatig bestuur gebruiken.

2.2 Rollen en verantwoordelijkheden binnen de gemeentelijke organisatie

Om daadwerkelijk te kunnen waarborgen dat de bescherming van persoonsgegevens ingebed wordt in de gemeentelijke organisatie is het noodzakelijk dat alle medewerkers die persoonsgegevens gebruiken dit op een zorgvuldige wijze doen en het proces beheerst wordt vanuit een centrale visie. In deze paragraaf wordt dit beschreven.

De bestuursorganen

De bestuursorganen van de gemeente Venlo zijn verantwoordelijk voor de naleving van privacywet- en regelgeving en het privacybeleid, ieder voor zover het hun bestuurlijke taken betreft. Zij zijn verantwoordelijk voor het verwerken van persoonsgegevens door de eigen organisatie en de aan externe organisaties gemandateerde taken. Voor zover de verwerking van persoonsgegevens gedelegeerd is aan externe organisaties die daarbij ook zelf doel en middelen kunnen bepalen, zijn de bestuursorganen van deze organisaties zelf verwerkingsverantwoordelijke in de zin van de AVG. De bestuursorganen

bevorderen de beschikbaarheid van voldoende middelen om de bescherming van persoonsgegevens passend te waarborgen.

Het college en de burgemeester leggen verantwoording af aan de raad over de status van de uitvoering van het privacybeleid en zullen binnen de jaarlijkse planning- en controlcyclus de gemeenteraad informeren over de risico's en over de getroffen beheersmaatregelen op het gebied van privacy. Het college en de burgemeester melden bijzonderheden ten aanzien van gegevensverwerkingen, te denken valt bijvoorbeeld aan ernstige datalekken, proactief aan de gemeenteraad.

Portefeuillehouder privacy binnen het college

Het college heeft de burgemeester als portefeuillehouder privacy aangewezen. Het college handhaaft haar privacybeleid op basis van afspraken over interne rekenschap zoals de planning- en controlcyclus. Het college neemt bij ontwikkeling van beleid, privacywet- en regelgeving en het privacybeleid in acht.

Directie

Het college belegt de nadere invulling van privacymanagement bij het directieteam. Het directieteam heeft de gemeentesecretaris als portefeuillehouder privacy op directieniveau aangewezen. Het directieteam is verantwoordelijk voor de integrale sturing van de ambtelijke organisatie op naleving van privacywet- en regelgeving en het privacybeleid. Daarmee is het directieteam ook verantwoordelijk voor het maken van keuzes met betrekking tot privacyrisico's en het eventueel accepteren van rest risico's. Zij legt verantwoording af aan het college over het gevoerde privacybeleid via de portefeuillehouder privacy. Privacy is een gespreksonderwerp in de verantwoordingsgesprekken tussen de directie en de hoofden.

Hoofden/proceseigenaren

Voor ieder primair of ondersteunend proces binnen gemeente Venlo is een hoofd/proceseigenaar aangewezen die zorgdraagt voor de vormgeving, uitvoering en monitoring van privacybeheersmaatregelen binnen zijn team en verwerkingsproces. Deze persoon is aanspreekbaar op het effectief waarborgen van privacy in dat proces en wint advies in bij de privacy officer alvorens aangevraagd wordt met een nieuwe of verdere verwerking van persoonsgegevens. Hoofden/proceseigenaren rapporteren over wat zij doen en wat de kwaliteit is van de uitvoering van het beleid aan de directie/portefeuillehouder. Daarnaast dienen zij de Functionaris Gegevensbescherming – gevraagd en ongevraagd – op de hoogte te brengen van relevante ontwikkelingen en of informatie voor wat betreft de realisatie van passende privacywaarborgen binnen hun processen. Ook nemen zij privacy als structureel onderdeel op in hun werkoverleggen. De organisatie werkt zo actief aan privacybewustzijn, het opbouwen van kennis bij medewerkers en aan een verantwoorde procesuitvoering.

Privacy officer

De privacy officer geeft invulling aan de centrale privacyfunctie voor de hele organisatie en is daarmee het eerste aanspreekpunt. De privacy officer ondersteunt en adviseert het management en de medewerkers van de gemeente Venlo bij de praktische invulling van het privacybeleid en privacywet- en regelgeving en het uitvoeren van privacyrisicomanagement. De privacy officer ontfermt zich over beleids- en planvorming.

