Regionaal Privacy beleid

gemeente Utrechtse Heuvelrug

Datum

Versie: 1.0

Vastgesteld: 24 september 2019

Inhoudsopgave

1 Regionale samenwerking

De gemeenten, De Bilt, Bunnik, Wijk bij Duurstede, Utrechtse Heuvelrug en Zeist werken al veel regionaal samen, onder andere op het gebied van ICT, informatiebeveiliging en binnen het Sociaal Domein. Als gevolg daarvan hebben deze gemeenten veel gemeenschappelijke raakvlakken en overeenkomsten in de werkprocessen waarbij persoonsgegevens worden verwerkt. De maatregelen die nodig zijn om binnen deze gemeenten de gegevensbescherming te kunnen borgen zullen daarom ook grotendeels overeenkomen. Daarom is ervoor gekozen om ook op het gebied van gegevensbescherming regionaal samen te werken. Met de regionale invulling van de functie van de Functionaris Gegevensbescherming is daarvoor de eerste stap gezet. Met een regionaal privacy beleid willen de regiogemeenten de samenwerking verder uitbreiden. Dit regionale privacy beleid bevat een visie op privacybescherming, het wettelijk kader, de organisatie van privacybescherming in de desbetreffende gemeente en de maatregelen die in de samenwerkende gemeenten zijn en worden genomen om privacy te beschermen.

1.1 Doel van het regionaal privacy beleid

De besturen en de medewerkers van de gemeenten in de regio Zuid Oost Utrecht hechten er veel waarde aan dat de verwerkingen van persoonsgegevens in overeenstemming is met de wet en dat die verwerkingen zorgvuldig, rechtmatig en veilig plaatsvinden.
Door uitvoering te geven aan de richtlijnen die in dit regionale privacy beleid zijn beschreven worden de inwoners van de gemeenten in de regio Zuid Oost Utrecht beschermd tegen risico's van de informatiemaatschappij en worden de gemeentelijke afbreuk- en aansprakelijkheidsrisico's beheerst.
Dit beleid biedt een basis voor andere regionale documenten voor de bescherming van persoonsgegevens, zoals uitvoeringsplannen, richtlijnen of procedures (zie figuur 1).

1.2 Couleur locale

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' in hoofdstuk 4. Maar ook hoofdstuk 5 over de maatregelen ter bescherming van persoonsgegevens hebben de afzonderlijke gemeenten waar nodig aangepast op hun eigen organisatie.

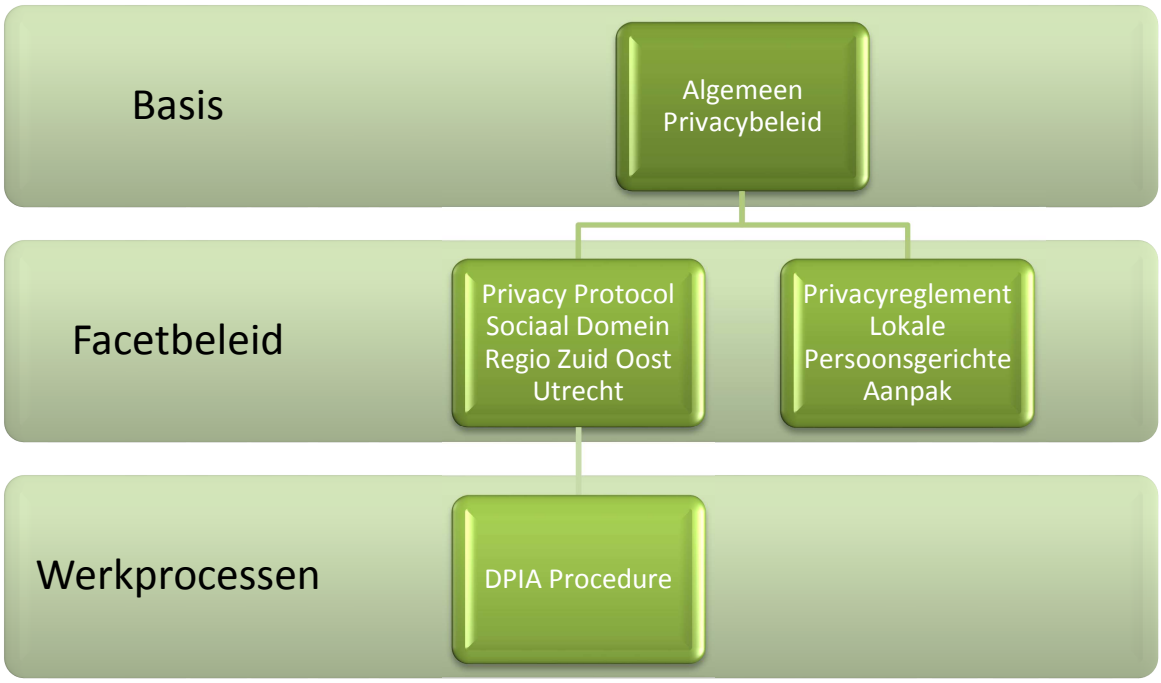
1.3 Reikwijdte van het regionaal privacy beleid

