Beleidsuitwerking Privacy gemeente Geldrop-Mierlo

Documenteigenaar:	Privacy Officers Gemeente Geldrop-Mierlo
Versie:	0.99 – aangeboden ter vaststelling
Datum:	29-02-2024

Vastgesteld door B&W op datum:	12 maart 2024

Evaluatie en controle:

Het college van Burgemeester en Wethouders van de gemeente Geldrop-Mierlo [Manager](hierna: college) is eindverantwoordelijke voor de gemeentelijke gegevensverwerking, en dus verantwoordelijk voor de vaststelling van dit document. Deze beleidsuitwerking privacy is vastgesteld door het college op d.d. zie 1ste pagina.

De beleidsuitwerking privacy wordt minimaal eens per 5 jaren beoordeeld en zo nodig tussentijds herzien[1] door de privacy officer. Daarbij worden de volgende aspecten in ieder geval bekeken: inhoud, uitvoerbaarheid, invoering en werking. De FG wordt geïnformeerd over deze evaluatie.

Referentie:

Het college beschrijft in deze beleidsuitwerking hoe de gemeente Geldrop-Mierlo aan de AVG wil voldoen. Dit is een uitwerking van de richtinggevende beleidskeuzes privacy die in het programma Organisatie zijn opgenomen. Het beleid geeft aan wat de verantwoordelijkheid is van elke medewerker bij het verwerken van persoonsgegevens

Detaillering en uitwerkingen worden uitgeschreven in andere documenten zoals procedures, handleidingen en werkinstructies. Om dit beleid compact te houden, maar ook omdat deze documenten mogelijk tussentijds gewijzigd kunnen worden.

Gerelateerde documenten:

De wetgeving: AVG, UAVG, WPG, BPG, BPG BOA en de Regeling Periodiek audit politiegegevens.

Wijzigingen beheer:

Versie	Status	Aanpassingen	Gedeeld met:	Datum
0.99	Ter vast-stelling	Aanpassingen FG, juridisch controller GM, CMT	CMT, B&W	29-2-2024
1	vastgesteld		doelgroep	Na de vaststelling

[1] bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van Data Protection Impact Assessment (DPIA) of Gegevensbeschermingseffectbeoordeling (GEB) of Privacy Impact Assessment (PIA)

INHOUD

1. Inleiding 5
1.1. Leeswijzer 6
1.1. Definities en afkortingen 6
1.2. Hardheidsclausule 6
1.3. Doel 6
1.4. Voor wie? 7
1.5. Reikwijdte 7
2. Privacy visie en Privacy ambitie, en uitgangspunten 8
2.1. Onze Privacy visie 8
2.2. Onze Privacy ambitie 8
2.3. Onze uitgangspunten 9
2.4. Wet politie gegevens (Wpg) vereisten 9
2.5. Diverse soorten persoonsgegevens 10
2.6. Raakvlakken met andere beleidsthema's 10
2.6.1. Domeinspecifieke wetgevingen gaan vóór de AVG 10
2.6.2. Richtinggevend en kader stellend 10
2.6.3. Ethiek en Algoritmen en andere nieuwe thema's 10
3. Organisatie, rollen en verantwoordelijken 11
3.1. Gemeenteraad (Informed) 11
3.2. College van B&W resp. Burgemeester (Accountable) 11
3.3. Concernmanagers en gemeentesecretaris (Responsible) 11
3.4. Alle medewerkers (Responsible) 11
3.5. Boa's (Responsible) 12
3.6. Bevoegd functionaris WPG (Responsible) 12
3.7. Privacy Officer (Consulted) 12
3.8. Chief Information Security Officer (Consulted) 12
3.9. Functionaris Gegevensbescherming (Consulted en Informed) 12
3.10. Belanghebbenden/betrokkenen (Informed) 12
3.11. Autoriteit Persoonsgegevens (Informed) 12
4. Privacy principes 13
4.1. Rechtmatig, behoorlijkheid en transparantie 13
4.2. Doel 13
4.3. Noodzaak en dataminimalisatie 13
4.4. Bewaartermijn 13

4.4.1. Bewaartermijn van politiegegevens 14
4.5. Juistheid/betrouwbaarheid, integriteit en vertrouwelijkheid (BIV) 14
5. Privacy inbedding in de organisatie 15
5.1. Bewustwording 15
5.2. Meldplicht datalekken (Inbreuk op persoonsgegevens) 15
5.3. DPIA/GEB 15
5.4. Delen van gegevens, convenanten, verwerkersovereenkomsten en geheimhoudingsverklaring 15
5.4.1. Ter beschikking stellen en verstrekken van politiegegevens 16
5.5. Privacy by Design en Privacy by Default 16
5.6. Verwerkingsregister 16
5.7. Rechten van Betrokkenen 17
5.8. Inzage rechten van betrokkenen 17
5.8.1. AVG rechten vs andere verzoeken 17
5.9. Klachten en geschillenbeslechting 17
5.10. Audio- en beeldmateriaal 18
5.11. PDCA Cyclus 18
5.12. Privacyplan 18
5.13. Toezicht en controle (auditplan) 18
5.13.1. ENSIA 18
5.13.2. WPG interne controle & externe audit 18
5.13.3. Informatieverstrekking, Toezicht en Onderzoek door FG 19

1. Inleiding

Dit document bevat de beleidsuitwerking privacy voor de [Manager]gemeente Geldrop-Mierlo (hierna: gemeente).