(Chief) Information security officer ((C)ISO)

De Functionaris Gegevensbescherming en de privacy officer stemmen regelmatig af met de (C)ISO over de raakvlakken van informatieveiligheid en privacy binnen de gemeentelijke processen. De CISO ontfermt zich over strategische beleids- en planvorming en strategische en tactische advisering. De ISO geeft op operationeel niveau invulling aan de informatiebeveiligingsfunctie voor de gemeente Venlo.

Verbijzonderde Interne Controle (VIC)

De VIC ziet toe op het control proces in de eerste en tweede lijn en rapporteert hierover, in het kader van toezicht op bescherming van persoonsgegevens, aan de directie en aan de Functionaris Gegevensbescherming.

Medewerkers

Alle medewerkers (inclusief inhuur en externen) van de gemeente Venlo zijn ervoor verantwoordelijk dat zij bij de uitoefening van hun werkzaamheden conform het privacybeleid en op basis van de daarin beschreven beginselen en uitgangspunten (zie paragraaf 3.2) werken. Zij dienen zich hiervan bewust te zijn en dienen te voldoen aan hun geheimhoudingsverplichting. Zij hebben zo een belangrijke bijdrage aan de rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens binnen de gemeente.

Functionaris Gegevensbescherming (FG)

De bestuursorganen hebben een FG aangesteld als interne toezichthouder op de naleving van privacybeleid en privacywet- en regelgeving en als adviseur voor het management inzake privacyvraagstukken. De taken van deze functionaris zijn, kort samengevat, adviseren, toezicht houden en optreden als contactpersoon van de Autoriteit Persoonsgegevens. In het monitorings- en verantwoordingsplan is vastgelegd op welke wijze toezicht door de FG wordt vormgegeven. De FG treedt daarnaast op als adviseur voor de directie en de bestuursorganen op beleidsniveau. In aanvulling op de wettelijke bepalingen over de FG hebben de bestuursorganen een statuut voor de FG vastgesteld waarin de positie, de taken en de bevoegdheden van de FG vastgelegd zijn. Het statuut is geïncorporeerd in het organisatiebesluit.

3 PRIVACYBELEID GEMEENTE VENLO 2024

3.1 Algemeen

De bestuursorganen zijn verantwoordelijk voor het opstellen, uitvoeren en handhaven van een privacy-beleid.

De belangrijkste wettelijke kaders zijn:

- de Algemene verordening gegevensbescherming;
- de Uitvoeringswet Algemene verordening gegevensbescherming; en
- de Wet politiegegevens.

Het privacybeleid schept een algemeen kader voor de omgang met persoonsgegevens. Er zijn echter ook veel andere wetten die aanvullende eisen stellen aan de bescherming van persoonsgegevens, zoals de Wet Basisregistratie Personen, de Wet maatschappelijke ondersteuning 2015 en de Jeugdwet, maar ook het Besluit politiegegevens of de Regeling periodieke audit politiegegevens. De gemeente dient zich ook aan die aanvullende privacyregels te houden.

Hoofden/proceseigenaren geven, waar nodig, via separate regelgeving (denk bijvoorbeeld aan specifiek beleid voor HR, de uitvoering van de Jeugdwet of de interne procedure voor de boa's hoe zij om dienen te gaan met politiegegevens) nadere invulling aan het privacybeleid.

3.2 Taakstelling en uitgangspunten

Gemeente Venlo gaat op een zorgvuldige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Gelet op de visie, verwoord in paragraaf 1.4, hecht de organisatie waarde aan een goede balans tussen adequate bescherming van persoonsgegevens en praktische werkprocessen. De gemeente houdt zich hierbij aan de volgende uitgangspunten.

Rechtmatigheid en behoorlijkheid

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Transparantie

Het is belangrijk dat betrokkenen erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze persoonsgegevens worden verwerkt en beheerd. Denk bijvoorbeeld aan het verwerkingsregister, de privacyverklaring op de website van de gemeente en informatie die voor aanvang van een verwerking aan een betrokkene wordt verstrekt. In uitzonderingsgevallen kunnen de bestuursorganen besluiten om geen informatie over de verwerking van persoonsgegevens te verstrekken. Dit kan bijvoorbeeld het geval zijn bij kwesties van openbare orde en veiligheid, zoals bij het vervolgen, voorkomen en opsporen van een strafbaar feit.

