Gemeente Heerde

cittaslow

2018

Privacybeleid gemeente Heerde

www.heerde.nl

INHOUD

Management samenvatting

De gemeente Heerde verzamelt en verwerkt persoonsgegevens in verband met de dienstverlening aan burgers en bedrijven. Het beschermen van de persoonlijke levenssfeer van onze inwoners vinden wij van groot belang. Privacy en het delen en openbaar maken van privacygevoelige informatie willen we dan ook goed regelen in de gemeente Heerde. In de maatschappij is privacy een onderwerp dat veel in de belangstelling staat.

Bij het verwerken van persoonsgegevens worden de volgende uitgangspunten in acht genomen:

1. Gegevens van burgers worden binnen de kaders van de geldende wet- en regelgeving en op behoorlijke en zorgvuldige wijze verwerkt.
2. De inbreuk op de eerbiediging van de persoonlijke levenssfeer van de burger wordt zoveel mogelijk beperkt (subsidiariteit).
3. De inbreuk op de belangen van de burger mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel (proportionaliteit).
4. Gegevens worden enkel gebruikt voor het met de verwerking te dienen doel en kunnen alleen worden gebruikt voor andere doelen of worden gedeeld voor zover de wet dat toestaat. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
5. Persoonsgegevens worden niet langer bewaard dan noodzakelijk.
6. In geval van samenwerking met derden, dan wel verstrekking van persoonsgegevens aan derden, worden afspraken gemaakt over de eisen en voorwaarden waar gegevensuitwisseling aan moet voldoen.
7. De burger wordt op een transparante wijze geïnformeerd over de verwerking van persoonsgegevens door de gemeente. De gemeente geeft in voorkomend geval gehoor aan inzage- en/of correctieverzoeken, dan wel verwijderingsverzoeken. Afhandeling van deze verzoeken gebeurt op een laagdrempelige, toegankelijke wijze.
8. De gemeente borgt middels technische en organisatorische maatregelen dat onbevoegde toegang en onbevoegd gebruik van gegevens wordt voorkomen.
9. Bij aanschaf, inrichting of ontwikkeling van producten of diensten houdt de gemeente rekening met de eerbiediging van de persoonlijke levenssfeer van burgers.
10. Beveiligingsincidenten waar potentieel persoonsgegevens bij betrokken zijn worden direct gemeld bij het datalekteam.

Inleiding

De gemeente Heerde verwerkt persoonsgegevens voor de goede uitvoering van haar publiekrechtelijke taken en in het kader van de bedrijfsvoering. De gemeente verzamelt en verwerkt persoonsgegevens voor de dienstverlening aan inwoners en bedrijven. Als gevolg van de decentralisaties van de Jeugdwet, Wmo 2015 en de Participatiewet beschikt de gemeente Heerde over nieuwe klantgroepen en dus nieuwe (bijzondere) persoonsgegevens. De beschikking over deze gegevens vormt een nieuwe belangrijke verantwoordelijkheid. Daarnaast zal de gemeente door deze taakuitbreiding vaker persoonsgegevens willen uitwisselen met andere instanties. De complexiteit van de bescherming van de persoonlijke levenssfeer van inwoners van de gemeente is hiermee toegenomen.

De gemeente vindt het belangrijk dat inwoners kunnen vertrouwen op een veilige verwerking van persoonsgegevens. Bescherming van persoonsgegevens is immers een grondrecht. Burgers hebben er recht op dat persoonsgegevens op een rechtmatige manier worden verwerkt. Uitgangspunt is dat de gemeente zorgvuldig en veilig, proportioneel en vertrouwelijk omgaat met persoonsgegevens. Een zorgvuldige omgang met de gegevens van burgers is van groot belang voor het vertrouwen van burgers in de overheid. De gemeente geeft met dit algemene privacybeleid verdere invulling aan de verplichtingen en bevoegdheden die uit de privacywetgeving voortvloeit. De Algemene Verordening Gegevensbescherming (AVG) en andere bij specifieke wet geregelde privacyregimes vormen het formele kader van de gemeente Heerde.

