

Privacybeleid 2025-2028 gemeente Laarbeek

Besluit

Vaststellen privacybeleid 2025-2028 gemeente Laarbeek.

1. Privacy algemeen

1.1 Algemeen

Iedereen heeft recht op privacy. Het is geregeld in de Grondwet en gaat over de rechten en persoonlijke vrijheden van eenieder. Lichamelijke integriteit, het huisrecht, het briefgeheim en informatieprivacy vallen allemaal onder dat begrip. De essentie van privacy is dat informatie over ons doen en laten binnen de oorspronkelijke context blijft én dat organisaties transparant zijn over hoe zij omgaan met persoonsgegevens.

Dit privacy beleid richt zich op de informatieprivacy en beschrijft de wijze waarop gemeente Laarbeek omgaat met persoonsgegevens en hoe zij in dat verband het recht van burgers om zelf te beschikken over de eigen persoonsgegevens borgt. Medewerkers, burgers, leveranciers en andere externe partijen van de gemeente weten op deze wijze welke uitgangspunten gelden en wat er van hen verwacht wordt ten aanzien van privacy en het verwerken van (bijzondere) persoonsgegevens. Daarnaast vormt dit privacy beleid een kapstok waaraan processen, procedures en/of werkafspraken worden opgehangen die gelden voor specifieke activiteiten en werkzaamheden waarbinnen persoonsgegevens worden verwerkt.

De gemeente hecht waarde aan een adequate wijze van dienstverlening en samenwerking met een daarop ingerichte efficiënte verwerking van persoonsgegevens, maar vindt het eveneens van groot belang dat de privacy van burgers wordt gerespecteerd. De burgers moeten erop kunnen vertrouwen dat de gemeente en haar partners de privacywetgeving in acht neemt en zorgvuldig omgaat met persoonsgegevens zodat de privacybescherming geborgd is.

Vanaf 25 mei 2018 beschermen alle landen in de Europese Unie de persoonsgegevens volgens dezelfde algemene regels van de Algemene Verordening Gegevensbescherming (AVG). Het doel van de AVG is:

- Het beschermen van natuurlijke personen in verband met de verwerking van hun gegevens.
- Het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.
- De AVG versterkt de grondrechten van de burgers in het toenemende digitale tijdperk.

Dit privacy beleid gaat in op de verplichtingen die de AVG stelt aan gemeente Laarbeek.

Dit privacy beleid is geldig voor vier jaar (2025-2028). Het beleid wordt om de vier jaar vierjaarlijks geëvalueerd en eventueel geactualiseerd of bijgesteld in het geval van een wetswijziging of groei van de organisatie en/of ambitie.

1.2 Reikwijdte privacy

Het gemeentelijk privacy beleid is van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is.

Het privacy beleid heeft betrekking op de persoonsgegevens van personen van wie gemeente Laarbeek gegevens verwerkt of laat verwerken.

Er is al snel sprake van 'verwerken' van persoonsgegevens. Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van persoonsgegevens valt allemaal onder het verwerken van persoonsgegevens.

1.3 Juridisch kader

De Europese Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) gelden als wettelijke kaders voor de omgang met persoonsgegevens. Naast de AVG moet elke EU-lidstaat op een aantal punten onder de AVG nog wetgeving maken. In Nederland is dit voor een belangrijk deel gebeurd in de Uitvoeringswet algemene verordening gegevensbescherming.

Wanneer persoonsgegevens worden verwerkt in het kader van de uitvoering van een politietaken, zijn dit politiegegevens. Ook deze gegevens worden door de gemeente verwerkt. Het wettelijke kader voor de omgang met politiegegevens is de Wet politiegegevens (Wpg) en het Besluit politiegegevens Boa's (Bpg Boa).

Gemeente Laarbeek voert publiekrechtelijke taken uit. Deze taken vloeien voort uit vele sectorwetten. Denk hierbij onder andere aan de wet Maatschappelijke Ondersteuning 2015, de Jeugdwet en de wet Basisregistratie Persoonsgegevens. In de sectorwet kan beschreven staan hoe met persoonsgegevens moet worden omgegaan. Dit is een aanvulling op de normen die in de AVG staan beschreven. Gemeente Laarbeek voert ook privaatrechtelijke taken uit. Hiervoor geldt naast de AVG ook de algemene wet- en regelgeving.