De gemeente verwerkt[2] persoonsgegevens[3] van inwoners, ondernemers, (inhuur)medewerkers en (keten)partners. Vanaf nu noemen we deze: betrokkenen[4]. Deze persoonsgegevens verzamelt de gemeente om de wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met diens persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker.
De gemeente is zich hiervan bewust. Dit beleid geeft de gemeente richting en toont aan dat zij de privacy waarborgt, beschermt en handhaaft. Dit privacy beleid is in lijn met de meest relevante lokale, nationale en Europese wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens.

Deze wetten en regelgevingen kennen op enkele gebieden onderlinge verschillen.
De Wpg heeft bijvoorbeeld specifieke bewaartermijnen voor de opslag van politiegegevens, terwijl de AVG geen concrete bewaartermijnen voorschrijft. Ook stelt de Wpg andere eisen bij het delen van politiegegevens tussen verschillende partijen, is er een verplichting tot logging[5], en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacy rechten van betrokkenen.

Andere verplichtingen zijn vergelijkbaar, maar kennen verschillen in de concrete uitwerking. Zoals de verplichting voor de verwerkingsverantwoordelijke voor het treffen van passende technische en organisatorische maatregelen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht, en elk jaar een interne controle.

---

[2] Zie artikel 4 sub 2 AVG: 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.
[3] Zie artikel 4 lid 1 Algemene Verordening Gegevensbescherming (hierna: “AVG”): 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, voornamelijk 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.
[4] Zie artikel 4 lid 1 AVG: een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”).
[5] Logging: het bijhouden en vastleggen van alle gebeurtenissen in een bepaald proces. Bijvoorbeeld wie er in een dossier heeft gekeken, of welke wijzigingen daarin zijn aangebracht.

De gemeente is verantwoordelijk voor het opstellen, uitvoeren, controleren en handhaven van een beleidsuitwerking privacy. Hiervoor gelden onder andere de volgende wettelijke kaders:

- AVG
- de Uitvoeringswet AVG
- Wet politie gegevens
- Besluit politiegegevens en Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg BOA)
- Reglement periodieke audit politiegegevens

1.1. Leeswijzer

Hoofdstuk 1 beschrijft het doel van dit document, wie hiervan kennis moeten hebben en de reikwijdte.
Hoofdstuk 2 beschrijft de visie, de ambitie en uitgangspunten van de gemeente.
Hoofdstuk 3 gaat in op de privacy organisatie, rollen en verantwoordelijken.
Hoofdstuk 4 beschrijft de privacy principes.
Hoofdstuk 5 maakt de vertaling hoe privacy in de gemeente ingebed is.

1.1. Definities en afkortingen

De begrippen zoals gedefinieerd in artikel 4 van de Algemene Verordening Gegevensbescherming (AVG) en artikel 1 van de Wet politiegegevens (Wpg) hebben in deze beleidsuitwerking privacy dezelfde betekenis. Daarnaast gebruikt de gemeente veel afkortingen en eigen begrippen. Die zijn opgenomen in het document “Definities en afkortingen AVG WPG”.

1.2. Hardheidsclausule

De gemeente kan in uitzonderlijke gevallen afwijken van deze beleidsuitwerking privacy, als de toepassing ervan voor de betrokkene buitensporige gevolgen zou hebben en in het geval van bijzondere omstandigheden, die niet in verhouding staan tot de doelen die met deze beleidsuitwerking privacy worden nagestreefd.

1.3. Doel

Het doel van deze beleidsuitwerking privacy is om richting te geven aan de gemeente ten aanzien van de privacy visie (paragraaf 2.1.), het privacy ambitieniveau (paragraaf 2.2.) en de uitgangspunten (paragraaf 2.3).
De richting is vastgelegd in richtlijnen die tot doel hebben een verantwoorde omgang met persoonsgegevens te waarborgen en de persoonlijke levenssfeer van de personen van wie de gemeente persoonsgegevens verwerkt (of laat verwerken) te beschermen.
Daarnaast heeft het beleidsuitwerking privacy als doel duidelijk omschreven taken en verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens en politiegegevens vast te leggen.

De concrete uitwerking van deze beleidsuitwerking privacy is – indien van toepassing – beschreven in andere documenten binnen de gemeente. In inrichtingsdocumenten zoals handreikingen en procedures zoals bijvoorbeeld procedure melden datalekken of afspraken ten aanzien van gegevensdeling in het kader van wetuitvoering. En in documenten die de verrichtingen beschrijven zoals procesbeschrijvingen en werkafspraken.

Raakvlakken met andere beleidsthema’s zijn beschreven in paragraaf 2.6.

