GEMEENTE UTRECHTSE HEUVELRUG

GEMEENTEBLAD

Officiële uitgave van de gemeente Utrechtse Heuvelrug

Nr. 318884

23 juli 2024

Regionaal Privacybeleid gemeente Utrechtse Heuvelrug 2024-2028

Hoofdstuk 1 Algemeen regionaal privacybeleid

1. Inleiding

De gemeenten De Bilt, Bunnik, Wijk bij Duurstede en Utrechtse Heuvelrug werken met (persoons)gegevens van burgers, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelen de gemeenten om de gemeentelijke 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 burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze 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 De Bilt, Bunnik, Wijk bij Duurstede en Utrechtse Heuvelrug zijn zich hiervan bewust en willen met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Geldigheidsduur

Dit beleid is vastgesteld door het college van B&W als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt tenminste eens per vier jaar beoordeeld en zo nodig herzien. Indien daar aanleiding toe is (bijvoorbeeld bij grote organisatorische veranderingen, wetswijzigingen, uitkomsten van privacy-toetsen kan het college besluiten tot een tussentijdse herziening.

Hoewel de gemeenten graag samenwerken op het gebied van privacy en gegevensbescherming, zijn niet alle gemeenten op dezelfde manier ingericht. Daarom is er ruimte gelaten voor lokale invulling op bepaalde aspecten, met name waar het gaat om de gemeentelijke organisatie. Dit geldt in elk geval voor het onderdeel ‘Organisatie van de gemeente’. Waar nodig hebben de afzonderlijke gemeenten de tekst aangepast op hun eigen organisatie. De gemeente Utrechtse Heuvelrug heeft domeinspecifiek beleid toegevoegd op het gebied van de Wet politiegegevens en het sociaal domein in twee addenda.

2. Begripsbepalingen

De definities van art. 4 AVG hebben in dit beleidsdocument dezelfde betekenis.

3. Visie

Ons gezamenlijke doel op het gebied van privacybescherming is dat betrokkenen het vertrouwen hebben dat hun persoonsgegevens bij ons in veilige handen zijn. Daarvoor treffen wij de maatregelen die nodig zijn om de risico’s op de schending van privacy zo klein mogelijk te houden. Om het vertrouwen van de betrokkenen te verkrijgen en te behouden maken wij inzichtelijk dat wij aan de eisen van privacybescherming voldoen door inzicht te geven in de wijze waarop wij de persoonsgegevens beschermen. Dit geldt voor zover dat redelijk en passend is en bijdraagt aan de doelstelling om de risico’s op privacy schending zo laag mogelijk te houden.

De komende jaren zet de gemeente in op het verhogen van de privacybewustwording en verdere professionalisering van de privacyfunctie in de organisatie. Een goede privacyboekhouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

4. Doel

Met dit privacybeleid geeft de gemeente een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken voor algemene onderwerpen zoals datalekken, maar ook domeinspecifieke onderwerpen als gegevensdeling voor de uitvoering van de Jeugdwet of de Wet maatschappelijke ondersteuning 2015.

Naast dit door het college vastgestelde privacybeleid is een informatiebeveiligingsbeleid vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

Verantwoordelijkheid van iedere werknemer, bestuurder en raadsleden
Iedereen werkzaam 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 dit privacybeleid worden opgevolgd en actief worden uitgedragen.

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

Dit privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens door of namens 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.

6. Principes voor de verwerking van persoonsgegevens
De AVG 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.

a Rechtmatige grondslag
Persoonsgegevens worden door de gemeenten slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

De gemeenten kunnen dit toetsen door middel van een ingebouwde risicoparagraaf in de besluitvormingsprocedure.

b Welbepaalde doeleinden
De gemeenten verwerken persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat de gemeenten alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken. De gemeente ziet af van de verwerking als het doel op een minder ingrijpende wijze kan worden bereikt, bijvoorbeeld door minder of geen persoonsgegevens te verwerken.

c Verdere verwerking
Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, of dat hiervoor extra waarborgen zijn 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.

d Minimale gegevensverwerking
Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest de gemeente bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden bereikt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest de gemeente bij voorkeur voor die mogelijkheid.

e Juiste en actuele gegevens
De gemeente zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzameld zijn of vervolgens worden verwerkt. De gemeente neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

f Gegevens worden op tijd vernietigd
De gemeente stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens worden dan niet langer bewaard dan noodzakelijk. De gemeente bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

g Integriteit en vertrouwelijkheid
De gemeente neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. De gemeente handelt hierbij in overeenstemming met het informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid verplicht de gemeente om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

De gemeente komt haar verplichting om technische en organisatorische maatregelen verder na door sectorspecifiek beleid (waaronder de Wet politiegegevens en het Sociaal Domein) op te stellen, haar personeel bewust te maken over gegevensbescherming, control-momenten in te bouwen in haar processen, en periodiek te controleren of de verwerkingen voldoen aan wet- en regelgeving.