Voor de Buitengewoon Opsporingsambtenaren (boa's) gelden twee verschillende privacy regimes: de AVG en de Wet politiegegevens (Wpg). Boa's hebben vaak meerdere taken en verwerken verschillende soorten persoonsgegevens. De persoonsgegevens die een boa verwerkt in zijn rol als toezichthouder vallen onder de AVG. Persoonsgegevens die de boa verwerkt in zijn rol als opsporingsambtenaar vallen onder de Wpg. Voor persoonsgegevens welke onder de Wpg worden verwerkt, gelden o.a. andere verwerkingstermijnen en andere regels voor het delen van gegevens in vergelijking met de AVG. De gegevenshuishouding, systemen en werkprocessen zullen anders moeten worden ingericht dan bij de verwerkingen welke in het kader van toezicht (AVG) worden gedaan. Tevens kent de Wpg een auditplicht. Eén keer per jaar dient er een interne audit plaats te vinden en één keer in de vier jaar een externe audit. Het externe auditrapport dient gedeeld te worden met de Autoriteit Persoonsgegevens; de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

Gemeente Laarbeek heeft boa's in dienst die verwerkingen uitvoeren welke onder het regime van de Wpg vallen. Daarom dient gemeente Laarbeek ervoor te zorgen dat de gegevenshuishouding, systemen en werkprocessen die van toepassing zijn op de werkzaamheden van boa's voldoen aan de normen van de Wpg.

1.4 Privacy missie en ambitie

Zorgvuldig omgaan met persoonsgegevens is de regel voor alle medewerkers van gemeente Laarbeek. De gemeente heeft de volgende missie en ambitie op het gebied van privacy:

Missie: Gemeente Laarbeek ziet 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. Wij werken daarom conform de regels van de AVG.

Hoe doen we dat?

Visie & ambitie: Gemeente Laarbeek zoekt bij de uitvoering van taken waarbij persoonsgegevens worden verwerkt altijd naar balans tussen de werkbaarheid voor de medewerkers en haar samenwerkende partijen en de risico's voor de inwoners van de gemeente. Gemeente Laarbeek streeft ernaar om eind 2028 op alle privacy-thema's genoemd in het AVG-borgingsproduct 3.0 van de Vereniging Nederlandse Gemeenten (VNG) te voldoen.

Dit privacy beleidskader draagt bij aan onze missie, visie en ambitie door het bieden van de noodzakelijke randvoorwaarden voor een privacy bestendige gemeentelijke bedrijfsvoering. Het college van burgemeester en wethouders (hierna: college) stelt de voorwaarden voor een privacy bewuste organisatiecultuur. We zijn transparant over onze gegevensverwerking en de manier waarop wij persoonsgegevens beschermen. Bij meningsverschillen gaan wij het gesprek met betrokkenen (onze inwoners) aan en zoeken we naar oplossingen.

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties ook voor gemeenten steeds belangrijker. Uitval van computers, het zoekraken van gegevensbestanden of het door onbevoegden kennisnemen dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de voortgang van de dienstverlening. Ook kan er imagoschade uit voortkomen.

Een betrouwbare, beschikbare en correcte informatiehuishouding is dan ook essentieel voor de privacy van onze inwoners én de dienstverlening van de gemeente.

2. Privacy beleidskader

2.1 Doelstelling

Het doel van dit privacy beleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen waarvan de gemeente Laarbeek persoonsgegevens verwerkt, en daarnaast te beschrijven waar de gemeente Laarbeek naartoe wil groeien op het gebied van de naleving van de (U)AVG.

Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van de gemeente en de privacy van onze inwoners. Dit privacy beleidskader draagt hieraan bij door het bieden van de noodzakelijke randvoorwaarden voor een privacy bestendige gemeentelijke bedrijfsvoering.