Dit algemeen regionale privacy beleid gemeente Utrechtse Heuvelrug geldt voor alle medewerkers, bestuurders en raadsleden die werkzaam zijn voor de gemeente Utrechtse Heuvelrug en is van toepassing op alle verwerkingen van persoonsgegevens waarvan de gemeente Utrechtse Heuvelrug de verwerkingsverantwoordelijke is. Het beleid geldt ook voor de verwerkers die namens de gemeente persoonsgegevens verwerken.

1.4 Relatie met informatieveiligheidsbeleid

Het kunnen borgen van de privacy kan niet gerealiseerd worden zonder adequate informatiebeveiliging. Het algemeen privacy beleid hangt daarom ook samen met het Informatiebeveiligingsbeleid. Het Informatiebeveiligingsbeleid is vastgesteld door het college van burgemeester en wethouders en is gebaseerd op de landelijke richtlijnen daarvoor die zijn vastgelegd in de Baseline Informatieveiligheid Overheid (BIO). In het Informatiebeveiligingsbeleid staan onder meer de beveiligingseisen die gelden voor informatiesystemen, gedragscodes en richtlijnen hoe de ambtelijke organisatie moet omgaan met privacygevoelige informatie en de fysieke maatregelen die daarvoor noodzakelijk zijn[1]

[1] Denk hierbij aan toegang tot kantoorruimtes, afsluiten van kasten etc.



Figuur 1

1.5 Begripsbepalingen

In dit regionale privacy beleid worden de volgende begrippen en afkortingen gebruikt:

Persoonsgegevens
de gegevens over een geïdentificeerde of identificeerbaar persoon, Zoals een naam, adresgegevens of een e-mailadres. Maar ook indirecte gegevens kunnen persoonsgegevens zijn, zoals bijvoorbeeld een kentekenplaat op een voertuig of een Burgerservicenummer (BSN), als het maar herleidbaar is tot een natuurlijk persoon.

Betrokkene
De persoon op wie de persoonsgegevens betrekking hebben.

Verwerken van persoonsgegevens
alle handelingen die met persoonsgegevens uitgevoerd worden zoals het verzamelen, vastleggen, bewaren, wijzigen, opvragen, gebruiken en inzien[2].

Verwerkingsverantwoordelijke
de natuurlijke of rechtspersoon, een overheidsinstantie of een dienst of orgaan die/dat alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Voor dit beleid is dat de gemeente.

AP
Autoriteit Persoonsgegevens: de landelijke toezichthoudende autoriteit.

AVG
De Europese Algemene verordening gegevensbescherming die in de lidstaten rechtstreeks van toepassing is.

[2] Voor de volledige omschrijving zie artikel 4 AVG

CISO
De Chief information security officer: de functionaris die informatieveiligheid in de gemeente coördineert, aanstuurt en initieert.

DPIA
Data privacy impact assessment: gegevensbeschermingseffectbeoordeling van de verwerking van persoonsgegevens in informatiesystemen of op andere wijze.

FG
Functionaris voor gegevensbescherming: de onafhankelijke controleur en adviseur die door de samenwerkende gemeenten is aangesteld.