Het is medewerkers niet toegestaan om persoonsgegevens die de gemeente onder zich heeft op te slaan op apparaten die niet door de gemeente worden beheerd of zijn goedgekeurd.

h Privacy by Default en Privacy by Design
De gemeente houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om tot een zo optimaal mogelijke bescherming van persoonsgegevens te komen. Dit uitgangspunt wordt Privacy by Design (PbD) genoemd. De gemeente draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

i Toegang tot gegevens
Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen de gemeente geldende beleid voor toegang tot gegevens, waaronder het informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

j Inbreuk in verband met persoonsgegevens
Bij toegang tot, verlies of wijziging van persoonsgegevens bij de gemeente, zonder dat dit de bedoeling is, is er sprake van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. De gemeente registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het protocol datalekken.

k Samenwerking
De gemeente schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

l Samenwerkingsverbanden
Verder kan het voorkomen dat de gemeente samenwerkt met andere (overheids)organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersver-

antwoordelijken (gezamenlijk of individueel). De gemeente maakt met deze organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Derden waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

m Doorgifte buiten de EER
Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, geschiedt alleen in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

n Transparantie
De gemeente informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt de gemeente van deze informatieplicht af.

o 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 uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid.

p Geschillenbeslechting
Indien de betrokkene van mening is dat de gemeente niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij contact opnemen met de privacy officers of de Functionaris Gegevensbescherming (FG). Meer informatie over privacybescherming is te vinden op heuvelrug.nl.
De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP), met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens (meer informatie is te vinden op autoriteitpersoonsgegevens.nl).

q Verantwoording
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. De AP houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de FG. De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

r Verwerkingsregister
De gemeente beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

s Gegevenseffectbeoordeling (GEB) of DPIA
Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet de gemeente een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. De gemeente voert in dat geval een gegevenseffectbeoordeling uit (meestal DPIA genoemd). Dat is een onderzoek naar de gevolgen voor privacy. Als uit de DPIA blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging[1] genoemd.

t Functionaris gegevensbescherming (FG)
De gemeente is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. De gemeente is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke intern toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het college van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

u 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

1) https://autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/voorafgaande-raadpleging

gemeente weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, 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. Dat is manier om continu te verbeteren aan de hand van een vaste structuur.

Daarnaast gebruikt de gemeente het borgingsproduct van de Vereniging Nederlandse Gemeenten (VNG) als het beoordelingskader voor het waarborgen van compliance op het gebied van de gegevensbescherming binnen de gemeente (dat de gemeente voldoet aan de wet- en regelgeving). Het borgingsproduct is een normenkader wat door de gemeente gebruikt wordt voor het duiden van privacyrisico's en de daarbij behorende beheersmaatregelen binnen de gemeente.

v Bewustwording
Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies en opleidingen. Dit gebeurt passend binnen de context van en bij het domein waarbinnen de gegevens worden verwerkt.

w Wet- en regelgeving
Op het onderhavig beleid is, onder meer, de volgende wet- en regelgeving van toepassing:
- AVG (Algemene Verordening Gegevensbescherming).
- UAVG (Uitvoeringswet Algemene Verordening Gegevensbescherming).
- Awb (Algemene wet bestuursrecht).
- Gemeentewet.
- Archiefwet.

7. Rollen en Verantwoordelijken
Het governancemodel van de gemeente (besturen en beheersen van de organisatie) biedt een overkoepelende visie en strategie van hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en verantwoordelijkheden van het college van B&W, het managementteam en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy Officer en de Chief Information Security Officer (CISO: de functionaris voor het informatiebeveiligingsbeleid).