2.2 Uitgangspunten

Op grond van artikel 5 AVG is de gemeente Laarbeek verplicht de AVG-beginselen in acht te nemen bij het verwerken van persoonsgegevens. Hieronder worden deze uitgangspunten beschreven:

a. Rechtmatigheid, behoorlijkheid, transparantie

Een verwerking is alleen rechtmatig indien en voor zover aan de voorwaarden is voldaan zoals opgenomen in de AVG, te weten:

- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking;
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was;
- Om een verplichting na te komen die in de wet staat;
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden;
- Voor de goede invulling van de gemeentelijke taak;
- Indien een zorgvuldige belangenafweging dit uitwijst.

Gemeente Laarbeek verwerkt persoonsgegevens zoveel als mogelijk vanuit de publieke taak welke zij heeft op grond van aan haar opgelegde taken. Gemeente Laarbeek verwerkt ook persoonsgegevens wanneer de wet haar daartoe verplicht.

b. Grondslag en doelbinding

De gemeente zorgt ervoor dat persoonsgegevens alleen voor specifiek en uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Wanneer gegevens later voor een ander doel worden gebruikt, dan moet dit nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel. Persoonsgegevens worden alleen met een rechtvaardige grondslag en in overeenstemming met wet- en regelgeving verwerkt.

c. Dataminimalisatie

De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

In bepaalde wet- en regelgeving is vastgelegd welke persoonsgegevens noodzakelijk zijn om het doel te bereiken. Wanneer dit niet het geval is, maakt gemeente Laarbeek zelf deze afweging in overleg met de Privacy Officer en Functionaris Gegevensbescherming.

d. Dataminimalisatie & Opslagbeperking

Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Er dient te worden gezorgd dat de bewaartermijn van persoonsgegevens tot een strikt minimum wordt beperkt. Wanneer er persoonsgegevens opgeslagen zijn die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld, moeten deze zo snel mogelijk worden vernietigd. Dit houdt in dat deze persoonsgegevens worden verwijderd óf zo worden aangepast dat de gegevens niet langer herleidbaar zijn naar een natuurlijke persoon.

Hoe lang de gemeente persoonsgegevens bewaart varieert. De Archiefwet, de Selectielijst van de Vereniging Nederlandse Gemeenten (VNG) en diverse andere wetten bepalen dat de gemeente persoonsgegevens voor een minimale of maximale termijn mogen of moeten bewaren.

In het Register van verwerkingsactiviteiten is de gehanteerde bewaartermijn opgenomen.

e. Integriteit en vertrouwelijkheid

De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Daarbij zorgt de gemeente voor passende beveiliging van persoonsgegevens. In de Baseline Informatiebeveiliging Overheid (BIO) staan de verplichte voorwaarden voor gemeenten om te voldoen aan het begrip passende beveiliging. In het Informatiebeveiligingsbeleid van gemeente Laarbeek wordt hier verder invulling aan gegeven.

3. Privacy management

Privacy management omvat alle maatregelen die ervoor zorgen dat de gemeente zich houdt aan de AVG-wetgeving en daarover verantwoording aflegt. Hiermee geeft de gemeente Laarbeek invulling aan de verantwoordingsplicht vanuit de AVG. De essentie van de verantwoordingsplicht is dat het verantwoordelijke bestuursorgaan, de 'verwerkingsverantwoordelijke', verantwoordelijk is voor het naleven van de AVG, en dit tevens aantoonbaar kan maken

In dit hoofdstuk wordt uiteengezet wie in de organisatie welke verantwoordelijkheden en taken heeft ten aanzien van de naleving van de AVG.

3.1 Rollen en verantwoordelijkheden

Alle bestuursorganen van de gemeente zijn verantwoordelijk voor de naleving van de privacywet- en regelgeving, zoals de AVG en het privacy beleid, ieder voor zover het haar bestuurlijke taken betreft. De bestuursorganen van de gemeente zijn de gemeenteraad, het college van burgemeester en wethouders (het college van B&W) en de burgemeester.

Het college is eindverantwoordelijk voor de naleving van privacywetgeving met de burgemeester als portefeuillehouder. De gemeentesecretaris en het lijnmanagement hebben de ambtelijke verantwoordelijkheid om een proactief privacy beleid te voeren op basis van afweging van belangen en risico's bij de verwerking van persoonsgegevens zodat dit evenwichtig plaatsvindt. Dat wil zeggen; behoorlijk, zorgvuldig en in overeenstemming met de wet.