Grondslag en doelbinding

Persoonsgegevens worden alleen verwerkt indien hiervoor een wettelijke grondslag bestaat. De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden vervolgens niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

Dataminimalisatie

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel.

Bewaartermijn (opslagbeperking)

Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Persoonsgegevens mogen echter niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze nodig zijn. De toepasselijke bewaartermijnen worden beschreven in verschillende wetten. Daar waar er geen wettelijke bepaling is die voorziet in een verplichte bewaartermijn, dient het college een eigen besluit over de bewaartermijn te nemen. Zoals toegelicht onder paragraaf 1.6 zal aan de hand van de Archiefwet en het archiefbeleid van de gemeente Venlo, in samenhang met privacywetgeving en – beleid, bekeken moeten worden hoe lang persoonsgegevens in een concreet geval bewaard mogen worden. De privacy officer en de gemeente archivaris adviseren in voorkomende gevallen.

Integriteit en vertrouwelijkheid

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Delen van gegevens

In bepaalde gevallen kan het nodig zijn dat persoonsgegevens gedeeld worden. Het delen van persoonsgegevens vindt alleen plaats als dit op grond van privacywetgeving toegestaan is. De gemeente maakt afspraken over de bescherming van persoonsgegevens met partijen waarmee gegevens worden gedeeld.

Subsidiariteit

Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk beperkt. Bij iedere verwerking wordt daarom

gecontroleerd of er een voor de betrokkene minder belastende manier vanuit privacy oogpunt is om de taak uit te voeren.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot een met de verwerking te dienen doel. Bij iedere verwerking wordt daarom gecontroleerd of er niet meer gegevens verwerkt worden dan noodzakelijk is voor het uitoefenen van de taak.

Privacy by design en privacy by default

De gemeente neemt bij de ontwikkeling van nieuwe diensten, systemen of processen aspecten van privacy en gegevensbescherming in acht om zo te komen tot een zo optimaal mogelijke bescherming van persoonsgegevens. Dit uitgangspunt wordt privacy by design genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente privacy by default als uitgangspunt: de standaardinstellingen zijn altijd zo privacyvriendelijk mogelijk.

4 INBEDDING BINNEN DE ORGANISATIE

4.1 Register van verwerkingen

De bestuursorganen zijn verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan zij de verwerkingsverantwoordelijke zijn. Het register beschrijft alle verwerkingen van persoonsgegevens binnen de gemeentelijke organisatie. Artikel 30 van de AVG en artikel 31d van de Wpg noemen de gegevens die tenminste in het register moeten staan.

Hoofden/proceseigenaren zijn verantwoordelijk voor het melden van nieuwe verwerkingen en relevante wijzigingen in bestaande verwerkingen, waarna deze in het register verwerkt worden. Voor het beheer van bestaande verwerkingen en registratie van nieuwe verwerkingen hanteert de gemeente een interne procedure.

4.2 Wijze van inrichten gegevensverwerking

De kwaliteit van de omgang met privacyvraagstukken wordt verhoogd door op verschillende niveaus en vanuit verschillende rollen de PDCA-cyclus te doorlopen. Door het cyclische karakter van de te nemen maatregelen en doordat privacy vast op de agenda van bestuur, management en lijnorganisatie is geplaatst, ontstaat een continu proces van veranderen en verbeteren.

4.3 Data protection impact assessment (DPIA)

Risico's worden onder andere bepaald aan de hand van DPIA's. Een DPIA brengt de effecten en risico's van nieuwe, gewijzigde of bestaande verwerkingen op de bescherming van persoonsgegevens in kaart. De gemeente is verplicht een DPIA uit te voeren als sprake is van een risicovolle verwerking van persoonsgegevens.

Gemeente Venlo heeft een DPIA procedure vastgesteld, waarin is vastgelegd op welke wijze een DPIA wordt uitgevoerd. Hierbij wordt ingegaan op de verwerkingen waarvoor een DPIA verplicht is en wie welke rol heeft binnen het proces. Daarnaast wordt in de procedure de wijze van vastlegging besproken. De monitoring van de maatregelen die voortvloeien uit de DPIA's vindt plaats middels een dashboard.