	Verantwoordelijk	
R	Responsible **Feitelijk verantwoordelijk**	• Management en teamleiders • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable **Eindverantwoordelijk**	• Het college van B&W
C	Consulted **Adviserend**	• Privacy Officer • CISO/ISO • FG
I	Informerend **Geï nformeerd**	• Gemeenteraad (bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

College van B&W
Het college is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente. Het college heeft de volgende rollen en verantwoordelijkheden:
– Eindverantwoordelijk voor de naleving van de privacywetgeving binnen de gemeente;
– Stelt het privacybeleid vast;
– Geeft sturing aan privacybeleidsvoering en legt rekenschap af over privacybeleidsvoering aan de FG;
– Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
– Bevordert duurzame privacycultuur.

Management

Het management is eindverantwoordelijk voor de naleving van de privacywetgeving binnen de Thema's, alsmede voor de uitvoering van het privacybeleid.

Het management heeft de volgende rollen en verantwoordelijkheden:
- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen het eigen thema;
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen het eigen thema;
- Informeert de FG op welke manier het eigen thema compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door werknemers binnen het eigen thema;
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingenregister voor zover dit betrekking heeft op het eigen thema;
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Aansturen van de privacy officers, voor zover benoemd binnen het eigen thema;
- Bevordert duurzame privacycultuur;
- Wint bij nieuwe of gewijzigde verwerkingen van persoonsgegevens altijd advies in bij de privacy officer en/of FG. Het management wordt daarbij geholpen door de "privacy-paragraaf" dat ingebouwd is in de besluitvormingsprocedure.
- Verantwoordelijk voor het treffen van mitigerende maatregelen en het accepteren van restrisico's. Bij afwijking van advies van de privacy officer en/of FG, wordt de afwijking schriftelijk gemotiveerd door het management.
- Verantwoordelijk voor privacyrisicomanagement, ondersteund door deskundige.
- Verantwoordelijk voor de beoordeling van privacyrisico's bij alle inkoop/aanbesteding van producten en diensten. Privacy-criteria en richtlijnen worden opgenomen in de inkoopvoorwaarden, getoetst voordat een overeenkomst wordt gesloten en opgenomen in de verwerkersovereenkomst

Functionaris Gegevensbescherming (FG).
Op basis van de AVG is het aanstellen van een FG verplicht voor de gemeente. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie. De FG heeft de volgende rollen en verantwoordelijkheden in de gehele organisatie van de gemeente:
- Interne toezichthouder op de naleving van de AVG namens de AP;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;
- Informeert en adviseert bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacyrisico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het college van B&W.

Privacy Officer
De privacy officer (privacy adviseur) is het eerste aanspreekpunt voor de gemeente rondom vraagstukken over gegevensbescherming, en heeft een monitorende en ondersteunende functie bij het naleven en uitvoeren van het privacybeleid. De privacy officer heeft de volgende rollen en verantwoordelijkheden:
- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van gegevenseffectbeoordeling (GEB) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;

– Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
– Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
– Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit of laat deze ontwikkelen en uitvoeren;
– Adviseert de verwerkingsverantwoordelijke over privacy by design & default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
– Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

Andere rollen en verantwoordelijkheden

Afdeling	Betrokkenheid
Juridische Zaken	Ondersteunen van de privacy officer over privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten.
CISO	Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens. Adviseren van de organisatie bij datalekken (volgens de meldprocedure). Tijdig melden van informatiebeveiligingsincidenten bij PO/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken. Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure)
Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).
Privacy ambassadeurs/contactpersonen	De privacy contactpersoon is het eerste aanspreekpunt binnen het thema waar deze contactpersoon werkzaam is en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.

Hoofdstuk 2 Privacybeleid sociaal domein Utrechtse Heuvelrug

1. Inleiding

Dagelijks gebruikt de gemeente Utrechtse Heuvelrug veel persoonsgegevens om het werk te kunnen doen. Het sociaal domein gebruikt niet alleen veel gegevens, maar ook bijzondere persoonsgegevens over de gezondheid. Dit vraagt veel van die medewerkers om goed en zorgvuldig te handelen. Zeker in het sociaal domein zijn cases waar gegevensdeling en privacy aan de orde zijn niet altijd "zwart-wit". In dit privacybeleid sociaal domein proberen wij helderheid te verschaffen over het gewenst gedrag bij het verwerken van persoonsgegevens binnen het sociaal domein.