PO
Privacy officer: de functionaris in dienst bij de gemeenten die zorgdraagt voor de uitvoering van het privacy beleid.

2 Regionale 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 privacy schending 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.

3 Wettelijk kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. Voorkomen moet worden dat er onnodige of te vergaande inbreuken worden gemaakt. De Algemene Verordening Gegevensbescherming, hierna: AVG biedt hiervoor het wettelijk kader. De AVG heeft als doel om de privacy van alle Europese burgers te beschermen. Dit regionale privacy beleid vindt zijn grondslag in artikel 24 AVG.

Artikel 24 AVG:

1. Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

2. Wanneer zulks in verhouding staat tot de verwerkingsactiviteiten, omvatten de in lid 1 bedoelde maatregelen een passend gegevensbeschermingsbeleid dat door de verwerkingsverantwoordelijke wordt uitgevoerd.

De AVG bevat in principe geen concrete verplichtingen waarmee aan artikel 24 wordt voldaan. De verwerkingsverantwoordelijken hebben zelf de verantwoordelijkheid om zodanig passende maatregelen te treffen dat de persoonsgegevens op een veilige wijze worden verwerkt en aan de beginselen van de AVG wordt voldaan. Deze beginselen van de verwerking van persoonsgegevens houden het volgende in:

- de verwerking van persoonsgegevens moet ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant zijn;
- persoonsgegevens mogen alleen worden verzameld voor een bepaald gerechtvaardigd doel en mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel (de eis van doelbinding);
- de verwerking van persoonsgegevens moet beperkt zijn tot wat noodzakelijk is voor het omschreven doel (minimale gegevensverwerking);
- de verwerkte persoonsgegevens moeten juist zijn; onjuist gebleken persoonsgegevens moeten worden gecorrigeerd of verwijderd;
- de persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het gerechtvaardigde doel waarvoor deze werden verwerkt. Hier zijn uitzonderingen op met het oog op het algemeen belang[3].
- persoonsgegevens moeten zodanig worden verwerkt dat een passende beveiliging ervan gewaarborgd is.

[3] Zie artikel 5 AVG

4 Organisatie van de gemeente

4.1 Organisatie gemeente Utrechtse Heuvelrug

De gemeentelijke organisatie bestaat uit een directie (een directeur en een adjunct directeur) met daaronder 6 thema's (Buitenruimte, Fundament, Koers, Omgeving, Publiek en Samenleving). Deze thema's worden geleid door themamanagers die samen het managementteam vormen. Binnen de hele organisatie worden persoonsgegevens verwerkt.

Gemeente Utrechtse Heuvelrug heeft als kernwaarden: omgevingsgevoelig, verantwoordelijk, dienstverlenend, samenwerken en zelfreflectie. In het verlengde hiervan vindt de gemeente het van groot belang en vanzelfsprekend dat goed wordt omgegaan met privacygevoelige gegevens. Dit is een kwestie van kwaliteit, klantgerichtheid, leefbaarheid en bestuurlijke integriteit in het digitale tijdperk. Iedereen mag er daarom op vertrouwen dat de gemeente persoonsgegevens volgens de wet en op een behoorlijke en zorgvuldige wijze verwerkt. Dat begint bij privacybewust gedrag van iedere medewerker. Het college ziet erop toe dat de gemeentelijke organisatie de privacywetgeving naleeft.

4.2 Verantwoordelijkheden

Het college van burgemeester en wethouders is eindverantwoordelijk voor gegevensverwerking, informatiebeveiliging en privacybescherming. Onderstaande tabel brengt de verantwoordelijkheden in beeld aan de hand van het RASCI-model:

	Verantwoordelijk	Rol
R	Responsible / Feitelijk verantwoordelijk	• Gemeentesecretaris (hoogste leidinggevende) • Themamanagers
A	Accountable / Eindverantwoordelijk	• Het college van B&W
S	Supporting / Uitvoerend	• Privacy officer • Privacy jurist • Applicatiebeheerders/beveiligingsbeheerders • Adviseur informatisering • Alle medewerkers
C	Consulted / Adviserend	• Privacy officer • Privacy jurist • Adviseur informatisering • FG (regionaal) • CISO (regionaal)
I	Informed / Geïnformeerd	• Gemeenteraad • Belanghebbenden/betrokkene(n)

Het college is als bevoegd gezag eindverantwoordelijk voor de bescherming van persoonsgegevens, de directeur/gemeentesecretaris is als hoogste leidinggevende eindverantwoordelijk voor de borging daarvan. Elke themamanager is verantwoordelijk voor de medewerkers binnen zijn of haar afdeling ten aanzien van de zorgvuldige verwerking van persoonsgegevens bij de uitoefening van hun taken.