Reikwijdte

Het algemeen privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die binnen de gemeente plaatsvinden. Dit algemeen privacybeleid vormt een verdere uitwerking van de wettelijke regelgevingen en dient als een praktische handleiding voor de organisatie. Het geeft de regels en uitgangspunten voor de eerlijke, zorgvuldige en rechtmatige verwerking van persoonsgegevens. Op die manier kan hiermee een nog betere verwerking van persoonsgegevens plaatsvinden binnen de gemeentelijke organisatie.

Juridisch kader

Het recht op eerbiediging van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens is een grondrecht. Het recht op privacy is niet alleen nationaal als grondrecht erkend, maar ook internationaal in onder andere het Europees Verdrag voor de Rechten van de Mens en het Internationaal Kinderrechtenverdrag.

Europese privacywetgeving

Sinds 25 mei 2018 is de AVG van toepassing zijn en heeft de Wet Bescherming Persoonsgegevens vervangen. De snelle technologische ontwikkelingen, de grote hoeveelheid beschikbare data en de aanzienlijke toename van de grensoverschrijdende stromen van persoonsgegevens heeft geleid tot harmonisatie van het Europees Unierecht met betrekking tot de bescherming van persoonsgegevens.

Het begrip persoonsgegevens omvat alle gegevens die een natuurlijk identificeerbaar persoon betreffen. NAW-gegevens, Burgerservicenummers, e-mail, maar ook kentekens en IP-adressen kunnen als persoonsgegeven worden aangemerkt, omdat deze kunnen leiden tot een persoon. De AVG zorgt voor een versterking en uitbreiding van privacyrechten van natuurlijke personen en brengt meer verantwoordelijkheden voor organisaties.

De gemeente moet aan (kunnen) tonen dat er is voldaan aan de wettelijke vereisten omtrent gegevensbescherming. Elke verwerking van persoonsgegevens gebeurt behoorlijk en rechtmatig. De verwerking moet transparant zijn over welke hen betreffende persoonsgegevens worden verzameld, gebruikt of geraadpleegd. Persoonsgegevens mogen enkel worden verwerkt als het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.
De opslagperiode is niet langer dan noodzakelijk voor het doel waar de persoonsgegevens voor zijn verzameld. Wanneer er geen concrete bewaartermijn in de wet is opgenomen voor een bepaald gegeven, bijvoorbeeld op grond van belastingwetgeving of op grond van de Archiefwet, betekent dit dat de gegevens vernietigd moeten worden als zij niet meer nodig zijn.

Grondslagen gegevensverwerking

De gemeente Heerde verwerkt enkel gegevens als aan tenminste een van de onderstaande voorwaarden is voldaan:

1. Er is sprake van een overeenkomst;
2. Er is sprake van een wettelijke plicht;
3. Er is sprake van een vitaal belang van de betrokkene;
4. Er is sprake van een publiekrechtelijke taak;

Bijzondere persoonsgegevens zijn gegevens die betrekking hebben op iemand godsdienst of levensovertuiging, etniciteit, politieke gezindheid, gezondheid, seksuele voorkeur en/of strafrechtelijk verleden. Deze persoonsgegevens worden door de gemeente Heerde met extra zorgvuldigheid beveiligd en verwerkt. De gemeente Heerde verzamelt en verwerkt persoonsgegevens enkel voor een bepaald doel.
Dit doel is specifiek en nadrukkelijk beschreven in het register van verwerkingen. Daarnaast wordt de verwerking getoetst aan het proportionaliteitsbeginsel en het subsidiariteitsbeginsel. Dit houdt in dat de verwerking in verhouding staat met het

beoogde doel en er enkel gegevens worden verwerkt als dit niet op een minder ingrijpende wijze kan worden bereikt.

