gemeente Heumen

GEMEENTEBLAD

Officiële uitgave van de gemeente Heumen

Nr. 109891

14 maart

2023

Privacybeleid gemeente Heumen

De raad van de gemeente Heumen in openbare vergadering bijeen;
gezien het voorstel en het besluit van burgemeester en wethouders d.d. 29 november 2022;
gelet op artikel 24 lid 2 van de Algemene Verordening Gegevensbescherming;

Besluit
Het geactualiseerde gemeentelijk privacybeleid (kenmerk 128409-129362) vast te stellen en dit beleid in werking te laten treden met ingang van 1 januari 2023, onder gelijktijdige intrekking van het huidige privacybeleid (kenmerk 26862-33426).

Inleiding

De gemeente verzamelt en verwerkt voor de uitvoering van diverse taken persoonsgegevens en slaat deze op ten behoeve van de dienstverlening aan haar inwoners en samenwerking met bedrijven en andere partners. De regels waaraan een gemeente moet voldoen staan in de Algemene Verordening Gegevensbescherming (AVG). De gemeente Heumen is bewust van het feit dat privacy geborgd moet worden. Met dit document wordt de vertaalslag gemaakt van geldende wet- en regelgeving naar de dagelijkse praktijk. Privacy is een onderwerp dat met de dag belangrijker wordt gezien de steeds digitaler wordende wereld waar we ons in bevinden. Ook gaat de gemeente steeds meer digitaal werken, wat meer eisen stelt aan de bescherming van (digitale) gegevens.

Dit privacybeleid is opgesteld voor alle medewerkers van de gemeente Heumen. Vrijwel alle medewerkers krijgen in de uitvoering van hun werkzaamheden te maken met persoonsgegevens. De gemeente wil een betrouwbare overheid zijn en blijven voor inwoners, bedrijven en andere partners. Dit betekent dat iedereen erop moet kunnen vertrouwen dat gegevens veilig zijn bij de gemeente. Zo draagt privacy bij aan het halen van onze gemeentelijke doelen en het bieden van goede dienstverlening.

In dit beleid wordt onder andere aangegeven op welke wijze een rechtmatige verwerking van persoonsgegevens plaatsvindt, hoe de AVG zich verhoudt tot de kernwaarden en daarvan afgeleide leidende principes van de gemeente Heumen, de wijze waarop de gemeente Heumen invulling geeft aan privacy in haar werkprocessen en waar hierbij de verantwoordelijkheden liggen.

Hoofdstuk 1 van het beleid gaat over de reikwijdte, uitgangspunten, doelstellingen en doelgroep van het beleid. Hoofdstuk 2 gaat in op de verschillende verantwoordelijkheden die in de organisatie zijn belegd. Hoofdstuk 3 zet de richtlijnen uiteen voor het werken volgens de AVG in de dagelijkse praktijk. In hoofdstuk 4 wordt aangegeven hoe de gemeente uiting geeft aan bewustwording in de organisatie over dit thema. Hoofdstuk 5 gaat over het opslaan, archiveren en vernietigen van persoonsgegevens en ten slotte wordt in hoofdstuk 6 de relatie tussen privacy en informatiebeveiliging uitgelegd.

De privacykernwaarden van Heumen
De zes uitgangspunten (paragraaf 1.3) uit de AVG zijn verbonden aan de leidende principes van Heumen en vertaald naar onderstaande privacykernwaarden:

Veiligheid
Gevoelige informatie over onze inwoners, medewerkers valt niet in verkeerde handen.

Transparantie
We zijn open over onze gegevensverwerking en verantwoorden onze overwegingen richting betrokken inwoners en toezichthouders.

Doelgerichte gegevensregistratie
We verwerken alleen de informatie die noodzakelijk is voor onze werkzaamheden.

Betrouwbaarheid
We zijn een betrouwbare partner voor onze inwoners en ketenpartners. Wij zijn proactief in het beschermen van hun rechten.