1.4. Voor wie?

Iedereen die werkzaam is binnen de gemeente is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens. De gemeente verlangt van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente dat de voorschriften van deze beleidsuitwerking privacy worden opgevolgd en actief worden uitgedragen.
Voor betrokkenen[6], zoals onze inwoners, geeft deze beleidsuitwerking privacy informatie over hoe de gemeente hun persoonsgegevens verwerkt.

1.5. Reikwijdte

De gemeente verzamelt en gebruikt persoonsgegevens van inwoners, leveranciers en medewerkers en andere natuurlijke personen (hierna te noemen: betrokkenen).

Deze beleidsuitwerking privacy is van toepassing op alle verwerkingen van persoonsgegevens en politiegegevens door of namens de bestuursorganen van de gemeente, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.
4. De verwerking van politiegegevens in het kader van de uitvoering van de dagelijkse politietaak door de daarvoor aangewezen buitengewoon opsporingsambtenaren (BOA's) en hun ondersteuners (niet-BOA's).

[6] Zie artikel 4 lid 1 AVG: een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene").

2. Privacy visie en Privacy ambitie, en uitgangspunten

Voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten en vrijheden van betrokkenen, is een goede privacy borging noodzakelijk. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Verantwoord en bewust gedrag van alle medewerkers is essentieel voor privacy binnen de gemeente.
Daarom beschrijft dit hoofdstuk onze privacy visie, privacy ambitie en uitgangspunten.

2.1. Onze Privacy visie

Ons privacy kompas is ingesteld op het voldoen aan de intentie van de AVG en de Wpg, en daarbij de rechten van inwoners en bedrijven te beschermen. De gemeente hanteert waar mogelijk de principes van privacy by design en privacy by default (zie paragraaf 5.5.).

Onze privacy visie (toekomstbeeld) is:

De gemeente zorgt voor haar inwoners en ondernemers door (persoons)gegevens te beschermen en op een privacyvriendelijke manier te werken.

2.2. Onze Privacy ambitie

We hanteren het volwassenheidsmodel CIP[7] dat identiek is aan het volwassenheidsmodel van de Informatie beveiliging dienst (IBD).



Figuur 2: Volwassenheidsmodel

Onze privacy ambitie[8] is:

De gemeente streeft naar een gestandaardiseerde vastgestelde werkwijze (niveau 3).

[7] https://www.cip-overheid.nl/media/uasdokan/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf
[8] Bepaald in het DOD-overleg 30-08-2023

2.3. Onze uitgangspunten

De gemeente hanteert in haar werkwijze de volgende uitgangspunten:

- Onze visie en ambitie
- Lijnmanagement is verantwoordelijk voor de borging van de gegevensbescherming in processen
- Privacy is de verantwoordelijkheid van iedere medewerker
- Persoonsgegevens worden verwerkt volgens de privacy principes
- Persoons- en politiegegevens worden adequaat beveiligd
- Persoons- en politiegegevens worden bewaard conform wetgeving (o.a. archiefwet, WPG)
- We hanteren een risico gestuurde aanpak, en registreren de impact voor betrokkenen bij geaccepteerde risico's.
- De privacy risicoclassificatie van het DocumentStructuurPlan[9] wordt gehanteerd, tenzij…..
- Politiegegevens worden verwerkt in systemen die de WPG-vereisten faciliteren, tenzij …
- De standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk (privacy by design / by default)

We werken hierbij vanuit onze kernwaarden:



Figuur 1: Kernwaarden

2.4. Wet politie gegevens (Wpg) vereisten

Het normenkader van de Wpg is grotendeels gelijk aan dat van de AVG. Op hoofdlijnen geldt voor de WPG aanvullend nog het volgende:

- De boa's van de gemeente kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens zowel met de AVG te maken als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg;
- De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Waaronder de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk;
- Het uitvoeren van interne en externe Wpg-privacyaudits.

De Wpg vereisten die in onze applicaties moeten zijn geborgd:

- Er moet een scheiding worden aangebracht tussen informatie die op feiten is gebaseerd en informatie die op een persoonlijk oordeel is gebaseerd;
- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP);
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in die systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging (Bpg, artikel 6:1A[10]).

[9] Informatiebeheer heeft een DocumentStructuurPlan (DSP) waarmee de gemeente aan de archiefwet voldoet
[10] Besluit politiegegevens: https://wetten.overheid.nl/BWBR0023086/2023-01-01

2.5. Diverse soorten persoonsgegevens

Persoons-, politie- en strafrechtelijke gegevens onderscheiden zich van elkaar door de taak waarvoor ze verwerkt worden.

Bijzondere persoonsgegevens door de gevoeligheid van de informatie. Het betreft dan informatie over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op unieke identificatie, gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid.

2.6. Raakvlakken met andere beleidsthema's

De beleidsuitwerking privacy heeft raakvlakken met andere beleidsthema's, vertoont hiermee overlap, of is hiervan afhankelijk.