De **Privacy Officer** (PO) implementeert de technische en organisatorische maatregelen die op grond van de AVG zijn vereist. Deze functionaris heeft ook een coördinerende functie voor datalekken en zorgt dat deze bij de Autoriteit Persoonsgegevens worden gemeld. De PO heeft een belangrijke rol in het bevorderen van privacy bewustzijn bij medewerkers. In die rol organiseert hij bewustwordingsactiviteiten. De PO is de eerste contactpersoon van de FG.

De **Privacy jurist** zorgt voor het opstellen van beleid en, samen met de PO, voor instructies, regelingen, procedures en processen. De Privacy jurist heeft een coördinerende functie bij de behandeling van verzoeken om uitoefening van rechten van betrokkenen.

Voor de uitvoering van de AVG is per applicatie een verantwoordelijkheid belegd voor de veilige verwerking van persoonsgegevens bij de **applicatiebeheerder** (ofwel de beveiligingsbeheerder zoals benoemd in het Informatieveiligheidsbeleid). Deze beheerder heeft de benodigde kennis van het informatiesysteem en signaleert eventuele risico's bij de verwerking van persoonsgegevens en meldt deze bij de Privacy Officer.

De **adviseur informatisering** heeft een organisatorisch/beleidsmatige functie op het gebied van informatieveiligheid. Deze werkt in die rol nauw samen met de CISO. De CISO en adviseur informatisering hebben geen specifieke verantwoordelijkheid voor de bescherming van privacy.

De **PO en Privacy jurist** en de **adviseur informatisering** hebben ook een interne adviserende functie.

De **CISO** adviseert op het gebied van veiligheid van informatiesystemen en treedt adviserend op naar aanleiding van beveiligingsincidenten. Ook heeft de CISO een adviserende en coördinerende rol in de bewustwording voor informatieveiligheid en werkt daarin samen met de PO.

De **FG** is de (regionale) onafhankelijke adviseur en toezichthouder die in de AVG wettelijk verplicht is gesteld voor een verwerkingsverantwoordelijke. Hij rapporteert c.q. adviseert aan de hoogste leidinggevende en/of het college, maar is ook lager in de organisatie raadpleegbaar.

De genoemde experts werken nauw met elkaar samen bij de opbouw van informatieveiligheid en privacybescherming.

4.3 Verantwoording aan de Gemeenteraad

Net zoals het college verantwoording moet afleggen over de gemeentelijk uitgaven, wordt ook verantwoording afgelegd over de realisatie van beleid. Dit geldt ook voor het privacy beleid en de toepassing daarvan. Het privacy beleid wordt om die reden onderdeel van de Planning & Control cyclus.
Met ingang van 2018 neemt het college in de jaarrekening een passage op over het gevoerde privacy beleid. Het college informeert de raad over belangrijke gebeurtenissen ten aanzien van gegevensverwerking. Te denken valt aan ernstige inbreuk op of verlies van persoonsgegevens. Binnen het college is de portefeuillehouder van Programma Bestuurlijke zaken van de Programmabegroting verantwoordelijk voor privacy.

5 Maatregelen

Met de maatregelen beschreven in dit hoofdstuk worden de privacy voorschriften nageleefd en de risico's worden beperkt.

5.1 Register van verwerkingsactiviteiten

Persoonsgegevens worden in de gemeente vrijwel alleen verwerkt voor het uitvoeren van wettelijke taken; de wet vormt in de meeste gevallen de rechtmatige grondslag voor de verwerking van persoonsgegevens. De persoonsgegevens worden alleen gebruikt voor het in de wet omschreven doel. Een overzicht van de verwerkingen van persoonsgegevens door de gemeente staan vermeld in het wettelijk verplichte register van verwerkingsactiviteiten. Daarin staan onder meer de aard van de gegevens, de rechtmatige grondslag en de bewaartermijn vermeld. Het register is in te zien op onze website.