2. Wat is gegevensbescherming?

Privacy is een grondrecht en verankerd in verschillende verdragen en verordeningen. Het is een voorwaarde om vrij te zijn in wie je bent en wat je doet en om regie te houden op je gegevens. Bescherming van het recht op privacy is niet alleen een zaak van de persoon zelf, maar ook van organisaties die persoonsgegevens verwerken. De gemeente is daar geen uitzondering op. Inwoners en organisaties ontkomen er vaak niet aan om persoonsgegevens te verstrekken, omdat de gemeente haar (wettelijke) taak moet uitvoeren.

3. Wat zijn de algemene uitgangspunten en doelen?

Regels waar de gemeente zich aan wil (en moet) houden en de rechten en plichten van betrokkenen zijn voor een belangrijk deel uitgewerkt in de Algemene Verordening Gegevensbescherming (de AVG) en in algemeen privacybeleid.

Met bepaalde privacy-eisen krijgt iedere medewerker in meer of mindere mate te maken. Bijvoorbeeld:
- De gemeente verwerkt persoonsgegevens rechtmatig, dat wil onder meer zeggen dat er een goede reden (grondslag) is om de gegevens te mogen verwerken.
- De gemeente gaat behoorlijk om met persoonsgegevens. Dit betekent dat de gemeente technische en organisatorische maatregelen neemt om persoonsgegevens te beschermen. Bijvoorbeeld: clean desk (zo min mogelijk op het bureau) en maatregelen om hacken te voorkomen.

- De gemeente is transparant over wat zij doet met persoonsgegevens (privacyverklaring op de gemeentelijke website).
- Persoonsgegevens mogen alleen voor bepaalde, uitdrukkelijk beschreven en gerechtvaardigde doelen worden verzameld (dat heet "doelbinding").
- Gegevensverwerkingen moeten minimaal zijn en noodzakelijk (proportionaliteit en subsidiariteit).
- Betrokkenen hebben rechten om invloed uit te oefenen en grip te houden op hun persoonsgegevens.

De betrokkene blijft altijd eigenaar van zijn of haar persoonsgegevens. Met een rechtmatige grondslag mag de gemeente slechts (tijdelijk) inbreuk maken op het recht op privacy van een betrokkene.

4. Hoe kijkt de gemeente Utrechtse Heuvelrug hier tegenaan?
Gemeenten uit de regio Zuidoost Utrecht hebben hun algemene uitgangspunten en doelen uitgewerkt in regionaal privacybeleid. In dit regionale beleid staat onder meer dat:
- Betrokkenen het vertrouwen moeten hebben dat hun persoonsgegevens in veilige handen is bij de gemeenten en daarom maatregelen moeten worden getroffen.
- De gemeenten transparant zijn over hoe zij persoonsgegevens beschermen en voldoen aan geldende eisen.
- Respect voor de persoonlijke levenssfeer van betrokkene(n) voorop staat.

5. Het sociaal domein heeft te maken met extra regels en uitgangspunten
De gemeente heeft veel verschillende verantwoordelijkheden en taken uit te voeren. Deze veelheid en veelzijdigheid laat zich ook voelen op het gebied van privacy. Sommige gemeentelijke teams verwerken nauwelijks persoonsgegevens terwijl andere teams dagelijks grote hoeveelheden persoonsgegevens verwerken. Voor sommige teams is aanvullend beleid handig om medewerkers goed in staat te stellen het werk zorgvuldig uit te voeren. Voor het sociaal domein is zulk aanvullend beleid ontwikkeld.

Het "sociaal domein" omvat meerdere sectoren. Ondersteuning bij werk, participatie en zelfredzaamheid in de maatschappij, zorg en jeugd vallen allemaal onder het sociaal domein.

6. Vuistregels
Medewerkers in het sociaal domein komen in aanraking met veel persoonsgegevens. Naast meer algemene persoonsgegevens worden ook bijzondere persoonsgegevens verwerkt, zoals gezondheidsgegevens, medische gegevens en het Burgerservicenummer (verder: het BSN). De hoeveelheid gegevens en het gevoelige karakter ervan vragen een groter privacybewustzijn van medewerkers in het sociaal domein. Onderstaande vuistregels zijn daarom van belang voor gebruik in de dagelijks praktijk. Het gaat immers om persoonsgegevens van vaak kwetsbare mensen, waar (extra) zorgvuldig mee om moet worden gegaan.