Dienstverlening
We zoeken actief de ruimte binnen de wetgeving om onze inwoners optimaal te kunnen bedienen.

Alertheid
Gegevensbescherming is een verantwoordelijkheid van ons allemaal. Elke medewerker is alert en maakt onderbouwde afwegingen en betrekt zo nodig de Functionaris Gegevensbescherming.

1. Doel van het beleid

In artikel 24 lid 2 van de AVG staat dat organisaties een passend privacybeleid dienen te hebben. De gemeente Heumen geeft hier invulling aan met dit document. Het doel van dit beleid is borgen dat persoonsgegevens veilig en rechtmatig worden verwerkt om zodoende een betrouwbare overheid en samenwerkingspartner te zijn en te blijven.

1.1 Begrippen en definities

In dit beleid wordt gebruikgemaakt van begrippen die ook in de AVG gehanteerd worden. Om de inhoud van dit beleid goed te kunnen begrijpen, worden hieronder een aantal veelgenoemde begrippen toegelicht. In bijlage 1 wordt tevens een overzicht weergegeven van de gehanteerde afkortingen en aanvullende begrippen.

Persoonsgegeven
Een persoonsgegeven is een gegeven dat iets zegt over een persoon. De informatie gaat direct over een persoon of is te herleiden tot een persoon.

Verwerken
Het verwerken van een persoonsgegeven houdt iedere handeling met een persoonsgegeven in. Dit kan bijvoorbeeld zijn het verzamelen, vastleggen, raadplegen, gebruiken en verstrekken van een persoonsgegeven.

Functionaris Gegevensbescherming (FG)
De FG is een onafhankelijk toezichthouder. De FG ziet er op toe dat de gemeente de privacywet en regelgeving correct toepast.

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens is de landelijke toezichthouder op het gebied van privacy.

Verwerkingsverantwoordelijke
In de gemeente Heumen is het college van Burgemeester en Wethouders verantwoordelijk voor het verwerken van persoonsgegevens. Dit betekent dat het college bepaalt wat er met de gegevens gebeurt. Als het gaat om openbare orde is de burgemeester verantwoordelijk. De Gemeenteraad is voor de eigen verwerkingen van persoonsgegevens en die van de griffier de verwerkingsverantwoordelijke.

Verwerker
Een verwerker is een persoon of organisatie die persoonsgegevens verwerkt namens de gemeente Heumen.

Betrokkene
De betrokkene is degene wiens gegevens worden verwerkt.

1.2. Uitgangspunten van de AVG

Algemeen uitgangspunt is dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving verwerkt worden. Voor een rechtmatige verwerking van persoonsgegevens dient aan de zes uitgangspunten van de AVG te zijn voldaan.

- **Rechtmatigheid, behoorlijkheid en transparantie:** persoonsgegevens mogen alleen verwerkt worden wanneer hier een grondslag voor is. Voor de gemeente geldt in de meeste gevallen dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang c.q. een taak in het kader van de uitoefening van het openbaar gezag. Ook kan het gaan om het nakomen van een wettelijke verplichting. Daarnaast dient de betrokkene te worden geïnformeerd over de verwerking van zijn persoonsgegevens.
- **Doelbinding:** Gegevens mogen slechts verwerkt worden voor de doeleinden waarvoor zij verzameld zijn.
- **Dataminimalisatie:** Er mogen nooit meer gegevens worden verwerkt dan noodzakelijk voor dat doel.
- **Juistheid:** De gegevens moeten actueel en correct zijn.
- **Bewaartermijn:** De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is.
- **Integriteit en vertrouwelijkheid:** De persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.