4.4 Datalekken

Datalekken zijn incidenten waarbij persoonsgegevens mogelijk verloren zijn gegaan, onrechtmatig zijn verwerkt of toegankelijk zijn geworden voor onbevoegden. Bij een datalek kan gedacht worden aan onbevoegde autorisaties in een informatiesysteem, het aan iemand toesturen van persoonsgegevens die niet voor de ontvanger zijn bestemd (brief of e-mail) of het zoekraken van een dossier. Ook het intern verwerken van persoonsgegevens door personen die hier niet bevoegd toe zijn vormt een datalek.

Indien een datalek of een vermoeden van een datalek zich voordoet, dient de gemeente snel en effectief te handelen. Naast de eigen verantwoordelijkheid die de gemeente Venlo als overheidsorgaan hierin heeft, is zij op grond van wetgeving verplicht een datalek zonder onredelijke vertraging, maar uiterlijk binnen 72 uur, te melden bij de Autoriteit Persoonsgegevens tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Een melding moet indien van toepassing ook onverwijld aan betrokkenen worden gedaan.

Gemeente Venlo heeft een procedure datalekken vastgesteld, met daarin nadere regels ten aanzien van de afhandeling datalekken. Daarnaast houdt gemeente Venlo een register voor datalekken bij.

4.5 Convenanten, geheimhoudingsverklaringen en privacy-afspraken

Met het oog op de bescherming van persoonsgegevens in gevallen waarin de gemeente samenwerkt met externe partners en waarbij een verwerking van persoonsgegevens plaatsvindt, worden convenanten, geheimhoudingsverklaringen en privacy-afspraken aangegaan. Hoofden/proceseigenaren dienen zorg te dragen voor het maken van deze afspraken en er voor te zorgen dat deze afspraken bevoegd worden vastgelegd. Hoe er afspraken worden gemaakt met externe partners is afhankelijk van de positie in de informatieketen en de aard van de samenwerking. De privacy officer ondersteunt hoofden/proceseigenaren hierin.

Het verlenen van opdrachten aan derden, verwerkers, brengt risico's met zich mee op het gebied van gegevensverwerking en informatieveiligheid. De bestuursorganen van de gemeente Venlo die derden opdracht geven persoonsgegevens namens hen te verwerken, blijven verantwoordelijk voor deze verwerking. Het aangaan van een verwerkersovereenkomst of een gegevensuitwisselingsovereenkomst

biedt de mogelijkheid om erop toe te zien en aan te tonen dat ook door verwerkers zorgvuldig omgegaan wordt met persoonsgegevens en een passende bescherming gewaarborgd is.

Om te borgen dat verwerkersovereenkomsten en gegevensuitwisselingsovereenkomsten worden aangegaan die voldoen aan wettelijke eisen gebruikt de gemeente een door het college vastgesteld model. Het aangaan van privacy-afspraken vormt, waar toepasselijk, bovendien vast onderdeel van het inkoopproces.

4.6 Bewustwording

Verantwoord en bewust gedrag van iedere medewerker die in aanraking komt met persoonsgegevens is essentieel om te kunnen waarborgen dat privacywet- en regelgeving en privacybeleid worden nageleefd. Het is van groot belang dat medewerkers die werken met persoonsgegevens weten wat er van hen verwacht wordt en hoe zij zorgvuldig om dienen te gaan met persoonsgegevens. Zij dienen over voldoende privacykennis te beschikken om in staat te zijn te beoordelen welke gegevens nodig zijn voor het uitvoeren van werkprocessen en in lijn met het privacybeleid te kunnen handelen.

Beleid en maatregelen alleen zijn niet voldoende om risico's op het gebied van de verwerking van persoonsgegevens uit te sluiten. Medewerkers worden daarom getraind in privacy-bewust handelen door middel van presentaties, workshops en trainingen en het altijd voorhanden hebben van een aanspreekpunt. Het doel is om de organisatie in zijn geheel op een "bewust bekwaam" niveau van omgaan met persoonsgegevens te brengen en houden. Om te borgen dat medewerkers doorlopend bewust gemaakt worden van de risico's en randvoorwaarden, waarmee rekening gehouden moet worden bij de verwerking van persoonsgegevens, wordt een privacy communicatieplan opgesteld.