Het college legt over de uitvoering van het privacy beleid verantwoording af aan de gemeenteraad. Het college zorgt ook voor een zodanige documentatie van beleid en maatregelen dat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak. Onderstaande tabel brengt de verantwoordelijkheden in beeld aan de hand van het RASCI-model:

Om daadwerkelijk te kunnen waarborgen dat privacybescherming ingebed wordt in de organisatie is het noodzakelijk dat alle in de organisatie werkzame personen (inclusief inhuur en externen), ieder vanuit hun rol worden gezien. Hieronder worden deze verschillende rollen en verantwoordelijkheden om uitvoering te geven aan dit privacy beleid kort uiteengezet.

Om rollen en verantwoordelijkheden van de personen bij lijnwerkzaamheden inzichtelijk te maken, hanteert de gemeente Laarbeek de RASCI-methode. Onderstaand is het RASCI-model privacy rollen opgenomen.

Verantwoordelijkheid	Rol	Functionies
Responsible	Ambtelijk verantwoordelijk	<u>1^e lijn</u> - Directie (gemeentesecretaris) - Managementteam (MT) - Afdelingshoofd - Alle medewerkers (inclusief inhuur/externen)
Accountable	Eindverantwoordelijk	<u>1^e lijn</u> - College van B&W (Bestuurlijk) - Gemeentesecretaris (Ambtelijk)
Supporting	Ondersteunend	<u>2^e lijn</u> - Privacy Officer (privacy adviseur) - Chief Information Security Officer - Informatieadviseurs - Juristen
Consulted	Controlerend	<u>3^e lijn</u> - Functionaris Gegevensbescherming - IT-auditor - Controller - Accountant

Informed	Geïnformeerd	Belanghebbenden - Gemeenteraad (bestuurlijke toezichttaak) - Betrokkene(n) - Autoriteit Persoonsgegevens
----------	--------------	---

3.2 Managementstructuur

Het college van B&W

- Is bestuurlijk eindverantwoordelijk voor de naleving van de privacywetgeving
- Stelt beleid vast voor de bescherming van de privacy op basis van wet-en regelgeving
- Legt over de privacy beleidsuitvoering verantwoording af aan de raad
- Wijst de Functionaris gegevensbescherming als interne toezichthouder aan

De gemeenteraad

- Heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan hen toekent, en controleert in die hoedanigheid de uitvoering van het privacy beleid door het college.

De burgemeester

- Is portefeuillehouder voor de uitvoering van de privacywetgeving binnen de gemeente

De gemeentesecretaris

- Is ambtelijk eindverantwoordelijk voor privacy
- Is verantwoordelijk voor de juiste implementatie van privacy in de bedrijfsprocessen en (informatie)systemen

Management Team

- Is operationeel verantwoordelijk voor een juiste implementatie en naleving van privacy in processen, (informatie)systemen en projecten. Zij wijzen voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan
- Zorgt ervoor dat het privacy bewustzijn binnen de organisatie wordt bevorderd
- Stuurt op organisatie- en privacy risico's
- Zorgt ervoor dat budget wordt vrijgemaakt om aan de naleving van de AVG te kunnen voldoen
- Evalueert periodiek het privacy beleid en stelt eventueel bij

De medewerkers

Elke medewerker, inclusief externen, is verantwoordelijk voor de bescherming van de privacy van betrokkene(n). Dat betekent dat iedereen onder andere zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens op operationeel vlak.

Medewerkers zorgen ervoor dat:

- Ze bewust bezig zijn met het onderwerp privacy binnen het dagelijks werk;
- Ze op de hoogte zijn waar ze terecht kunnen met vragen omtrent privacy;
- Ze datalekken tijdig melden;
- Ze de communicatiekanalen en -middelen gebruiken die door de gemeente Laarbeek worden voorgeschreven;
- Ze werken vanuit het zaaksysteem en andere daarvoor ingerichte systemen, welke afdeling ICT beschikbaar heeft gesteld. Opslag van officiële documenten of documenten met persoonsgegevens op andere plaatsen is niet toegestaan.