1.3. Verantwoordingsplicht

Om aan te kunnen tonen dat de gemeente aan de geldende wet- en regelgeving voldoet, wordt er uitvoering gegeven aan de verantwoordingsplicht. Dit houdt in dat de gemeente de volgende documentatie bijhoudt en kan overleggen indien nodig:

- Register van verwerkingen
- Register van datalekken en beveiligingsincidenten
- Overzicht van klachten en bezwaren over de verwerking van persoonsgegevens
- Overzicht van verzoeken op grond van de AVG met de genomen beslissingen
- Verslagen van uitgevoerde Data Protection Impact Assessments (DPIA's)
- Verwerkersovereenkomsten

1.4. Doelgroep

Het privacybeleid wordt toegepast door het bestuur en de medewerkers van de gemeente Heumen, inclusief alle extern ingehuurde medewerkers. De verantwoordelijkheden, taken en bevoegdheden die een medewerker heeft met betrekking tot de bescherming van persoonsgegevens, zijn nader uitgewerkt in dit privacybeleid en de daaronder hangende richtlijnen, reglementen en gedragscodes. Het beleid is opgesteld in het kader van de transparantie over de verwerking van persoonsgegevens.

1.5. Reikwijdte

Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens van de gemeente Heumen. Dat betekent dat dit beleid van toepassing is op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen. De betrokkenen zullen meestal inwoners of werknemers van de gemeente zijn, maar ook verwerkingen van persoonsgegevens van andere personen vallen onder dit beleid.

2. Governance / verantwoordelijkheden

Bij de inrichting en ontwikkeling van privacy is het van belang om de rollen en verantwoordelijkheden te bepalen rondom de zorgvuldige omgang met persoonsgegevens. In onderstaande paragrafen worden de organisatie-eenheden benoemd met daarbij hun verantwoordelijkheden op het gebied van privacy.

2.1.1. Het college van burgemeester en wethouders

De verwerkingsverantwoordelijke is degene die het doel van en de middelen voor de verwerking vaststelt. In de meeste gevallen zal dat het college van burgemeester en wethouders zijn, vooropgesteld dat het college doel en middelen van de verwerking vaststelt. Maar ook de burgemeester of de Raad kunnen verwerkingsverantwoordelijke zijn. Privacy valt onder de verantwoordelijkheid van het college.

2.1.2. Portefeuillehouder

De portefeuilleouder ICT van de gemeente Heumen is verantwoordelijk voor de uitvoering van het gemeentelijk privacybeleid en voor controle op de naleving van afspraken. Hij is het eerste aanspreekpunt binnen het college voor het onderwerp privacy.

2.1.3.. De Gemeenteraad

De gemeenteraad is verwerkingsverantwoordelijk voor de eigen verwerkingen, die onder andere door de griffier worden uitgevoerd. De griffier beschikt over een eigen protocol om te werken conform AVG. Daarnaast heeft de raad een controlerende functie ten opzichte van het college voor de naleving van de AVG en stellen zij budget beschikbaar.

2.1.4. Afdelingshoofden

Het creëren van bewustwording en de naleving van het beleid is onderdeel van de integrale bedrijfsvoering. Ieder afdelingshoofd heeft de taak om er voor te zorgen dat medewerkers op de hoogte zijn van het beleid en dat dit wordt nageleefd. Daarnaast dient ieder afdelingshoofd het onderwerp privacy onder de aandacht te brengen. De afdelingshoofden zijn hierbij verantwoordelijk voor de verwerkingen die uitgevoerd worden in het betreffende team. Welke verwerkingen dit zijn is te zien in het register van verwerkingen. Afdelingshoofden hebben regelmatig contact met de portefeuillehouder en de FG. Ten slotte zijn de afdelingshoofden ervoor verantwoordelijk dat hun teams de FG betrekken bij alle aangelegenheden die met persoonsgegevens te maken hebben.