Sectorspecifieke wetgeving

De voorwaarden en eisen die de AVG stelt, fungeren als parapluwetgeving: bijna alle sectoren, instellingen en bedrijven in Nederland moeten eraan voldoen. Naast dit algemeen wettelijk kader zijn er in sectorspecifieke wetten aanvullende regels opgenomen omtrent gegevensuitwisseling en het waarborgen van privacy. De Jeugdwet, de Wet Basisregistratie Personen, de Participatiewet en de WMO 2015 zijn voorbeelden van dergelijke wetgeving met specifieke aanvullende eisen.

Governance

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, ambtenaar en hulpverlener moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van de persoonlijke levenssfeer van de burger. De gemeente zal dit bewustwordingsproces ondersteunen met behulp van e-learning of door het geven van trainingen.

De eindverantwoordelijkheid

Het College van Burgemeester en Wethouders is in het merendeel van de verwerkingen verwerkingsverantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaats vindt. Er zijn echter ook verwerkingen waar enkel de burgemeester of de gemeenteraad de eindverantwoordelijkheid draagt.

Het College is voor de wijze waarop het invulling geeft aan het privacybeleid verantwoording verschuldigd aan de Gemeenteraad. Om privacy goed te borgen in de organisatie is het van belang dat er in de lijnorganisatie genoeg aandacht is voor dit onderwerp. De rollen en verantwoordelijkheden moeten zijn bepaald en vastgelegd.

1. Het College stelt het gemeentelijk privacybeleid vast met inachtneming van de aanbevelingen van de functionaris voor de gegevensbeschermingen (FG) bevordert de beschikbaarheid van voldoende middelen om privacybescherming passend te waarborgen.
2. Het College wijst een FG aan voor onafhankelijk toezicht op de uitvoering van het privacybeleid conform artikel 37 van de AVG.
3. De gemeente stelt een Privacy Officer aan voor de uitvoering en het adviseren over praktische privacyvraagstukken binnen de organisatie.
4. Het College wijst uit haar midden een portefeuillehouder privacy & gegevensbescherming aan die bestuurlijk verantwoordelijk is voor de uitvoering van het gemeentelijk privacybeleid en voor controle op de naleving van afspraken. De feitelijke uitvoering wordt opgedragen aan de FG.
5. De portefeuillehouder privacy ziet toe op de ontwikkeling en uitvoering van themagericht privacybeleid. De Privacy Officer en de FG rapporteren minstens één keer per jaar aan de portefeuillehouder over de resultaten die zij hieromtrent hebben bereikt. Privacy vormt een onderdeel van het planning en control proces van de gemeente. De portefeuillehouder informeert de Raad binnen de jaarlijkse planning en control cyclus over het privacybeleid binnen de gemeente.

In de praktijk is het afdelingshoofd (proceseigenaar) verantwoordelijk.

De Privacy Officer is belast met de uitvoering.

De Functionaris voor de gegevensbescherming ziet toe op de juiste uitvoering, beoordeelt en rapporteert.

Intern: Advies, uitvoering, controle en Toezicht

Door de functies uitvoering, advies en controle te scheiden, wordt voorkomen dat de FG toezicht moet houden op zijn eigen werk en waarborgt de gemeente haar geloofwaardigheid en betrouwbaarheid. Dit komt de kwaliteit ten goede.

Functionaris voor de gegevensbescherming

De FG fungeert als onafhankelijke interne toezichthouder. Hij ziet toe op de naleving van de Verordening, andere privacywetgeving en het beleid van de gemeente Heerde met betrekking tot de bescherming van persoonsgegevens, inclusief de toewijzing van verantwoordelijkheden, bewustwording en opleiding van de medewerkers. Om deze taak uit te voeren heeft de FG controlebevoegdheden, zoals nader bepaald in de Regeling taken en bevoegdheden FG. Daarnaast geeft de FG advies omtrent de uit te voeren gegevensbeschermingseffectbeoordelingen (DPIA's) en ziet toe op de uitvoering hiervan. De FG rapporteert zo nodig rechtstreeks aan het College.