5.2 Herkomst van de persoonsgegevens

In het merendeel van de gevallen worden persoonsgegevens door de betrokkene zelf verstrekt. Wanneer voor het uitvoeren van bepaalde wettelijke taken en regelingen persoonsgegevens verwerkt moeten worden, dan worden deze gegevens opgevraagd uit de basisregistratie personen. Dit is in overeenstemming met het principe van 'eenmalige uitvraag en meervoudig gebruik' dat door de overheid en de gemeente wordt gepropageerd.

5.3 Doel van de verwerking

Wat er precies met de verzamelde gegevens gebeurt, is afhankelijk van het doel waarvoor ze verzameld worden. De verwerking moet noodzakelijk zijn voor het doel dat daarvoor in de grondslag is omschreven. De persoonsgegevens worden op enkele uitzonderingen na, in een beveiligd zaaksysteem opgenomen waar ze alleen toegankelijk zijn voor de medewerkers die belast zijn met het uitvoeren van de taak.
Als een wettelijke grondslag ontbreekt, dan worden de persoonsgegevens alleen verwerkt met uitdrukkelijke toestemming van de betrokkene, voor een concreet omschreven doel.
Omdat alleen de minimaal noodzakelijke persoonsgegevens worden verwerkt waarvoor een rechtmatige grondslag bestaat, worden bijzondere persoonsgegevens die gaan over onder andere ras, gezondheid, geloofsovertuiging, biometrische gegevens[4] in principe niet verwerkt. Gegevens over gezondheid worden op grond van de Jeugdwet of de Wet maatschappelijke ondersteuning voor zover noodzakelijk wel verwerkt en zijn extra beveiligd.

5.4 Meldplicht datalekken

Een datalek is een inbreuk op de beveiliging, waarbij een kans bestaat dat dit ernstige nadelige gevolgen heeft voor de bescherming van de persoonsgegevens. Hierbij kan gedacht worden aan het kwijtraken van een USB stick met persoonsgegevens, inbraak door een hacker, maar ook onbevoegde autorisaties in een informatiesysteem.
De gemeente is verplicht om ernstige datalekken te melden bij de Autoriteit Persoonsgegevens (AP).
Het gaat hier om datalekken waar de gemeente voor verantwoordelijk is. Daaronder vallen ook datalekken die ontstaan bij een derde partij die werkzaamheden uitvoert namens de gemeente. Om datalekken zo snel mogelijk te ontdekken en de gevolgen daarvan te beperken heeft de gemeente een datalek protocol en -instructie voor medewerkers. Datalekken Om datalekken te voorkomen houdt de gemeente zich aan richtlijnen waaraan informatiesystemen moeten voldoen om gegevensbescherming te borgen.

[4] Zie artikel (9 t/m 11 AVG)

5.5 Bewust omgaan met persoonsgegevens

Voor het borgen van privacy is het met name van belang dat er bewust met persoonsgegevens wordt omgegaan. Om bewustwording te realiseren is kennisoverdracht nodig. De FG, Privacy officer, Privacy jurist CISO en de adviseur informatisering zorgen ervoor dat informatie over gegevensbescherming en informatiebeveiliging herhaaldelijk onder de aandacht wordt gebracht van themamanagers, teamleiders en medewerkers.

5.6 Dataminimalisatie

Zorgvuldig omgaan met persoonsgegevens betekent ook dat er niet meer gegevens worden uitgevraagd en verwerkt dan strikt noodzakelijk voor het doel van de verwerking. Dit is het zogenaamde dataminimalisatie principe. Dit principe wordt toegepast op alle processen en er wordt aandacht voor gevraagd bij de medewerkers.