3.3 Proceseigenaarschap

Het management is er verantwoordelijk voor dat de gemeentelijke taakuitoefening binnen de grenzen van dit privacy beleidskader plaatsvindt en rapporteert hierover aan de directie die op haar beurt rapporteert aan het college. Het college legt verantwoording af aan de gemeenteraad.

Een manager is proceseigenaar. Proceseigenaren voeren regie over hun proces(sen) op basis van procesplannen die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een procesplan dient te passen binnen dit privacy beleidskader en is steeds in overeenstemming met de feitelijke situatie.

Bij afdeling overstijgende processen kan een coördinerend manager of een andere functionaris worden aangewezen.

De 'verwerkingsverantwoordelijke' in de zin van de AVG, in de meeste gevallen het college, is en blijft eindverantwoordelijk voor de privacy bestendigheid van de gemeentelijke processen.

3.4 Organisatie

Privacy Officer

De Privacy Officer (PO) geeft uitvoering aan het privacy beleid van de gemeente. Door het aanstellen van de PO wordt in de organisatie geborgd dat de wettelijke privacy taken worden uitgevoerd. De PO is het eerste aanspreekpunt bij vragen voor alle collega's ten aanzien van privacy. De PO dient bij alle processen waar persoonsgegevens worden verwerkt betrokken te worden door de organisatie.

Taken

De taken van de PO zijn:

- Adviseur binnen de gemeente met betrekking tot privacy gerelateerde vragen
- Het eerste aanspreekpunt op het gebied van privacy door medewerkers
- Stelt beleidsdocumenten op, zoals het privacy beleid, de privacyverklaring(en), verwerkingsregister, procedures rondom bijvoorbeeld datalekken en DPIA's
- Zorgt ervoor dat deze documenten periodiek worden geactualiseerd
- Ondersteunt en voert acties uit welke bijdragen aan privacy bewustwording binnen de gemeente
- Reageert op datalekken en zet deze door naar de functionaris gegevensbescherming
- Coördineert en ondersteunt bij de uitvoer van DPIA's
- Rapporteert rechtstreeks aan het management en het college
- Is het centrale aanspreekpunt voor de implementatie van de Wpg

Door de functies advies (PO) en controle (FG) te scheiden wordt voorkomen dat de FG haar eigen werk controleert. Dit bevordert de kwaliteit en integriteit.

De Chief Information Security Officer

De Chief Information Security Officer (CISO) ondersteunt, coördineert en adviseert de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. Dit doet hij vanuit een onafhankelijke positie. De CISO rapporteert rechtstreeks aan de gemeentesecretaris.

Taken

De taken van de CISO zijn:

- Het opstellen, implementeren, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen
- Het optreden als informatiebeveiligingsadviseur voor de proceseigenaar op managementniveau
- Het inrichten van de informatiebeveiligingsorganisatie
- Het coördineren en adviseren bij afhandelen van beveiligingsincidenten
- De afstemming van informatiebeveiliging met andere beveiligingsdomeinen
- Het toezien op naleving van de eisen voor informatiebeveiliging
- Het bevorderen van het informatiebeveiligingsbewustzijn over de gemeente
- De voorbereiding op toekomstige informatiebeveiligingsrisico's en ICT-beveiligingsrisico's
- Het adviseren bij en begeleiden van risicoanalyses
- Het meten van en rapporteren over informatiebeveiliging, door het initiëren of laten uitvoeren van (periodieke) beveiligingsaudits en evaluaties

De Functionaris Gegevensbescherming

De Functionaris Gegevensbescherming (FG) heeft een onafhankelijke positie binnen de organisatie. De FG is in ieder geval verantwoordelijk voor het houden van toezicht op en adviseren van de organisatie over de juiste en zorgvuldige omgang met persoonsgegevens. Dit betekent dat de FG bij alle processen waar persoonsgegevens worden verwerkt betrokken moet worden door de organisatie.