2.6.1. Domeinspecifieke wetgevingen gaan vóór de AVG

De gemeente voert taken uit voor diverse wetgevingen, zoals de Wet Basisregistratie Persoonsgegevens (BRP), Jeugdwet, de Wet Maatschappelijke Ondersteuning (WMO).
De in die wetgeving beschreven gegevensbeschermingsmaatregelen gaan vóór de AVG-bepalingen.
Daar waar niets in de specifieke wet vermeld staat over gegevensbescherming, geldt de AVG.
Zodra vanuit de BRP gegevens verstrekt worden, is de AVG van toepassing.
Daarnaast is er ook nog het Europees Verdrag voor de Rechten van de Mens[11] waarin de universele rechten van de Mens en fundamentele vrijheden zijn vastgelegd.

2.6.2. Richtinggevend en kader stellend

Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens en politiegegevens. Het informatiebeveiligingsbeleid is richtinggevend en kader stellend ten aanzien van de maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen.
Zorgvuldig 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.
Het archiefbeleid is vastgelegd in de Archiefverordening en Beheerregeling Informatiebeheer, en gebaseerd op de Archiefwet. Beleidsuitwerking privacy en archiefbeleid worden in onderlinge samenhang bekeken.

2.6.3. Ethiek en Algoritmen en andere nieuwe thema's

Ethiek speelt een belangrijke rol op het (negatief) effect voor betrokkenen of de samenleving. Het gaat over het juist handelen en het evalueren ervan, op ethische principes[12] zoals respect voor autonomie (vrijheid, eigen regie), weldoen, niet schaden en rechtvaardigheid. De methodiek Impact Assessment Mensenrechten en Algoritmen (IAMA[13]) wordt binnen de overheid veelal gebruikt om de ethische risico's in kaart te brengen, met name voor vragen met betrekking tot gegevensdeling en inzet van algoritmes. We gaan bekijken of deze methodiek overlap heeft of is samen te voegen met de Data Protection Impact Assessment (DPIA).
Algoritmes[14] hebben impact op (automatische) besluitvorming voor betrokkenen. Daarom is het belangrijk om te begrijpen wat algoritmes doen en hierover transparant zijn. De gemeente is aangesloten op het landelijke Algoritmeregister Nederlandse Overheid.

[11] Europees Verdrag voor de Rechten van de Mens
[12] 4 ethische principes van de Amerikaanse bio-ethici Tom Beachamp en James Childress
[13] Ontwikkelt iom University Utrecht
[14] Een proces, stappenplan of een serie regels die een computer moet volgen om een probleem of rekensom op te lossen.

3. Organisatie, rollen en verantwoordelijken

De bestuursorganen van de organisaties zijn verantwoordelijk voor de naleving van de AVG en het beleidsuitwerking privacy, ieder voor zover het hun bestuurlijke taken betreft. Zij zijn verantwoordelijk voor het verwerken van persoonsgegevens door de eigen gemeente en bij externe organisaties belegde taken.

Hieronder worden de rollen en verantwoordelijkheden kort aangestipt. Deze worden in detail beschreven in het document 'Privacy organisatie', inclusief de aanwezige overlegstructuren.

3.1. Gemeenteraad (Informed)

De gemeenteraad wordt geïnformeerd over de privacy binnen de gemeente, omdat zij een bestuurlijke toezichttaak heeft op basis van de Gemeentewet en decentralisatiewetgeving.

3.2. College van B&W resp. Burgemeester (Accountable)

Het College is eindverantwoordelijk (verwerkingsverantwoordelijke) voor de naleving van de privacywetgeving binnen de gemeente en het aantoonbaar maken hiervan, óók voor het gedeelte dat via mandaat bij de Dienst Dommelvallei is belegd.
De burgemeester is verantwoordelijk voor (het naleven en aantonen daarvan voor) de Wpg.
College en burgemeester zijn daarmee verantwoordelijk voor het vaststellen van de beleidsuitwerking privacy, het aansturen van de uitvoering ervan, en de verantwoording aan de partijen benoemd bij Informed, waaronder de Gemeenteraad.

3.3. Concernmanagers en gemeentesecretaris (Responsible)

De concernmanagers zijn feitelijk verantwoordelijk voor de uitvoering van de beleidsuitwerking privacy en de naleving van de privacywetgeving binnen de teams of de programma's.
Het dagelijks bestuur Dienst Dommelvallei is verantwoordelijk dat de aan de GR gemandateerde taken worden uitgevoerd conform deze beleidsuitwerking privacy en de naleving van de privacywetgeving.

De gemeentesecretaris is eindverantwoordelijk voor de uitvoering van de beleidsuitwerking privacy en de naleving van de privacywetgeving van gemeentebrede of teams en programmas overstijgende zaken. Deze verantwoordelijkheid kan, indien gewenst, per onderdeel toegewezen worden aan een van de concernmanagers of aan de directeur Dienst Dommelvallei.

Zij zorgen voor de verantwoording, voor voldoende middelen, voor de uitvoering van (verbeter)activiteiten en voor de bewaking en beveiliging van de persoonsgegevens en politiegegevens.

3.4. Alle medewerkers (Responsible)

Iedereen werkzaam binnen de gemeente is betrokken bij de verwerking van persoonsgegevens en is daarom verantwoordelijk voor het verantwoord omgaan met persoonsgegevens de behoren bij zijn/haar taak. De gemeente verlangt daarom van al haar medewerkers en alle personen die werkzaam zijn voor de gemeente, dat de voorschriften van deze beleidsuitwerking privacy worden opgevolgd en actief worden uitgedragen. Daarnaast worden geheimhoudingsverklaringen afgesloten met de (interne en externe) medewerkers.