5.7 Bewaren van gegevens

De AVG schrijft voor dat gegevens niet langer bewaard mogen worden dan noodzakelijk voor het doel waarvoor ze verwerkt zijn[5]. De bewaartermijnen van persoonsgegevens lopen hierdoor uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Daar waar er geen wettelijke regeling is die voorziet in een verplichte bewaartermijn, kan het college een besluit over de bewaartermijn nemen. Daarnaast geldt de Archiefwet voor het bewaren van papieren en elektronische documenten. De gemeente geeft gevolg aan de bewaartermijnen door periodiek vernietigingslijsten op te stellen van documenten waarvan de bewaartermijn is verstreken.

5.8 Toestemming

Als de rechtmatige grondslag van een verwerking van persoonsgegevens bestaat in de toestemming van de betrokkene, dan wordt de toestemming uitdrukkelijk gevraagd en kan deze op elk moment weer worden ingetrokken. Toestemming kan echter niet altijd als rechtmatige grondslag gelden als er geen wettelijke grondslag voor de verwerking bestaat. De gemeente houdt zich aan de wettelijke grondslagen en omzeilt deze niet door toestemming aan de betrokkene te vragen. Als het delen van persoonsgegevens op grond van de wet niet is geregeld maar wel gewenst is voor een optimale behandeling van een zaak, wat kan voorkomen bij de uitvoering van de Jeugdwet of de Wet matschappelijke ondersteuning, dan wordt concreet en per gewenste uitwisseling toestemming gevraagd van de betrokkene. Hierbij worden de aanbevelingen uit het onderzoeksrapport van de AP over de rol van toestemming[6] meegenomen.

5.9 Transparantie

Wij vinden het belangrijk dat betrokkenen erop kunnen vertrouwen dat wij zijn of haar persoonsgegevens zorgvuldig verwerken. Daarom hebben wij op onze website informatie over de verwerking van persoonsgegevens geplaatst (het register van verwerkingsactiviteiten, informatie over datalekken, informatie over de rechten van betrokkenen). Op onze webformulieren hebben wij ook informatie over de behandeling van persoonsgegevens opgenomen. Hierbij wordt duidelijk:

1. welke gegevens worden verzameld,
2. waarom deze gegevens worden verzameld,
3. wat vervolgens met deze gegevens gebeurt,
4. wie toegang heeft tot deze gegevens,
5. welke rechten inwoners en ondernemers hebben.

---

[5] Zie artikel 5 AVG

[6] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_de_rol_van_toestemming_in_het_sociaal_domein.pdf

5.10 Verwerking van persoonsgegevens door derden

Bij veel gemeentelijke processen worden persoonsgegevens namens de gemeente verwerkt door derden[7], dat worden verwerkers genoemd. Denk hierbij aan uitbestede werkzaamheden aan andere instanties of samenwerkingsverbanden. Het mandateren van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. Het college van burgemeester en wethouders blijft verantwoordelijk voor de verwerking van de gegevens door een verwerker. Wij moeten er daarom op toezien dat gegevens door de verwerkers juist verwerkt[8] en beveiligd worden.
Om aan de wettelijke vereisten te voldoen sluiten wij verwerkersovereenkomsten met de verwerkers. Daarin worden de beveiligingseisen opgenomen die ook voor de gemeente als verwerkingsverantwoordelijke gelden. Wij hanteren het model van de verwerkersovereenkomst van de Vereniging Nederlandse gemeenten/ Informatiebeveiligingsdienst (VNG/IBD) De gemeente heeft de bevoegdheid om de naleving van de verwerkersovereenkomst periodiek te controleren.

5.11 Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's bij het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn van de medewerkers voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Dat gebeurt vooral tijdens de werkprocessen zelf, door advisering van de PO en Privacyjurist, maar er vinden ook regelmatig terugkerende bewustwordingsactiviteiten plaats.

5.12 Data Privacy Impact Assessment

De systematische verwerking van persoonsgegevens kan een hoog risico voor de bescherming van persoonsgegevens inhouden. Met name geldt dit bij de toepassing van nieuwe technologieën voor de verwerking van persoonsgegevens.
De AVG schrijft in gevallen dat bij de verwerking van persoonsgegevens een hoog risico voor de rechten en vrijheden van natuurlijke personen zal bestaat of ontstaat, een gegevensbeschermingseffectbeoordeling voor, DPIA genoemd. De verwerkingsverantwoordelijke bepaalt wanneer een DPIA wordt gehouden. Omdat de verwerkingsverantwoordelijke hierin beoordelingsvrijheid wordt gegeven, heeft de AP richtlijnen gegeven om te bepalen of een DPIA nodig is. De samenwerkende gemeente hebben op basis daarvan een procedure opgesteld aan de hand waarvan wij bepalen of wij een DPIA uitvoeren. Deze DPIA procedure geeft ook aan wie binnen de organisatie een taak hebben voor het opstellen van een DPIA.