Taken

De FG heeft de volgende taken:

- Informeren en adviseren over privacywetgeving voor afdelingsspecifieke zaken kan rechtstreeks het betreffende DT/MT lid benaderd worden
- Toezien op de naleving van de AVG en het privacy beleid van de organisatie;
Rapporteert rechtstreeks aan de algemeen directeur/gemeentesecretaris;
In geval van crisis of ernstige gebreken mag de FG direct aan de portefeuillehouder privacy en het college rapporteren
- Zorgen voor bewustwording
- Adviseren over DPIA's, en toezien op de uitvoering daarvan;
- Samenwerken met en optreden als contactpunt voor de AP; en
- Zorgen voor de waarborging van privacy van de medewerkers
- De FG werkt nauw samen met de PO en de CISO.

Onafhankelijkheid

De FG kan vrij en onafhankelijk advies uitbrengen. Zij mag geen instructies ontvangen over de behandeling van een zaak, of op andere wijze worden beïnvloed. De FG kan geen bindend advies geven, maar zijn advies is wel zwaarwegend. De FG wordt de gelegenheid geboden om een (eventuele) afwijkende mening duidelijk te maken aan het college en er wordt vastgelegd waarom een advies niet wordt opgevolgd. De FG kan rechtstreeks aan het college rapporteren. Bovendien krijgt de FG geen andere taken of plichten opgelegd die kunnen leiden tot een belangenconflict. Tevens behoudt de FG het recht om rechtstreeks contact op te nemen met de AP wanneer haar advies herhaaldelijk niet wordt gehoord / opgevolgd binnen de organisatie.

De FG doet jaarlijks verslag van haar bevindingen ten aanzien van naleving van de AVG met daarbij adviezen om dit te verbeteren. De raad wordt via de planning en control cyclus geïnformeerd.

4. Inbedding in de organisatie

De volgende maatregelen zijn intern getroffen om de privacy in te bedden in de organisatie en daarmee de privacy te kunnen waarborgen:

Informatieplicht

Betrokkenen krijgen vooraf duidelijke informatie via de privacyverklaring op de website en de dienstverlening welke zij mogen verwachten (telefonisch, schriftelijk) over de verwerking van hun persoonsgegevens en het doel van de verwerking.

Bewustwording

Bewustwording op het gebied van privacy is essentieel voor het borgen van privacy in de organisatie. Er wordt doorlopend aandacht geschonken aan de bewustwording van privacy in de gemeente, o.a. door periodieke trainingen.

Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten bevat alle verwerkingsactiviteiten van persoonsgegevens welke voor de gemeente wordt bijgehouden.

Data Protection Impact Assessment

Bij de invoering van een nieuw beleid of regelgeving of bij het gebruik van nieuwe technologieën houdt de gemeente rekening met de bescherming van persoonsgegevens door een DPIA uit te voeren.

De DPIA wordt opgesteld met als doel de privacy risico's op hoog risicoverwerkingen te mitigeren tot een minimum.

Datalekken melden

Er is een procedure binnen de gemeenten voor het melden van incidenten en datalekken. Deze meldingen verlopen via het ticketsysteem. Er wordt een register bijgehouden van de gemelde beveiligingsincidenten/datalekken.

Toezichtrapportage en evaluatie

Periodiek wordt gecontroleerd of het beleid en de dagelijkse praktijk overeenkomen. In samenspraak met de Privacy Officer wordt bepaald of een privacy-audit wordt uitgevoerd in aanvulling op het toezicht door de FG.

Jaarlijks legt het college in de verantwoording af aan de raad waar het gaat over risico's en beheersmaatregelen met betrekking tot het privacy beleid. Het privacy beleid wordt na vier jaar geëvalueerd, of indien nodig bij een interne wijziging of veranderende wet-en regelgeving.

4.1 Uitwisseling met derden

Bij de uitvoering van haar gemeentelijke taken werkt gemeente Laarbeek veel samen met externe partijen zoals andere gemeenten, overheden, gemeenschappelijke regelingen, softwareleveranciers en adviesbureaus 's. Met het oog op de bescherming van de persoonsgegevens maakt de organisatie afspraken met deze externe partijen over de omgang met privacy.