4.7 Verantwoording

Eén van de belangrijkste verplichtingen voortvloeiende uit de AVG en de Wpg is de verantwoordingsplicht: de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de in privacywetgeving neergelegde eisen en kan aantonen dat hij hieraan voldoet (verantwoordingsplicht). Om hieraan te kunnen voldoen dient binnen de gemeentelijke organisatie sturing en monitoring plaats te vinden op naleving van privacywet- en regelgeving en privacybeleid. In het document "Monitoring en verantwoording in het kader van bescherming van persoonsgegevens" is vastgelegd hoe het college van burgemeester en wethouders en de directie hier invulling aan geven. De rol van de VIC is hierin ook vastgelegd. Er vindt extern en intern toezicht plaats op de wijze waarop de gemeente persoonsgegevens gebruikt. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de privacywet- en regelgeving in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de FG (zie paragraaf 2.2). De FG ziet erop toe dat de AVG en de Wpg intern worden nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

5 CONTACT MET BETROKKENEN

5.1 Rechten van betrokkenen

Om betrokkenen in staat te stellen controle uit te oefenen over hun eigen persoonsgegevens zijn in wetgeving diverse rechten neergelegd. De gemeente hecht eraan dat de procedures die waarborgen dat betrokkenen op effectieve wijze hun rechten uit kunnen oefenen op transparante wijze ingericht zijn.

Op grond van de AVG hebben betrokkenen de volgende rechten:

- Recht op informatie
- Recht op inzage
- Recht op rectificatie en aanvulling
- Recht op gegevenswissing of recht op vergetelheid
- Recht op beperking van de verwerking
- Recht van bezwaar
- Recht op overdraagbaarheid van gegevens of dataportabiliteit
- Recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit

Op grond van de Wpg hebben betrokkenen de volgende rechten:

- Recht op informatie
- Recht op inzage
- Recht op rectificatie en aanvulling
- Recht op vernietiging

Gemeente Venlo heeft een procedure rechten betrokkenen vastgesteld, met daarin nadere regels ten aanzien van de uitvoering van rechten van betrokkenen. In de privacyverklaring op de gemeentelijke website is een toelichting opgenomen over de betreffende procedure, zodat betrokkenen effectief hun rechten uit kunnen oefenen en weten hoe zij dit kunnen doen. Als het verzoek wordt afgewezen bestaat de mogelijkheid om bezwaar te maken bij de gemeente en om een klacht in te dienen bij de gemeente en/of de Autoriteit Persoonsgegevens. Hierover zal betrokkene geïnformeerd worden.

5.2 Klachten

In het contact met de gemeente kan wel eens wat misgaan. Een betrokkene kan zich onheus bejegend voelen. Dan is het goed om te weten, dat ieder op grond van de Algemene wet bestuursrecht (Awb) het recht heeft een klacht in te dienen over de wijze waarop een gemeentelijk bestuursorgaan of iemand die in dienst van de gemeente werkzaam is, zich jegens hem of een ander heeft gedragen.

Hoofdstuk 9 van de Awb regelt de behandeling c.q. het buiten behandeling laten van klachten. In aanvulling daarop kan er een klachtenregeling zijn. De klachtenregeling binnen de gemeente Venlo is vastgelegd in de Verordening interne klachtadviescommissie 2010. Deze verordening is terug te vinden op www.overheid.nl onder lokale wet- en regelgeving.

Indien de klachtenprocedure in relatie staat tot de verwerking van persoonsgegevens zal de behandelend ambtenaar van de klachtadviescommissie afstemming zoeken met de FG.

6 MOGELIJKE AFWIJKINGEN VAN BELEID

De burgemeester en de gemeentesecretaris kunnen beargumenteerd van het privacybeleid afwijken op basis van een belangenafweging. Zij laten zich daarbij adviseren door de FG.

7 BEHEER EN ONDERHOUD

Er bestaat niet alleen een wettelijke verplichting om een passend gegevensbeschermingsbeleid te hebben en uit te voeren, maar ook om dit beleid te evalueren en waar nodig te actualiseren.

De privacy officer is in de uitvoerende zin eigenaar van het privacybeleid en daarmee verantwoordelijk voor het beheer en onderhoud ervan.

Het privacybeleid wordt na verloop van drie jaar geëvalueerd, waarbij in ieder geval de volgende aspecten beoordeeld zullen worden: inhoud, uitvoerbaarheid, invoering en werking. De FG wordt geïnformeerd op basis van deze evaluatie. Indien daartoe aanleiding bestaat wordt het privacybeleid geactualiseerd.

Aldus vastgesteld in de openbare raadsvergadering van 02 april 2025.

De griffier, De voorzitter

Etienne Franken, Antoin Scholten