2.1.5. Afdelingen/Teams

De feitelijke verwerking van persoonsgegevens vindt plaats binnen de verschillende teams. Bij de uitvoering van taken zijn medewerkers zich bewust van het feit dat privacy een rol kan spelen bij deze taken. Dit betekent dat medewerkers handelen naar het privacybeleid en de interne procedures ten aanzien van beheer en beveiliging. Medewerkers zijn in staat situaties te herkennen waarin expertise nodig is

van de FG en/of CISO. Als een medewerker twijfelt of het beleid goed uitgevoerd wordt of kan worden dan zal dit vraagstuk met het afdelingshoofd besproken worden, aangezien deze verantwoordelijk is voor de verwerkingen van het betreffende team.

2.1.6. Functionaris Gegevensbescherming (FG)
De FG heeft de taak om toe te zien op de naleving van de wettelijke verplichtingen bij het verwerken van persoonsgegevens door de gemeente Heumen. De FG toetst onder andere de naleving van de wettelijke eisen, de gemeentelijke richtlijnen op het gebied van privacy en het privacybeleid. Daarnaast geeft de FG gevraagd of ongevraagd advies over bijvoorbeeld het doen van een data privacy impact assessment (DPIA) en ziet toe op de uitvoering van het advies. Tevens is de FG het contactpunt voor de Autoriteit Persoonsgegevens (AP). De FG brengt jaarlijks een verslag uit met bevindingen over de naleving van de AVG aan het college.

2.1.7. CISO
De Chief Information Security Officer (CISO) is de belangrijkste adviseur op het gebied van informatiebeveiliging. De CISO is belast met het toezicht op de betrouwbaarheid van de informatievoorziening ter waarborging van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie binnen de organisatie. De CISO ziet toe op de controle van een juiste uitvoering van het informatiebeveiligingsbeleid, de realisatie van de veiligheidsmaatregelen en de classificatie, coördinatie en escalatie van beveiligingsincidenten. De CISO werkt nauw samen met de FG.

3. Richtlijnen
Om privacy te kunnen borgen in de dagelijks praktijk zijn er verschillende richtlijnen geformuleerd. Deze richtlijnen borgen dat persoonsgegevens rechtmatig en gestructureerd verwerkt worden. De richtlijnen die voortvloeien uit de AVG worden in paragraaf 3.1. t/m 3.10 toegelicht.

3.1. Wet- en regelgeving naast de AVG
Naast de AVG bestaan er nog meer wetten die in acht genomen moeten worden bij het verwerken van persoonsgegevens. Dit zijn onder meer de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG), de Wet politiegegevens (Wpg) en de Wet basisregistratie personen (BRP). Daarnaast zijn er, afhankelijk van het proces, nog andere wetten van toepassing op een gegevensverwerking. Om te beoordelen of een verwerking rechtmatig is wordt er altijd gekeken of er naast de AVG nog andere wet- en regelgeving van toepassing is op de gegevensverwerking.

Verwerkingen op basis van de wet BRP (Basisregistratie Personen) kennen een eigen regime dat minimaal gelijk is aan of strenger is dan de AVG-regels. Dit heeft tot gevolg dat sommige rechten worden beperkt of uitgesloten. Daar waar de Wet BRP niets regelt gelden de bepalingen van de AVG en de UAVG.

3.2. Verwerking van bijzondere persoonsgegevens
In artikel 9 van de AVG worden de regels uiteengezet voor het verwerken van bijzondere persoonsgegevens. In beginsel is het verwerken van deze categorieën van persoonsgegevens verboden, maar het is toegestaan als de verwerking noodzakelijk is om te kunnen voldoen aan een wettelijke verplichting of in het geval van een zwaarwegend algemeen belang.

De gemeente Heumen verwerkt in principe alleen bijzondere persoonsgegevens als dit noodzakelijk is om aan wet- en regelgeving te kunnen voldoen.