A. Wat is de regelgeving?
Wetten in het sociaal domein kennen soms eigen regels over hoe om moet worden gegaan met persoonsgegevens. Deze regels zijn vaak een aanvulling op of verduidelijking van de algemene regels uit de AVG. De Jeugdwet heeft bijvoorbeeld in hoofdstuk 7 veel regels opgenomen over gegevensverwerking, privacy en toestemming. Van medewerkers wordt verwacht dat zij bekend zijn met deze wet- en regelgeving.

B. Gerechtvaardigd doel?
Persoonsgegevens mogen alleen verwerkt worden voor een gerechtvaardigd doel. Het doel moet specifiek zijn en vooraf zijn omschreven (in het kader van de Jeugdwet en de Wmo 2015 bijvoorbeeld het behandelen van aanvragen). Gegevens mogen niet ineens worden gebruikt voor een heel ander doel dan waarvoor de gegevens zijn verzameld.

C. Noodzakelijk?
Alleen persoonsgegevens die noodzakelijk zijn voor de uitvoering van de (wettelijke) taak mogen verwerkt worden. Als persoonsgegevens niet noodzakelijk zijn, worden ze niet verwerkt. Als een afweging wordt gemaakt of bepaalde persoonsgegevens nodig zijn en er wordt gedacht aan woorden als "handig, praktisch, fijn, behulpzaam", dan is de verwerking meestal niet noodzakelijk.
Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het zijn dus alle gegevens waarmee je een uniek persoon kunt herleiden. Denk aan een naam, een identificatienummer, (online) locatiegegevens, fysieke kenmerken van een persoon of een kenteken van een auto.

D. Wat is verwerken?
In het sociaal domein worden al snel persoonsgegevens verwerkt. Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorsturen, verspreiden of op andere wijze ter beschikking stellen of combineren, afschermen, wissen of vernietigen van gege-

vens, dat is allemaal verwerken. Ook een telefoongesprek van een medewerker met een collega over een cliënt valt dus onder het verwerken van persoonsgegevens.

E. Bijzondere persoonsgegevens
Bijzondere persoonsgegevens worden alleen verwerkt als dit in de wet is bepaald. Gevoelige gegevens, bijvoorbeeld over iemands ras, godsdienst of gezondheid worden bijzondere persoonsgegevens genoemd. Deze zijn in de AVG extra beschermd. Binnen het sociaal domein kom je verschillende bijzondere persoonsgegevens tegen, bijvoorbeeld gezondheidsgegevens en strafrechtelijke gegevens. Artikel 7.4.0 van de Jeugdwet geeft bijvoorbeeld aan wanneer strafrechtelijke gegevens mogen worden verwerkt. Bijzondere persoonsgegevens worden alleen gebruikt als dit noodzakelijk is voor de uitvoering van de wettelijke taak en ze worden niet gedeeld.

F. Omgaan met een identiteitsbewijs
Voor de uitvoering van de wettelijke taak moet de gemeente vaak de identiteit vaststellen van een aanvrager of verzoeker. Hiervoor is het niet altijd nodig een kopie van het identiteitsbewijs te bewaren. Het is niet de bedoeling om identiteitsbewijzen in de computersystemen op te slaan. In principe moeten kopieën van identiteitsbewijzen direct na de identificatie van de persoon worden vernietigd.

G. Anonimiseer
Informatie wordt indien mogelijk anoniem verwerkt. Casussen die door medewerkers van de gemeente besproken worden, kunnen vaak worden geanonimiseerd door namen en adressen weg te laten.

H. Een leeg bureau
Een “clean desk” is uitgangspunt. De papieren dossiers worden opgeborgen in een afgesloten kast als er niet mee wordt gewerkt. De beeldschermen worden vergrendeld bij verlaten van de werkplek (op kantoor en bij thuiswerken).

I. Rechten van betrokkenen
De AVG kent betrokkenen verschillende rechten toe, zoals het recht op inzage in een dossier. Een verzoek kan mondeling, schriftelijk of digitaal worden gedaan. In het sociaal domein kan bij een beroep op deze AVG-rechten de leeftijd van een verzoeker of betrokkene belangrijk zijn. Kinderen vanaf twaalf jaar kunnen bijvoorbeeld zelfstandig een verzoek indienen om inzage te krijgen, tenzij het kind niet in staat is tot een ‘redelijke waardering van zijn belangen’. Tot het kind zestien jaar is hebben daarnaast de ouders met gezag recht op inzage in het dossier van hun kind. Pas vanaf zestien jaar oefenen kinderen volledig zelfstandig hun privacyrechten uit.