Voor zover de samenwerkingspartners worden aangemerkt als verwerkende partij sluit de gemeente met deze partij een zogeheten verwerkersovereenkomst. In de verwerkersovereenkomst worden afspraken gemaakt over het waarborgen van privacy verplichtingen en beveiliging van persoonsgegevens. Wanneer samenwerkingspartners worden aangemerkt als verwerkingsverantwoordelijke worden de afspraken over de omgang met persoonsgegevens vastgelegd in een overeenkomst inzake persoonsgegevens, algemene inkoopvoorwaarden, bestaande samenwerkingsovereenkomsten, convenanten, gemeenschappelijke regelingen etc. De privacy officer ziet toe op de naleving van de gemaakte afspraken.

4.2 Privacy by design & Privacy by default

Gemeente Laarbeek hanteert de principes 'privacy by design' en 'privacy by default' bij haar verwerkingen.

'Privacy by design' houdt in dat de bescherming van persoonsgegevens bij de ontwikkeling van producten, procedures en diensten waarbij persoonsgegevens worden verwerkt, wordt meegenomen en ingebouwd.

'Privacy by default' houdt in dat de standaardinstellingen bij de inrichting van systemen zodanig zijn gekozen dat de bescherming van persoonsgegevens wordt gewaarborgd. Dit houdt in dat waar dit mogelijk is niet méér persoonsgegevens worden gedeeld/getoond dan noodzakelijk voor de uitoefening van de taak.

Borging van deze principes dient onder andere plaats te vinden in het inkoopproces en het wijzigingsbeheer van systemen. We hebben hier een gemeenschappelijke aanpak voor nodig tussen de afdelingen, informatievoorziening en Informatiebeveiliging en Privacy. Op deze werkwijze worden eventuele (privacy-) risico's tijdig gemitigeerd.

5. Privacyrechten van betrokkenen

5.1 Rechten

De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken maar ook de rechten van personen van wie de gegevens worden verwerkt. Deze betrokkenen hebben de volgende rechten:

- Recht op informatie: betrokkenen hebben het recht om te weten wat er met hun persoonsgegevens gebeurt en waarom;
- Inzagerecht: betrokkenen hebben het recht om de persoonsgegevens die van hem verzameld zijn in te zien en daarmee te controleren op welke manier die gegevens verwerkt worden;
- Correctierecht: betrokkenen hebben het recht om foutieve persoonsgegevens te laten corrigeren als blijkt dat deze niet kloppen;
- Recht van verzet: betrokkenen kunnen in bepaalde gevallen de gemeente vragen (tijdelijk) te stoppen met het verwerken of wijzigen van zijn persoonsgegevens;
- Recht om vergeten te worden: in gevallen dat toestemming is gegeven om gegevens te verwerken, kan verzocht worden om die gegevens te laten verwijderen;
- Recht op bezwaar: het recht om bezwaar te maken tegen de verwerking van zijn/haar gegevens. De gemeente zal hieraan voldoen tenzij er gerechtvaardigde gronden zijn voor de verwerking.
- Recht om gegevens over te dragen (dataportabiliteit): het recht om persoonsgegevens in bepaalde gevallen over te dragen;
- Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming: het recht op een menselijke blik bij besluiten.

Om gebruik te maken van zijn/haar rechten kan het betrokkene schriftelijk, via een e-mail of via de website van de gemeente een verzoek indienen. Identificatie van de betrokkene vindt plaats bij het indienen van een verzoek aan de balie van het gemeentehuis in persoon. De gemeente beoordeelt binnen een maand of het verzoek gerechtvaardigd is. Indien dat het geval is, dient de gemeente in diezelfde maand het verzoek in te willigen.

5.2 Verzoeken en bezwaren

Verzoeken met betrekking tot bovenstaande rechten en bezwaren kunnen schriftelijk en digitaal worden ingediend bij de FG via het e-mailadres fg@laarbeek.nl. Deze verzoeken worden geregistreerd en de afhandeling ervan wordt verantwoord.

het college van burgemeester en wethouders,

*gemeentesecretaris van Laarbeek,
J.W.M. van de Ven*

*de burgemeester van Laarbeek,
L.A.G.P. van der Aa*