5.13 Dataclassificatie

De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen[9], zijn niet voor elk proces en informatiesysteem hetzelfde. Hierom is het nodig dat alle processen en informatiesystemen die gegevens verwerken een dataclassificatie ontvangen. Dataclassificatie heeft als doel om de continuïteit, integriteit en vertrouwelijkheid van het proces en het informatiesysteem te benoemen. Dit maakt inzichtelijk welke maatregelen genomen moeten worden om de gegevens die verwerkt worden te beschermen.
De CISO voorziet elk proces en informatiesysteem van dataclassificatie zoals deze is voorgeschreven door de landelijke Informatiebeveiligingsdienst[10]voor gemeenten.

5.14 Logging van gegevensgebruik

Elk geautomatiseerd systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. In deze logging staat minimaal vermeld welke gebruiker, op welke moment, welke gegevens heeft verwerkt,

---

[7] Zie voor betekenis artikel 4 AVG

[8] Zie artikel 32 AVG

[9] Denk hierbij aan encryptie van gegevens, bewaartermijnen, wachtwoord vereisten

[10] https://www.ibdgemeenten.nl/wp-content/uploads/2014/04/13-1018-handreiking-dataclassificatie.pdf

maar eventueel ook registratie van relevante gebeurtenissen die zich gedurende een periode in een verwerking hebben voordoen. Voor informatiesystemen met persoonsgegevens die een hoger beschermingsniveau vereisen, zoals gezondheidsgegevens en Burgerservicenummer is logging ingesteld.

5.15 Privacy by design en privacy by default

Privacy by design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant gebruiken van persoonsgegevens
- de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat de standaard instellingen in systemen zo zijn ingesteld dat privacybescherming maximaal is geborgd.

6 Rechten van betrokkenen

De AVG geeft rechten aan betrokkenen over de verwerking van hun eigen persoonsgegevens. Dit zijn onder meer het recht op informatie, inzage, wijziging, verwijdering, beperking. Er zijn twee nieuwe rechten. Ten eerste het recht om vergeten te worden, dat wil zeggen dat de verwerkingsverantwoordelijke (de gemeente) haar best moet doen om de persoonsgegevens van de verzoeker ook te (laten) verwijderen uit systemen buiten haar eigen organisatie. Ten tweede het recht op overdraagbaarheid van persoonsgegevens, wat inhoudt dat in sommige gevallen de persoonsgegevens in een overzichtelijk machine leesbaar document moeten worden verstrekt om te worden overgedragen aan een andere verwerkingsverantwoordelijke. Betrokkenen kunnen een verzoek doen om van hun recht gebruik te maken. Wij zijn ingericht op de meest voorkomende te verwachten verzoeken met een speciaal webformulier om zo'n verzoek in te dienen.

Onze website bevat informatie over elk recht, de wijze van gebruikmaking daarvan, de besluitvorming en de rechtsmiddelen daartegen.

7 Slotbepalingen

1. Dit beleid is vastgesteld op 24 september 2019
2. Het Algemeen privacybeleid Utrechtse Heuvelrug van [29 augustus 2017] wordt ingetrokken
3. Dit beleid kan worden aangehaald als 'Regionaal Privacy beleid gemeente **Utrechtse Heuvelrug**'
4. Dit beleid wordt bekend gemaakt in het gemeenteblad en gepubliceerd op de website www.heuvelrug.nl en
   treedt in werking op de dag na bekendmaking.
5. Dit beleid wordt elke twee jaar, gerekend vanaf de inwerkingtreding, geëvalueerd en zo nodig aangepast.

Het college van burgemeester en wethouders van gemeente Utrechtse Heuvelrug,

De secretaris

De burgemeester,