J. Informatie over derden
Een Wmo- of jeugdhulpdossier kan informatie bevatten over anderen dan de aanvrager zelf, zoals een vader of moeder. Als één van deze betrokkenen verzoekt om inzage, betekent dat niet dat hij of zij ook zomaar inzage krijgt in persoonsgegevens van anderen. Andere persoonsgegevens moeten worden weggelaten of er moet toestemming worden gevraagd aan de andere betrokkene(n) om deze te mogen delen.

K. Als informatie in verkeerde handen komt (datalek)
Ondanks alle zorgvuldigheid en voorzorgsmaatregelen kan het gebeuren dat een datalek ontstaat. Een datalek moet worden gemeld via het datalekkenprotocol van de gemeente. Het naar een verkeerd adres versturen van een brief of e-mail kan al een datalek betekenen.

L. Bewaren van documenten
De gemeente heeft bepaald waar documenten moeten worden opgeslagen en welke applicaties mogen worden gebruikt. Dossiers mogen niet worden opgeslagen in privé-omgevingen of op eigen apparaten. Met het bewaren van te veel persoonsgegevens neemt het risico op datalekken of andere beveiligingsincidenten toe.

M. Veilig e-mail versturen
E-mails, al dan niet met bijlagen, moeten met een beveiligde applicatie worden verstuurd.
E-mails bevatten vaak veel persoonsgegevens, zeker als sprake is van een omvangrijke e-mailwisseling of bijlagen. Telkens moet goed worden afgewogen of en wat er moet worden verstuurd per e-mail. Ook moet iedere keer goed worden gecheckt of het juiste e-mailadres wordt gebruikt om datalekken te voorkomen.

7. Rollen en verantwoordelijkheden
Binnen het sociaal domein is het college van burgemeester en wethouders eindverantwoordelijk voor de juiste en zorgvuldige naleving van de AVG. Het managementteam is verantwoordelijk voor de sturing op het naleven van de privacyregels. Dit betekent onder meer het inzichtelijk maken van de risico’s die

kleven aan verwerkingen, het daadwerkelijk invoeren van technische en organisatorische maatregelen om het werk juist en veilig te kunnen doen en het monitoren van de nakoming ervan.

Van medewerkers wordt verwacht dat zij regels en afspraken op het gebied van privacy naleven in de uitvoering van het werk en gebruik maken van de aangeboden tools.

8. Naleving
De naleving van het privacybeleid gebeurt ten eerste bij "incidenten". Als een betrokkene een beroep doet op een van de AVG-rechten of bij de melding van een datalek, beoordelen we wat er is gebeurd en of het privacybeleid is nageleefd.

De FG beoordeelt jaarlijks vanuit de toezichthoudende rol of de gemeente zich houdt aan het privacybeleid en of we werken volgens de regels uit de AVG. Als dat niet het geval is, doet de FG aanbevelingen om zaken te verbeteren. De FG brengt het jaarlijkse advies uit aan het Managementteam en het college over de naleving van de privacyregels.

9. RIVACY-UITGANGSPUNTEN VAN DE UTRECHTSE HEUVELRUG

1. Wij respecteren de rechten van de inwoner/cliënt.
2. Wij informeren de inwoner/cliënt dat we samenwerken binnen het sociaal domein. Wij werken integraal wanneer dat nodig is.
3. Persoonlijke gegevens van de inwoner/cliënt beschouwen we als strikt vertrouwelijk. Dat zorgt ervoor dat we de drempel van de toegang tot de hulp- en zorgverlening laag houden en de kwaliteit hoog.
4. Wij vertrouwen elkaar in onze deskundigheid en professionaliteit.
5. Wij vragen nooit meer persoonsgegevens dan strikt noodzakelijk.
6. Wij zijn altijd transparant over het doel waarvoor wij (persoons-)gegevens vragen.
7. Wij respecteren de positie en eigen verantwoordelijkheid van de professional aan wie wij vragen om gegevens over een inwoner/cliënt te verstrekken.
8. Wij maken altijd een zorgvuldige afweging of het mogelijk is om gegevens te verstrekken in het belang van de inwoner/cliënt.
9. Wij vertrouwen erop dat een andere professional een zorgvuldige afweging heeft gemaakt om wel of geen gegevens te vragen of te verstrekken.
10. Wij voelen ons verantwoordelijk om bij te dragen aan oplossingen voor het probleem van een inwoner/cliënt, ook als bepaalde gegevensuitwisseling niet mogelijk is.