3.3. Cameratoezicht
De gemeente Heumen heeft een gerechtvaardigd belang voor het inzetten van cameratoezicht. In en rondom het gemeentehuis zijn camera's bevestigd. Dit beleid is van toepassing op de camera in het gemeentehuis zelf en de vier camera's in de parkeergarage. De camerabeelden worden gebruikt voor het beveiligen van het gebouw, de bezittingen van de gemeente en de werknemers of bezoekers. Ook kan cameratoezicht worden ingezet voor het handhaven van openbare orde en veiligheid. In voorkomende situaties kunnen de beelden worden gedeeld met de politie.

3.4. Basisregistratie Personen
Iedere gemeente beheert persoonsgegevens die in de Basisregistratie Personen (BRP) staan. De BRP is een database waarin de basis gegevens van inwoners zijn opgenomen. Iedere gemeente verstrekt een kopie van deze gegevens aan de Rijksdienst voor Identiteitsgegevens (RvIG van het MINBZK). Het RvIG beheert deze landelijke database van persoonsgegevens en verstrekt hieruit gegevens aan (semi-) overheidsinstanties voor het uitvoeren van wettelijke taken. De gemeente verstrekt geen persoonsgegevens aan commerciële instellingen.

3.5. Rechten van betrokkenen

Betrokkenen hebben in het kader van transparantie het recht om helder geïnformeerd te worden over de rechten die zij hebben en de wijze waarop hun persoonsgegevens verwerkt en beheerd worden door de gemeente. Indien betrokkenen hun rechten willen uitoefenen, neemt de gemeente Heumen deze verzoeken in behandeling. Er is een procedure opgesteld en een werkproces ingericht om verzoeken gestructureerd te kunnen behandelen. Op de website van de gemeente wordt toegelicht welke rechten inwoners hebben als het gaat om privacy en op welke wijze zij deze rechten kunnen uitoefenen. Hieronder wordt kort toegelicht wat de rechten van betrokkenen inhouden. Ten opzichte van deze rechten gelden een aantal algemene uitgangspunten die hieronder toegelicht worden.

Rechten van betrokkenen zoals in artikel 15 t/m 21 AVG:

Inzage
Een betrokkene heeft het recht om van de verwerkingsverantwoordelijke antwoord te krijgen op de vraag of er hem betreffende persoonsgegevens verwerkt worden en zo ja, inzicht te krijgen in welke gegevens dit zijn.

Rectificatie
Een betrokkene heeft het recht om zijn of haar persoonsgegevens te laten rectificeren. Dit houdt in dat fouten hersteld moeten worden.

Wissen van persoonsgegevens
Een betrokkene heeft het recht een verzoek te doen tot wissen van de persoonsgegevens die worden verwerkt door de gemeente.

Beperking
Een betrokkene heeft het recht om een verzoek te doen tot beperking van de verwerking. Dit houdt in dat de gemeente de gegevens nog wel mag bewaren, maar dat de gegevens niet meer verwerkt mogen worden.

Bezwaar
Een betrokkene heeft te allen tijde het recht om bezwaar te maken tegen de verwerking van hem of haar betreffende persoonsgegevens. Als dit bezwaar gegrond wordt verklaard, dan moet de gemeente de gegevensverwerking waar bezwaar tegen is gemaakt staken.

Recht op overdraagbaarheid van persoonsgegevens
Betrokkenen hebben het recht om persoonsgegevens over te laten dragen. Dit houdt in dat de betrokkene het recht heeft om de persoonsgegevens te ontvangen die de gemeente heeft. Zo kunnen gegevens bijvoorbeeld makkelijk rechtstreeks overgedragen worden aan een andere organisatie.