Privacy Officer

Binnen de gemeente wordt een Privacy Officer aangesteld. De Privacy Officer vormt de vraagbaak binnen de gemeente voor privacyvraagstukken, geeft advies omtrent de uitvoering, ondersteunt bij de uitvoering en draagt bij aan kennisverspreiding en cultuur. Tevens actualiseert de Privacy Officer het register van verwerkingen en controleert de verwerkingen op rechtmatigheid.

Privacy op de werkvloer

Alle medewerkers van de gemeente Heerde dragen bij aan de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Privacy moet dan ook ingebed zijn in de door hen te hanteren werkwijze(n). De gemeente werkt actief aan het optimaliseren van kennis omtrent privacy en een transparante procesuitvoering. Individuele casussen, bevindingen en vragen omtrent dit onderwerp worden voorgelegd aan de Privacy Officer. De leidinggevenden zien toe op de naleving van wet- en regelgeving en het privacybeleid. De leidinggevende zorgt ervoor dat de FG naar behoren en tijdig wordt geïnformeerd en betrokken bij gelegenheden die verband houden met de bescherming van persoonsgegevens, zodat de FG zijn taken adequaat kan uitvoeren. Wanneer persoonsgegevens tussen de verschillende teams worden uitgewisseld worden hier afspraken over gemaakt.

Informatieveiligheid

De gemeente neemt passende technische en organisatorische maatregelen teneinde persoonsgegevens te beveiligen tegen verlies, onbevoegde toegang of onrechtmatige verwerking (op basis van de Baseline Informatiebeveiliging Gemeenten (BIG)). Hoe gevoeliger de informatie is, des te hoger het beveiligingsniveau. Daarnaast besteedt de gemeente Heerde reeds bij de ontwikkeling en aanschaf van producten en diensten aandacht aan privacy verhogende maatregelen.

In 2017 is het informatieveiligheidsbeleid vastgesteld, waarin kaders en maatregelen voor de beveiliging van (persoons)gegevens zijn opgenomen. Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

- Beschikbaarheid: hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
- Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen.
- Vertrouwelijkheid: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

Met het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het vereiste beschermingsniveau kenbaar gemaakt wordt. In het geval zich – ondanks de getroffen maatregelen – een beveiligingsincident voor doet waarbij persoonsgegevens zijn betrokken, wordt dit direct gemeld bij de FG. Onder een dergelijk beveiligingsincident valt onbevoegde toegang of kennisname van persoonsgegevens, dan wel verlies of onjuiste vernietiging van bestanden welke persoonsgegevens bevat.

Uitwisseling met en (intergemeentelijke) samenwerking met derden

Met het oog op de bescherming van persoonsgegevens maakt de gemeente Heerde met externe partijen afspraken omtrent de omgang met privacy. Dit kan in bijvoorbeeld convenanten of verwerkersovereenkomsten. Deze afspraken voldoen aan de wet.

Convenanten

Als de gemeente Heerde structureel informatie uitwisselt of samenwerkt met externe organisaties of andere gemeenten, maakt de gemeente Heerde vooraf duidelijke afspraken over de gegevensuitwisseling in de vorm van een convenant.

Verwerkersovereenkomst

Als de gemeente Heerde een externe vraagt voor haar gegevens te verwerken is het College verplicht met die externe een verwerkersovereenkomst te sluiten. In de verwerkersovereenkomst worden afspraken gemaakt omtrent de waarborgen en beveiliging van persoonsgegevens.
De FG ziet toe op de naleving van de verwerkersovereenkomst.
Binnen de gemeente Heerde wordt gebruik gemaakt van de meest recente standaard template voor een verwerkersovereenkomst opgemaakt door de VNG.