Hoofdstuk 3 Privacybeleid Wet politiegegevens Utrechtse Heuvelrug

1. Inleiding
Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente heeft in haar privacybeleid en informatiebeveiligingsbeleid vastgelegd hoe zij omgaat met de bescherming van persoonsgegevens.
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 wat onderlinge verschillen.

Zo kent de Wpg 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 en zijn er in de Wpg aanvullende beperkingen en uitzonderingen op de in de AVG geldende privacyrechten van betrokkenen. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen 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 moeten elk jaar interne audits worden gehouden.

Het huidige privacybeleid van de gemeente gaat alleen uit van de AVG. Het is daarom wenselijk er de verplichtingen uit de Wpg aan toe te voegen.

2. Doelstellingen van het privacybeleid
Het privacybeleid van de gemeente beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor be-

scherming van persoonsgegevens uit de Wpg en de genoemde regelingen. De gemeente wil met dit addendum op het privacybeleid onder andere bereiken dat de boa's:

- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële en imagoschade minimaliseren.

3. Wpg-kader

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt 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 te maken 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. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De hierna genoemde verplichtingen uit de Wpg zijn veelal geborgd binnen onze applicaties:

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en gegevens die op een persoonlijk oordeel zijn 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 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 uit het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van externe privacy-audits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de Autoriteit Persoonsgegeven (AP). Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een hercontrole plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

4. Register van verwerkingen

Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

5. Informatiebeveiligingsbeleid
Het informatiebeveiligingsbeleid is een richtinggevend en kaderstellend beleidsdocument. De gemeente vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.
Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

6. FG en bevoegd functionaris
De Functionaris Gegevensbescherming (FG)
Net als de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

De bevoegd functionaris
De bevoegd functionaris is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben. De bevoegd functionaris heeft onder andere de volgende taken:
- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevens rechtmatig worden verkregen en verwerkt.

7. Rechten van betrokkenen
De rechten van betrokkenen onder de AVG staan beschreven in het privacybeleid van de gemeente. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend.

8. Het bewaren van politiegegevens
Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

Politiegegevens dienen na verwijdering nog maximaal vijf jaar te worden bewaard. Daarna, of binnen deze periode van vijf jaar (afhankelijk van welke bewaartermijn geldt) dient definitieve vernietiging plaats te vinden. Indien sprake is van een cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.

Alle politiegegevens worden gelabeld in artikel 8, 9 en 13-informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

9. Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan.

Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Hierbij moet altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, als dit echt noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Wanneer gegevens verstrekt worden, moet er voldaan worden aan de documentatieplicht. Bovendien mag alleen verstrekt worden in overeenstemming met het bevoegd gezag indien

dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet Bibob.

10. Het melden van datalekken
De datalekprocedure is op hoofdlijnen gelijk aan die op grond van de AVG. Specifiek voor de Wpg geldt nog het volgende:
Op de mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven 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.

11. Bewustwording
Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Elke nieuwe BOA moet daarom een Wpg-training volgen. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Boa's die al in dienst zijn en deze training nog niet hebben doorlopen, doorlopen deze training alsnog. Daarnaast is er in ieder geval jaarlijks aanvullend aandacht voor bewustwording rondom de omgang met politiegegevens. Dit kan bijvoorbeeld in de vorm van een aanvullende training, een bijeenkomst over een specifiek Wpg-onderwerp of in de vorm van een toets. Ook van deelname aan deze initiatieven wordt een notitie in het personeelsdossier gemaakt.

12. Open communicatie
Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze zij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring die op de website is te vinden.

Hoofdstuk 4 Slotbepalingen

Slotbepalingen
1. Het Regionaal Privacybeleid van 24 september 2019 wordt ingetrokken.
2. Dit beleid treedt in werking op de dag na bekendmaking.
3. Dit beleid kan worden aangehaald als 'Regionaal Privacybeleid Utrechtse Heuvelrug 2024-2028".
4. Dit beleid wordt in elk geval elke vier jaar, gerekend vanaf de inwerkingtreding, geëvalueerd en zo nodig aangepast.

Aldus vastgesteld in de vergadering van het college van burgemeester en wethouders van de gemeente Utrechtse Heuvelrug van 16 juli 2024.

het college van burgemeester en wethouders van de gemeente

de secretaris,
de burgemeester,