3.6.. Meldplicht datalekken
De gemeente gaat zorgvuldig om met persoonsgegevens. Toch kan het voorkomen dat onbevoegde personen toegang krijgen tot persoonsgegevens of dat persoonsgegevens kwijtraken. In dat geval spreken we van een datalek. Datalekken die een mogelijk risico opleveren voor de rechten en vrijheden van betrokkenen moeten altijd binnen 72 uur bij de Autoriteit Persoonsgegevens worden gemeld. Bij een groot risico voor de betrokkenen moeten ook zij geïnformeerd worden.
De medewerker die een (mogelijk) datalek constateert, meldt dit zo snel mogelijk bij de FG. De FG schakelt met de CISO over de te nemen maatregelen en maakt de melding bij de Autoriteit Persoonsgegevens. Indien er een beveiligingsrisico geconstateerd wordt, dan wordt er melding gemaakt bij het team informatiebeveiliging en privacy zodat deze conform de geldende procedure voor het melden van beveiligingsincidenten en datalekken kan worden afgehandeld.

3.7. Data Protection Impact Assessment (DPIA)
Wanneer er sprake is van een verhoogd risico bij het gebruik van persoonsgegevens, worden de privacy risico's in kaart gebracht door een DPIA (ook wel Data Protection Impact Assessment (DPIA) genoemd) uit te voeren. Door middel van een DPIA wordt het proces omtrent de verwerking van persoonsgegevens omschreven, wordt aangetoond in hoeverre de privacy van betrokkenen gewaarborgd is en worden de al dan niet te nemen maatregelen gemotiveerd. Voor het uitvoeren van een DPIA is eveneens een procedure opgesteld.

Een DPIA wordt bij voorkeur in een zo vroeg mogelijk stadium van het ontwerpproces uitgevoerd, zodat uitkomsten van de DPIA meegenomen kunnen worden in het ontwerp en invulling gegeven kan worden aan 'privacy by design'. Een DPIA kan ook in een later stadium uitgevoerd worden, omdat processen zich verder ontwikkelen en privacyrisico's in een later stadium beperkt kunnen worden.

Bij het uitvoeren van de DPIA wordt de FG advies gevraagd, Dat advies en wat met dat advies wordt gedaan, dient in de DPIA te worden gedocumenteerd. Met de uitkomsten van een DPIA wordt bepaald of de verwerking van persoonsgegevens zal aanvangen of dat er eventueel aanpassingen in het proces of systeem vereist zijn. Dit betekent dat gemotiveerd wordt welke keuzes worden gemaakt ten aanzien van de verwerking van persoonsgegevens.

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een DPIA uit te voeren. Er zullen enkel DPIA's worden uitgevoerd in geval van nieuwe verwerkingen van persoonsgegevens en verwerkingen waarbij sprake is van een grote verzameling van persoonsgegevens of een verzameling met bijzondere categorieën van persoonsgegevens. De checklist die de AP heeft opgesteld geldt hierbij als richtsnoer.

Pas nadat de DPIA is uitgevoerd en de maatregelen zijn getroffen die nodig zijn om de risico's te beperken, verwerkt de gemeente de persoonsgegevens. Wanneer uit de DPIA blijkt dat de beoogde verwerking een hoog risico oplevert, maar het niet gelukt is om maatregelen te treffen, dan wordt de AP geraadpleegd. Dit wordt voorafgaande raadpleging genoemd. Bij een voorafgaande raadpleging geeft de AP advies met betrekking tot hoe de risico's van de voorgenomen verwerking beperkt kunnen worden. Als deze maatregelen uitgevoerd worden, mag de verwerking aanvangen. Het kan ook dat de AP adviseert om helemaal van de verwerking af te zien.

3.8. **Register van verwerkingsactiviteiten**
In het register van verwerkingsactiviteiten wordt bijgehouden welke verwerkingen van persoonsgegevens de gemeente uitvoert. De FG beheert het register centraal. De afdelingshoofden zijn verantwoordelijk voor het correct en tijdig bijhouden van het register.