Positie en rechten van de burger

Transparantie richting de burgers staat bij de gemeente Heerde voorop. Naast informatie over de doeleinden van de verwerkingen, de categorieën van de verwerkte gegevens, de herkomst van de gegevens en de ontvangers verstrekt de gemeente ook informatie over de mogelijkheid van geautomatiseerde besluitvorming, alsmede de bewaartermijnen en klachtrechten.

Burgers hebben de volgende rechten:

- recht op informatie: Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt;
- inzagerecht: Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt;
- correctierecht: Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren;
- recht van verzet: Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken als er geen wettelijke basis bestaat voor het vastleggen van deze gegevens;
- recht om vergeten te worden: Als er geen wettelijke basis bestaat voor het vastleggen van deze gegevens, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen
- recht op bezwaar: Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Klachten en verzoeken met betrekking tot de bescherming van de persoonlijke levenssfeer worden direct doorgegeven aan het team waar de klacht betrekking op heeft. Er is een procedure opgesteld hoe de gemeente omgaat met een verzoek van een betrokkene.

Verwerking persoonsgegevens

Welke gegevens wordt door de gemeente verzameld?
Door de gemeente Heerde worden persoonsgegevens verzameld en verwerkt. Voor de uitvoering van diverse wetten geeft de betreffende wet veelal aan welke persoonsgegevens nodig zijn en dus verwerkt mogen worden.

Waarom worden deze gegevens verzameld?
Gegevens worden verzameld omdat zij nodig zijn ten behoeve van de uitvoering van bepaalde wetten en regelingen. Ook bij handhaving (zowel bestuursrechtelijk als strafrechtelijk) kan het nodig zijn om informatie te vergaren en uit te wisselen.

Hoe komt de gemeente aan deze gegevens?
In het merendeel van de gevallen worden deze gegevens door de betrokkene verstrekt. Soms zijn de gegevens afkomstig van derden, bijvoorbeeld van uitkeringsinstanties.

Wat gebeurt er precies met de gegevens?
Wat er precies met de verzamelde gegevens gebeurt, is vooral afhankelijk van het doel waarvoor ze vergaard worden. Meestal worden ze in een geautomatiseerd systeem opgenomen en zijn ze alleen toegankelijk voor de medewerkers die belast zijn met de uitvoering.

Wat zijn de bewaartermijnen van gegevens;
De bewaartermijnen van de gegevens lopen uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan het College een besluit over de bewaartermijn nemen. Als er geen besluit is genomen worden gegevens niet langer bewaard dan noodzakelijk.

Op welke manier worden de gegevens worden beveiligd?
Voor de beveiliging van gegevens is onder meer het Informatiebeveiligingsbeleid vastgesteld, waarin de kaders en de maatregelen zijn opgenomen, dit conform de BIG (Baseline Informatiebeveiliging Gemeenten). Uitvoering daarvan is belegd in een Informatiebeveiligingsplan.

Hoe worden de burgers hierover geïnformeerd?
Als de burger gegevens aan de gemeente Heerde verstrekt dan worden zij op de hoogte gesteld van de gegevens die de gemeente nodig heeft. Dikwijls staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene hoeft niet geïnformeerd te worden als deze al weet dat de gemeentepersoonsgegevens van hem of haar worden verwerkt en weet voor welk doel dat gebeurt. Als de gegevens bij de betrokkene zelf worden verkregen, moet de betrokkene vóór de verkrijging geïnformeerd worden. Meestal zal de informatie op het aanvraagformulier zijn opgenomen, waardoor de betrokkene de informatie dan heeft voordat hij de gegevens verstrekt.

Als de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd in het geval dat de gegevens verwerkt worden om deze aan een derde te verstrekken, uiterlijk op het moment van eerste verstrekking aan die derde.