Privacy is de verantwoordelijkheid van iedere medewerker!

3.5. Boa's (Responsible)

De functionaris die zorgt draagt voor de opsporing van strafbare feiten en de voorbereiding van eventuele vervolging van deze feiten. De gecertificeerde en aangestelde buitengewoon opsporingsambtenaren (BOA's) verwerken politiegegevens, en zijn verantwoordelijk voor de juiste verwerking van deze politiegegevens conform de Wpg.

3.6. Bevoegd functionaris WPG (Responsible)

De team[Manager][15]) van de BOA is aangewezen als bevoegd functionaris (BF). De BF is de 'hoeder' van de politiegegevens en beoordeelt wie er toegang mag hebben tot deze gegevens. Daarnaast bepaald de BF of deze politiegegevens voor onderzoek verder verwerkt mogen worden (Wpg artikel 9 lid 3, artikel 11 lid 1 en 4, artikel 13 lid 3) en of ze kunnen worden verstrekt aan een samenwerkingspartner.

3.7. Privacy Officer (Consulted)

De Privacy Officer (PO) is het interne aanspreekpunt voor de gemeente rondom (praktische invulling van) privacy gerelateerde vraagstukken, heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van de beleidsuitwerking privacy, en is belast met de coördinatie en uitvoering van het privacy- en gegevensbeschermingsbeleid van de gemeente. Daarnaast kan de Privacy Officer de lijn ondersteunen (support) bij de uitwerking van privacy vraagstukken.

3.8. Chief Information Security Officer (Consulted)

De Chief Information Security Officer (CISO) stelt kaders op het gebied van informatiebeveiliging die voor de gehele organisatie gelden, zorgt voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, adviseert over de beveiliging bij datalekken (volgens de procedure Datalekken) en is coördinator van de Eenduidige Normatiek Single Information Audit (ENSIA).

3.9. Functionaris Gegevensbescherming (Consulted en Informed)

De Functionaris Gegevensbescherming (FG) is als onafhankelijk interne toezichthouder aangewezen, en ziet toe op de naleving van de AVG en Wpg (art. 36) bij de gemeente. De FG kan ambtshalve een onderzoek instellen naar de wijze waarop wordt voldaan aan de AVG en WPG en dit privacy beleid. De FG stelt jaarlijks een AVG Jaarrapportage en WPG jaarrapportage op en stuurt dit aan het College van Burgemeester en Wethouders. De FG stemt af met portefeuillehouder en gemeentesecretaris hoe de gemeenteraad hierover wordt geïnformeerd.
De FG is de contactpersoon voor de Autoriteit Persoonsgegevens (AP) en voor de inwoners in geval van privacy klachten en adviseert bij datalekken (volgens de procedure Datalekken).
De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.10. Belanghebbenden/betrokkenen (Informed)

Alle personen van wie de gemeente persoonsgegevens verwerkt, worden tijdig geïnformeerd over de inhoud van dit privacy beleid en hoe zij hun rechten kunnen uitoefenen (bijvoorbeeld via flyers, gesprekken en de website), zie 5.7. Betrokkenen zijn onder andere (onze) inwoners en medewerkers.

3.11. Autoriteit Persoonsgegevens (Informed)

De Autoriteit Persoonsgegevens (AP) is de onafhankelijke landelijke toezichthouder en houdt toezicht op de naleving van de privacyregels in Nederland.

[15] Verbeterplan Wpg audit vastgesteld door MT op dd 19-april-2023 (artikel 2:10 lid 2 Besluit politiegegevens)

4. Privacy principes

De beleidsuitwerking privacy is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. De gemeente onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

We gaan zorgvuldig om met persoonsgegevens en respecteren de privacy van betrokkenen.

4.1. Rechtmatig, behoorlijkheid en transparantie

De gemeente verwerkt persoonsgegevens alleen in overeenstemming met de wet, dan is de verwerking rechtmatig. Veelal verwerkt de gemeente gegevens op basis van een wet (wettelijke verplichting) of een publiekrechtelijke taak. Soms gebeurd de verwerking op basis van toestemming on in het kader van algemeen belang.

De gemeente vindt het belangrijk dat betrokkenen erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. Daarom informeert de gemeente de betrokkenen op welke wijze hun persoonsgegevens verwerkt worden. Dit gebeurd op een begrijpelijke en toegankelijke manier, via diverse communicatiekanalen waaronder de privacyverklaring van de gemeente. De betrokkene wordt daarbij ook geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen.
Alleen als de wet anders bepaalt, wijkt de gemeente van de informatieplicht af.

4.2. Doel

De gemeente verwerkt persoonsgegevens alleen met een gerechtvaardigd en gespecificeerd doel. De persoonsgegevens worden niet voor andere doelen gebruikt. Tenzij geldt dat de twee doelen aan elkaar verwant zijn, er geen nadelige effecten voor de betrokkenen zijn of hiervoor extra waarborgen worden getroffen.
De gemeente voert voordat de verwerking start, een toets uit om te bepalen of de gegevens (voor andere doelen) mogen worden gebruikt op grond van de wet- en regelgeving.