3.9. **Verwerkersovereenkomst**
Wanneer de gemeente een dienst uitbesteedt, dan blijft de gemeente de verwerkingsverantwoordelijke en daarmee verantwoordelijk voor de gegevensverwerking. De partij waar de dienst aan wordt uitbesteed, wordt de verwerker genoemd. De gemeente als verwerkingsverantwoordelijke stelt in die situatie het doel en de middelen vast voor de verwerking van persoonsgegevens. De verwerker heeft geen zeggenschap over de wijze van verwerken, en werkt volgens de instructies en in opdracht van de gemeente. Een verwerker neemt tevens geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc. Indien er sprake is van bovenstaande situatie, is de gemeente verplicht een verwerkersovereenkomst af te sluiten. Dit is een overeenkomst waarin afspraken ten aanzien van de verwerking worden vastgelegd om daarmee de rechten van de inwoners te beschermen. Het afsluiten van een verwerkersovereenkomst is een verplichting voor zowel de verwerkingsverantwoordelijke als de verwerker.

3.10. **Gebruik van toestemming**
De verwerking van persoonsgegevens dient zoals in paragraaf 1.3. aangegeven, gebaseerd te zijn op een grondslag. Als de verwerking van gegevens niet op een van de grondslagen is gebaseerd, is de verwerking per definitie onrechtmatig. Gemeenten doen voor hun verwerkingen meestal een beroep op de grondslag van 'algemeen belang' of de grondslag 'wettelijke verplichting'. Er zijn echter situaties denkbaar waarbij deze grondslagen niet van toepassing zijn, maar gegevens verwerken wel noodzakelijk is om de inwoner van dienst te kunnen zijn. In die situaties kunnen gegevens verwerkt worden indien de betrokkene hiervoor toestemming heeft gegeven. Er wordt alleen gebruik gemaakt van de grondslag 'toestemming' als er geen andere mogelijkheid is. In enkele gevallen zal het verwerken op basis van toestemming onoverkomelijk zijn. Wanneer dit zo is, wordt op een duidelijke en begrijpelijke wijze uitgelegd waar het toestemmingsverzoek over gaat. Ook deze gegevens worden alleen voor dat doel gebruikt waarvoor ze oorspronkelijk bedoeld waren. Indien het toch nodig blijkt dat de gegevens ook voor andere doeleinden gebruikt worden, dient de betrokkene daarover geïnformeerd te worden en dient hiervoor opnieuw toestemming gevraagd te worden. De betrokkene is te allen tijde vrij om de toestemming te geven of te weigeren. Indien de betrokkene toestemming geeft, mag deze op ieder moment weer ingetrokken worden.

4. Bewustwording & Training
Privacy is een onderwerp dat betrekking heeft op de hele organisatie en is meer dan alleen het nemen van technische maatregelen. Bewustwording is belangrijk voor het slagen van privacybescherming. Hiermee kunnen namelijk menselijke fouten worden voorkomen, die vaak de belangrijkste oorzaak zijn van inbreuken. Van belang is dat medewerkers van de gemeente zich bewust zijn van het belang van privacy zodat zij ook de knelpunten kunnen signaleren en actief melding maken bij de FG zodat zij hun controlerende en adviserende taken kunnen vervullen. Bewustwording vereist onderhoud. Dit houdt in dat privacy in combinatie met informatiebeveiliging met regelmaat onder de aandacht wordt gebracht in onder andere werkoverleggen en bijvoorbeeld tijdens kennissessies of trainingen.

5. Beheer en opslag van gegevens

Bij het beheren van persoonsgegevens speelt informatievoorziening en ICT een belangrijke rol. Persoonsgegevens worden binnen de gemeente Heumen (vrijwel) altijd digitaal opgeslagen. In het informatiebeleidsplan staat welke kant de gemeente zich op ontwikkelt op digitaal gebied en hoe inwoners hier zo goed als mogelijk in gefaciliteerd worden. Hier worden de regels uit het privacy- en informatiebeveiligingsbeleid in acht genomen.