Maatregelen

Gegevensbeschermingseffectbeoordeling - DPIA

Bij de invoering van nieuw beleid of regelgeving of bij het gebruik van nieuwe technologieën houdt de gemeente Heerde rekening met de bescherming van de persoonlijke levenssfeer door een gegevensbeschermingseffectbeoordeling of ook wel Data Protection Impact Assessment(DPIA) uit te voeren.
De volgende indicatoren zullen als toetsingskader worden gehanteerd om te bepalen of een DPIA noodzakelijk is:

- een nieuwe gemeentelijke taak;
- aanleg van een groot databestand;
- verwerking van nieuwe (bijzondere) persoonsgegevens;
- aanschaf van een nieuw ICT-systeem;
- systematische gegevensuitwisseling met een externe.

In het geval sprake is van één of meerdere indicatoren, kan de uitvoering van een DPIA noodzakelijk zijn.
In de DPIA komt tenminste naar voren:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen;
- een beoordelingen van de risico's voor de rechten en vrijheden van burgers;
- de beoogde maatregelen om de risico's aan te pakken.

Wanneer het effect van een verwerking beoordeeld is, kan de FG geraadpleegd en om advies gevraagd worden.

Register van verwerkingen

De gemeente Heerde houdt een register van verwerkingen bij met alle verwerkingsactiviteiten van persoonsgegevens per proces. De privacy officer controleert en actualiseert het register. Onder andere de doeleinden van de verwerkingen, de categorieën van persoonsgegevens, welke derden de gegevens ontvangen en de rechtmatige grondslag worden hierin opgenomen.

Privacy by design en privacy by default

Bij de aanschaf of ontwikkeling van producten, systemen of processen moet altijd rekening worden gehouden met de bescherming van persoonsgegevens. We noemen dit Privacy by Design (Pbd) en privacy by default. Voor alle producten, systemen of processen moeten de technische en organisatorische maatregelen ervoor zorgen dat standaard alleen die gegevens worden gebruikt die nodig zijn voor het doel. Als het niet mogelijk is om binnen bestaande producten en systemen invulling te geven aan de basis privacy vereisten (b.v. verwijderen van gegevens) wordt de leverancier hiervan op de hoogte gebracht en gevraagd dit mee nemen in toekomstige versies. Als blijkt dat bij een systeem gevoelige of bijzondere persoonsgegevens worden verwerkt en dit mogelijk een hoog privacy risico met zich meebrengt, zijn we verplicht om een Data Protection Impact Assessment(DPIA) uit te voeren.

Melding Datalekken

Beveiligingsincidenten en datalekken of een vermoeden daartoe worden zo spoedig mogelijk na de eerste ontdekking gemeld bij het betreffende teammanager, bij de FG of via mailadres datalek@heerde.nl. Als er sprake is van een meldplichtig datalek zal de FG daarvan melding doen aan de Autoriteit Persoonsgegevens (AP) en zo nodig aan de betrokkene(n). Voor de afhandeling van dergelijke incidenten zal de procedure m.b.t. datalekken worden gevolgd.

Bewustwording en communicatie

Naast het inrichten van het privacybeleid en werkprocessen is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Daarom is het belangrijk dat de professionals in het veld en binnen de gemeente zich bewust zijn van de regels en gedragsnormen rondom gegevensbescherming. De gemeente zal dit proces ondersteunen door het ontwikkelen van bijvoorbeeld trainingen of e-learning.

De gemeente streeft een cultuur na waarbij professionals elkaar in alle openheid aanspreken op het eigen gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimale inbedding van het privacybeleid.
Richting de burger is communicatie over gegevensbescherming van belang. De burger heeft het recht te weten wat er met zijn of haar gegevens gebeurt. De burger zal actief geïnformeerd worden over het privacybeleid via website en andere kanalen. Het gaat hierbij niet alleen om informatie over de manier waarop de gemeente met persoonsgegevens omgaat maar ook om informatie over de rechten van burgers, zoals inzage- en correctierecht van gegevens, de mogelijkheid verzet aan te tekenen tegen verwerking en het vernietigingsrecht als wel informatie over de bezwaar- en klachtenprocedure.

Bijlage 1 Definities privacywetgeving

bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

toestemming: van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.