4.3. Noodzaak en dataminimalisatie

De gemeente verwerkt alleen persoonsgegevens die noodzakelijk zijn – in verhouding staan – om het doel te bereiken. Dit betekent dat als het doel op een andere wijze – zonder of met minder persoonsgegevens[16] of die minder inbreuk maken op de privacy van betrokkene[17] – kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. We slaan zo min mogelijk gegevens op.

4.4. Bewaartermijn

De gemeente stelt de bewaartermijn van de verwerking vast op basis van wettelijke bepalingen of de Archiefwet 1995 selectielijsten. Als hierop geen bewaartermijn kan worden vastgesteld, dan stelt de gemeente zelf de bewaartermijn vast waarbij de persoonsgegevens niet langer worden bewaard dan noodzakelijk. Bewaart de gemeente gegevens toch langer, dan worden deze geanonimiseerd zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

[16] Proportionaliteit: inbreuk op de belangen van de betrokkene mag niet onevenredig. Alleen de noodzakelijke gegevens worden verwerkt voor het bereiken van het vastgestelde doel.
[17] Susidiariteit: er wordt gecontroleerd bij een verwerking, of er een minder verregaande manier is om de taak uit te voeren. Bijv. geen geboortedatum maar de maand/geboortejaar.

4.4.1. Bewaartermijn van politiegegevens

Alle politiegegevens worden gelabeld conform de Wpg-artikelen 8, 9 en 13 en hiervoor wordt de bewaartermijn ingericht. De gemeente regelt hiermee dat politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, conform de toepasselijke wet- en regelgeving of voor de doeleinden waarvoor deze zijn verwerkt.
Politiegegevens worden na verwijdering nog maximaal vijf jaar bewaard en worden daarna vernietigt, of eerder als een andere bewaartermijn geldt. In geval van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens, echter dan voldoen we aan bewaareisen van de Archiefwet.

4.5. Juistheid/betrouwbaarheid, integriteit en vertrouwelijkheid (BIV)

De gemeente verwerkt alleen persoonsgegevens die juist en actueel zijn, oftewel betrouwbaar, gelet op het doel waarvoor zij zijn verzameld. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.
Betrokkenen kunnen aan de gemeente vragen hun persoonsgegevens aan te passen als die niet kloppen (zie paragraaf 5.7).

Daarnaast neemt de gemeente passende (technische en organisatorische) beveiligingsmaatregelen om te voorkomen dat (met name bijzondere) persoonsgegevens misbruikt, onrechtmatig of ongeautoriseerd verwerkt of bekend gemaakt worden. Deze zijn vastgelegd in het informatiebeveiligingsbeleid en bijbehorende documenten.
Persoonsgegevens worden alleen verwerkt door medewerkers/personen die voor geheimhouding hebben getekend, en voor de bevoegdheden die aan hen zijn toegekend op grond van het geldend toegangsbeleid.
Periodiek wordt gecontroleerd (onder andere door logging en monitoring) op ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens, om deze zo te voorkomen.

De gemeente schakelt soms andere organisaties in om taken uit te voeren. Daarbij zorgt de gemeente voor de juiste privacy afspraken (zie paragraaf 5.4) en legt die vast bij het contract (conform contractmanagement).

5. Privacy inbedding in de organisatie

Beleid en bovenstaande principes zijn onvoldoende om de risico's van het verwerken van persoonsgegevens uit te sluiten. De gemeente zet onderstaande middelen in, om de privacy van betrokkenen te waarborgen.

5.1. Bewustwording

Het zorgvuldig omgaan met persoonsgegevens is een kwestie van een adequate informatiebeveiliging, van correcte werkprocessen, en van bewustwording van de medewerkers. Het bewustzijn van medewerkers wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en verantwoord gedrag wordt aangemoedigd.
Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies.
Elke Boa doorloopt verplicht een Wpg training

5.2. Meldplicht datalekken (Inbreuk op persoonsgegevens)

Er is sprake van een datalek als toegang tot, verlies of wijziging van persoonsgegevens heeft plaatsgevonden zonder dat dit de bedoeling was.
De gemeente behandelt en registreert deze datalekken conform de procedure 'datalekken'. Als een datalek meldplichtig is, dan wordt dit gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens). Afhankelijk van het risico voor de betrokkenen worden ook zij geïnformeerd. Een mededeling aan betrokkenen blijft achterwege indien daarvoor een Wpg-uitzondering van toepassing is. Bijvoorbeeld ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.
De gemeente zet de bevindingen om in verbeterpunten en bewaakt de opvolging hiervan.

5.3. DPIA/GEB

Als de verwerking gelet op de aard en omvang, de context en de doeleinden mogelijk een hoog risico[18] inhoudt voor de rechten en vrijheden van betrokkene, dan voert de gemeente een beoordeling uit op het effect van de verwerking van persoonsgegevens.
Deze beoordeling wordt Data Processing Impact Assessment, DPIA) of gegevenseffectbeoordeling (GEB) genoemd.

Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, neemt de gemeente voldoende maatregelen om deze risico's te verminderen. Als het niet lukt om met maatregelen de risico's tot een acceptabel niveau te verlagen, dan motiveert de gemeente dit.
De FG geeft over elke DPIA een zwaarwegend advies aan de verwerkingsverantwoordelijke.

De gemeente overlegt met de AP voordat wordt gestart met een verwerking met een hoog risico: dit wordt een voorafgaande raadpleging[19] genoemd.

5.4. Delen van gegevens, convenanten, verwerkersovereenkomsten en geheimhoudingsverklaring

De gemeente werkt veel samen met externe partners. De gemeente zorgt voor bescherming van de privacy en gegevensverwerking door afspraken te borgen in contracten, via een vast onderdeel van het inkoopproces. Deze afspraken voldoen aan wettelijke eisen en aan de modelovereenkomsten van de Vereniging Nederlandse Gemeenten of de Informatiebeveiligingsdienst.

[18] Ons basis/startpunt is de privacy risicoclassificatie van het DocumentStructuurPlan
[19] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging

De gemeente beoordeelt of de externe partner een verwerker of een verwerkingsverantwoordelijke is. Zie **Voorbeeldlijst: wie is hier de verwerker en wie de verantwoordelijke?**

Verwerkers
Indien de externe organisatie in opdracht van de gemeente persoonsgegevens verwerkt, dan is dit een verwerker. Bijvoorbeeld een cloudsysteem leverancier. Ook een verwerker moet zich houden aan de privacyregelgeving. Daarom legt de gemeente afspraken met verwerkers vast in verwerkersovereenkomsten.

Samenwerkingsverbanden
Als de gemeente samenwerkt met andere (overheid)organisaties om een taak van algemeen belang uit te voeren, kan er sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). Ook dan maakt de gemeente afspraken over de wijze waarop persoonsgegevens worden verwerkt en beschermd, bijvoorbeeld in een privacyconvenant.

Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of aan een internationale organisatie, gebeurt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en deze beleidsuitwerking privacy.

5.4.1. Ter beschikking stellen en verstrekken van politiegegevens
Conform de Wpg hanteert de gemeente het ‘need to know’-principe, waarbij altijd een afweging wordt gemaakt t.a.v. de noodzakelijkheid, de proportionaliteit en de subsidiariteit. Het houdt in dat de gemeente politiegegevens deelt met personen of instanties binnen het politiedomein die de politiegegevens nodig hebben voor de uitvoering van hun politietaak. Dit wordt ‘ter beschikking stellen’ genoemd.

Gegevensdeling buiten het politiedomein wordt ‘verstrekken’ genoemd. De gemeente verstrekt alleen politiegegevens voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd, en zorgt daarbij dat zij voldoet dan aan de documentatieplicht. Indien vereist is, zorgt de gemeente dat de verstrekking plaatsvindt in overeenstemming met het bevoegd gezag. Bijvoorbeeld bij verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob.

5.5. Privacy by Design en Privacy by Default
De maatschappij staat niet stil en ook de gemeente verandert. Bijvoorbeeld ontwikkelt en levert nieuwe diensten/producten, krijgt nieuwe of wijzigt bestaande processen of systemen, of gaat nieuwe samenwerkingsverbanden aan. Door bij het ontwerp van deze nieuwe ontwikkelingen de privacy mee te nemen, inclusief een adequate bescherming van persoonsgegevens, beperkt de gemeente het risico op onrechtmatige verwerkingen en datalekken. Dit wordt Privacy by Design genoemd.
Daarbij richt de gemeente de standaardinstellingen zo privacy-vriendelijk mogelijk in (Privacy by Default).

5.6. Verwerkingsregister
De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens en politiegegevens gedocumenteerd en inzichtelijk zijn gemaakt.
Het verwerkingsregister voldoet aan de eisen die daaraan zijn gesteld (art. 30 AVG). Zie voor meer informatie de privacyverklaring op de website van de gemeente.

5.7. Rechten van Betrokkenen

In de maatschappij en ook binnen de gemeente, worden op steeds grotere schaal gegevens van betrokkenen vastgelegd. En de tendens is dat die informatie steeds vaker aan elkaar gekoppeld wordt.
De gemeente zal zorgvuldig omgaan met diens persoonsgegevens, en zorgt dat betrokkenen voor zichzelf op kunnen komen door controle te houden over de verwerking van hun persoonsgegevens. De rechten worden gerespecteerd en verankerd in onze procedures.

5.8. Inzage rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens de gemeente over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG (art. 13 t/m 22) en de WPG (paragraaf 4) uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking van de verwerking en het recht op overdraagbaarheid (dataportabiliteit).

Om te zorgen dat de persoonsgegevens aan de juiste betrokkene worden afgegeven, moet de gemeente bij een verzoek altijd eerst de identiteit van de betrokkene vastgesteld worden. Desnoods wordt hiervoor aanvullende informatie opgevraagd.
De gemeente reageert binnen één maand op het verzoek. In uitzonderlijke gevallen mag de gemeente er drie maanden over doen, maar dan wordt de betrokkene hierover geïnformeerd binnen een maand. Indien nodig ondersteunt de Privacy Officer.

Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in de procedure ‘rechten van betrokkenen’ . Voor audio-en beeldmateriaal zie paragraaf 5.10.

5.8.1. AVG rechten vs andere verzoeken

De gemeente kan ook verzoeken ontvangen die onder andere wetgevingen vallen en vanuit die wetgeving beoordeeld worden. Bij beoordeling van het verzoek bekijkt de gemeente telkens of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen.
Bijvoorbeeld: BRP geheimhouding, Jeugddossier inzage, Wet maatschappelijke ondersteuning dossier inzage, Wet Open Overheid (WOO), Wet hergebruik van overheidsinformatie (WHO).

5.9. Klachten en geschillenbeslechting

Als de betrokkene van mening is dat de gemeente niet tijdig heeft gereageerd of niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan de FG worden benaderd zoals beschreven in de privacyverklaring op de website van de gemeente.

Mocht de betrokkene niet tevreden zijn met de reactie van de FG, dan kan de betrokkene een klacht indienen bij de Autoriteit Persoonsgegevens (zie www.autoriteitpersoonsgegevens.nl) of kan betrokkene de gemeente in gebreke stellen wegens niet tijdig beslissen, zie website van de gemeente.

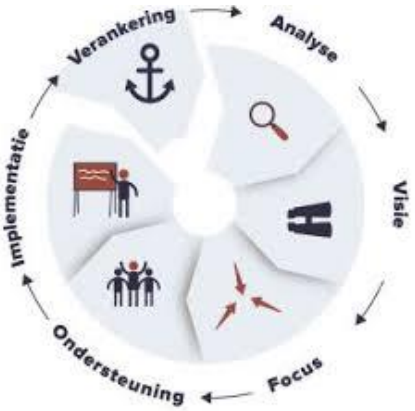
Voelt de betrokkene zich onheus bejegend over de wijze waarop de het bestuursorgaan of medewerker van de gemeente zich jegens hem heeft gedragen, dan kan de betrokkene een klacht indienen middels de van toepassing zijnde klachtenprocedure zoals is opgenomen op de website of www.overheid.nl (dit gebeurd dan op grond van de Algemene wet bestuursrecht Awb).
Indien de klachtenprocedure in relatie staat tot de verwerking van persoonsgegevens zal de behandelend ambtenaar van de klachtadviescommissie afstemming zoeken met de FG.

5.10. Audio- en beeldmateriaal

De gemeente zet op verschillende plekken audio- en beeldopnames in, bijvoorbeeld tijdens de in beginsel openbare raads- en commissievergaderingen en voor veiligheid.
De gemeentelijke website vermeld waar deze zijn ingezet en waarvoor, en kunnen betrokkenen lezen hoe ze hun audio/beelden kunnen inzien.
De inzet van audio- en beeldopnames gebeurt conform passende wetgeving, de beleidsregels van de Autoriteit Persoonsgegevens en het 'audio en beeldmateriaal beleid'.

5.11. PDCA Cyclus

De gemeente streeft ernaar om rondom de verwerking van persoonsgegevens *in control* te zijn en daarover op professionele wijze verantwoording af te leggen.
In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens[20], dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.



Figuur 3: Plan-Do-Check-Act cyclus

5.12. Privacyplan

Jaarlijks wordt een privacyplan geactualiseerd. Onder andere naar aanleiding van jaarverslagen van de AP/IBD en toekomstige verwachtingen, organisatorische en maatschappelijke ontwikkelingen, actueel privacy volwassenheidsniveau, datalekken, risico's en verbetermaatregelen.

5.13. Toezicht en controle (auditplan)

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats.

5.13.1. ENSIA

In de Eenduidige Normatiek Single Information Audit, het verantwoordingstraject informatiebeveiliging dat jaarlijks wordt uitgevoerd, wordt de AVG (gedeeltelijk) meegenomen.

5.13.2. WPG interne controle & externe audit

De gemeente laat overeenkomstig de Regeling periodieke audit politiegegevens één keer in de vier jaar een externe audit uitvoeren op naleving van de WPG voor het verwerken van politiegegevens. Indien er tekortkomingen zijn, wordt binnen 3 maanden een verbeterrapport opgesteld en volgt

[20] Het borgingsproduct van de VNG kan worden gebruikt voor de privacy compliance en risico's in beeld te brengen, en daarbij behorende beheersmaatregelen.

binnen 1 jaar een externe her-controle op die onderdelen waar tekortkomingen geconstateerd zijn. De resultaten van de Wpg-privacyaudit en eventuele her-controle worden aan de AP verstrekt. Daarnaast voert de gemeente jaarlijks een interne controle uit op de naleving van een aantal onderdelen van de WPG voor het verwerken van politiegegevens. Dit gebeurd door een auditor die Wpg-getraind is. Voor 2023 tot en met 2025 is dit belegd bij een extern bureau.

5.13.3. Informatieverstrekking, Toezicht en Onderzoek door FG

De FG is de interne toezichthouder. Zie paragraaf 3.9.