Opslag gebeurt op de volgende manieren:

- Het heeft sterk de voorkeur om gegevens op te slaan in centrale databases die door verschillende gebruikers te benaderen en te bewerken zijn. We sluiten ook zoveel mogelijk aan bij landelijke (standaard) ICT infrastructuur en benaderen gegevens waar mogelijk direct bij de bron zonder opslag. Eenmalige opslag en meervoudig gebruik is hierbij het uitgangspunt.
- Binnen decentrale databases en spreadsheets die middels algemene kantoorautomatiseringssoftware te benaderen zijn. Dit betreft kleinschalige registraties met een zeer specifiek doel.
- Op ongestructureerde basis: in documenten, afbeeldingen en dergelijke. Dit betreft geen registraties maar specifieke persoonsgegevens over een of enkele personen.

Voor de opslag van persoonsgegevens gelden de volgende uitgangspunten:

- Opslag in centrale databases heeft sterk de voorkeur boven decentrale opslag. Centrale databases kennen een hogere beschikbaarheid, daarnaast is de integriteit en de vertrouwelijkheid van de data veel beter te waarborgen.
- Indien de applicatie geïnstalleerd is binnen het netwerk van de gemeente Heumen dan dient de opslag van persoonsgegevens te geschieden op een goed beveiligd netwerk.
- Lokale opslag zoals smartphones en laptops worden afdoende versleuteld.
- De gemeente Heumen kent diverse voorzieningen om de beschikbaarheid van de persoonsgegevens te waarborgen.
- Vitale ICT-systemen en componenten zijn dubbel uitgevoerd, en alle gegevens op het interne netwerk worden dagelijks geback-upt. Ook deze maatregelen zijn in lijn met de gemeentelijke beveiligingsnormen.
- Bij het aanschaffen van nieuwe software of het vervangen van software wordt in veel gevallen Software as a Service (SAAS) ingezet. Met deze SAAS leveranciers moeten van te voren heldere afspraken worden gemaakt over beveiliging en beheer data, opslaglocatie, verwerker versus verwerkingsverantwoordelijke en businesscontinuïteit.

Bewaren en archiveren van gegevens

- De AVG geeft geen concrete bewaartermijnen voor persoonsgegevens.
- Uitgangspunt van de gemeente Heumen is dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is.
- Om te beoordelen of en hoelang gegevens bewaard mogen worden maakt de gemeente gebruik van een geldige selectielijst. Dit is een lijst van werkprocessen met de bijbehorende bewaartermijnen en komt voort uit verschillende wetten, onder andere de Archiefwet.
- In het register van verwerkingen worden de bewaartermijnen van persoonsgegevens weergegeven.

Toegang tot persoonsgegevens

- De gemeente draagt zorg voor een goede beveiliging van persoonsgegevens, door het nemen van passende technische en/of organisatorische maatregelen, waaronder het inzetten van multifactorauthenticatie, autorisaties, logging en periodieke controles.
- De gemeente voorkomt ongeoorloofde toegang en gebruik van persoonsgegevens.

6. Informatiebeveiligingsbeleid

Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de AVG. Artikel 32 van de AVG schrijft voor dat gegevens passend beveiligd moeten. Voor de uitwerking van artikel 32 wordt gebruikgemaakt van de Baseline Informatiebeveiliging Overheid (BIO). In de BIO staan de regels waar gemeenten zich voor wat betreft informatiebeveiliging aan moeten houden. Informatiebeveiliging is om die reden een integraal onderdeel van de AVG. Informatiebeveiliging heeft als uitgangspunt dat de integriteit, vertrouwelijkheid en beschikbaarheid van informatiesystemen geborgd is. Om dit te kunnen bewerkstelligen heeft de gemeente een apart informatiebeveiligingsbeleid opgesteld.

Bijlage 1 Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
Wpg	Wet politiegegevens
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basisregistratie Personen
CISO	Chief Information Security Officer
FG	Functionaris voor gegevensbescherming
DPIA	Data Protection Impact Assessment