Strategisch Privacybeleid Heumen 2020

Definitieve versie | Mei 2020

Inhoud

Leeswijzer

Voor de totstandkoming van dit beleid is gebruik gemaakt van het VNG raamwerk bestaande uit vijf thema's die samenhangen: Governance, Beleid, Werkprocessen, Bewustwording & Training en Beheer & Opslag. Privacy omvat veel onderwerpen en komt dan ook door de gehele gemeente terug. Met behulp van dit raamwerk worden alle aandachtsgebieden met betrekking tot privacy in kaart gebracht waardoor op een gestructureerde wijze invulling gegeven kan aan het onderwerp privacy.

De onderliggende privacyprocedures, formats en overige documentatie zijn op zichzelf staande documenten die kunnen worden aangepast conform de Plan-Do-Check-Act cyclus.

Beleid

In het hoofdstuk Beleid zijn de aanleiding voor dit beleid, de reikwijdte en het doel ervan beschreven en zijn de belangrijkste uitgangspunten geformuleerd.

Governance / verantwoordelijkheden

In het hoofdstuk Governance komen de rollen en verantwoordelijkheden ten aanzien van privacy ter sprake.

Werkprocessen

Werkprocessen en privacy hebben een plek in het dagelijks werk van medewerkers van de gemeente. In dit hoofdstuk worden de processen besproken die voortvloeien uit de AVG en de reguliere processen van de gemeente waar privacy een rol in speelt.

Bewustwording & Training

In dit hoofdstuk is beschreven hoe de gemeente Heumen privacy onder de aandacht brengt bij haar medewerkers.

Beheer & opslag van gegevens

In dit hoofdstuk wordt beschreven hoe persoonsgegevens geregistreerd, beheerd en beveiligd worden.

Samenvatting
De gemeente verzamelt en verwerkt voor de uitvoering van diverse taken persoonsgegevens en slaat deze op ten behoeve van de dienstverlening aan haar inwoners, bedrijven en instellingen. Het privacybeleid is opgesteld voor alle medewerkers van de gemeente Heumen. Alle medewerkers krijgen in de uitvoering van zijn of haar werkzaamheden te maken met persoonsgegevens. De gemeente wil een betrouwbare partner zijn en blijven voor haar 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.

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 voor gemeente Heumen. Privacy is een onderwerp dat met de dag belangrijker wordt gezien de digitale wereld waar we ons nu in bevinden. Ook de gemeente gaat steeds meer digitaal werken, wat meer eisen stelt aan de bescherming van (digitale) gegevens. De gemeente is zich hiervan bewust en daarom is gekozen om een nieuw beleid op te stellen waarin omschreven wordt waar wij nu staan als gemeente, waar we naar toe willen en hoe we er gezamenlijk voor zorgen dat we dit doel kunnen behalen. Om dit te kunnen bepalen, heeft overleg plaatsgevonden met het management en enkele betrokken medewerkers.

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.

De privacykernwaarden van Heumen
De zes uitgangspunten (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 en partners mag niet in verkeerde handen vallen.

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:

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

De basis van dit beleid is gebaseerd op het VNG raamwerk. Dit raamwerk bestaat uit de volgende vijf thema's: Beleid, Governance, Werkprocessen, Bewustwording & Training en Beheer & en Opslag van gegevens. Aan de hand van de vijf thema's in dit raamwerk worden de aandachtspunten met betrekking tot privacy voor een gemeente overzichtelijk weergegeven. Elk thema is een stukje van de puzzel en de complete puzzel laat zien hoe alle thema's met elkaar samenhangen: samen vormen ze de kapstok waaraan alle onderwerpen van de AVG kunnen worden opgehangen.

1. Beleid

In artikel 24.2 van de AVG staat dat we als organisatie een passend privacybeleid dienen te hebben. Voor de structuur van dit beleid komen de thema's uit het raamwerk van de VNG naar voren. Om deze criteria te kunnen bepalen is het belangrijk eerst de kaders en uitgangspunten van de AVG in kaart te brengen. Deze dienen als richtsnoer voor het hele privacybeleid en onze kernwaarden zijn gebaseerd op wat de AVG ons verplicht, maar ook op basis van onze eigen invulling waar deze ruimte wordt gegeven.

1.1. Begrippen en definities

In dit beleid wordt gebruik gemaakt 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.

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. Aanleiding

De gemeente Heumen heeft persoonsgegevens nodig om haar taken uit te kunnen voeren. Zonder de verwerking van persoonsgegevens is het onmogelijk om bijvoorbeeld aan een inwoner een nieuw paspoort te verstrekken of een vergunning te verlenen. Om aan de AVG en onze kernwaarden te kunnen voldoen is een gedegen privacybeleid van belang.

Het verwerken van persoonsgegevens dient met uiterste zorgvuldigheid te gebeuren, omdat onjuiste omgang met persoonsgegevens schade tot gevolg kan hebben. Door publicaties van de Autoriteit Persoonsgegevens (AP) blijkt ook regelmatig dat er met persoonsgegevens niet voorzichtig genoeg omgegaan kan worden. Het op een juiste manier verwerken van persoonsgegevens is de

verantwoordelijkheid van het college van Burgemeester en Wethouders, maar de uitvoering begint bij de individuele medewerker. De AVG stelt hiervoor algemene kaders om persoonsgegevens correct te verwerken, maar de AVG laat ook ruimte voor een eigen invulling. Met dit beleidsdocument vult de gemeente Heumen deze kaders nader in en neemt hiermee tevens haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren.

Met dit document wordt de vertaalslag gemaakt van geldende wet- en regelgeving naar de dagelijkse praktijk voor gemeente Heumen.

1.3. 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.

1.4. Criteria uit de AVG

Om aan te kunnen tonen dat de gemeente aan de geldende wet- en regelgeving voldoet, heeft de AVG een aantal criteria opgesteld. Dit heet de verantwoordingsplicht, ook wel accountability genoemd. De belangrijkste criteria zijn hieronder opgesomd. In de komende hoofdstukken wordt bij ieder criterium een nadere toelichting gegeven. Tevens wordt hieronder verwezen naar de procedures voor de standaardformats, waarmee de gemeente Heumen invulling geeft aan elk onderwerp.

- Register van verwerkingen
- Governance informatiebeveiliging en privacy
- Verwerkersovereenkomst afsluiten met partners
- Uitvoeren en documenteren van een privacy impact assessment (DPIA)
- Procedure rechten van betrokkenen
- Register en protocol voor datalekken
- Technische en organisatorische beveiligingsmaatregelen
- Aanstellen van een functionaris voor de gegevensbescherming

1.5. Doelen van de gemeente Heumen

Dit privacybeleid is opgesteld om te bepalen hoe de gemeente Heumen om wil gaan met persoonsgegevens. De gemeente Heumen stelt met dit privacybeleid de kaders en formuleert uitgangspunten over het zorgvuldig omgaan met persoonsgegevens binnen de kaders van de verschillende wetten. Voldoen aan de AVG betekent dat op verschillende terreinen binnen de gemeentelijke organisatie aandacht moet zijn voor privacy. Om die reden zullen de governance, werkprocessen, triages, bewustwording en het beheer en de opslag van gegevens in dit beleidsplan onder de loep genomen worden.

1.6. 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 opgeteld in het kader van de transparantie over de verwerking van persoonsgegevens.

1.7. Reikwijdte

Een gegeven wordt een persoonsgegeven genoemd wanneer dit informatie bevat over een persoon (de betrokkene) en/of tot een individu te herleiden is. Dit beleid is van toepassing op alle verwerkingen van persoonsgegevens van alle betrokkenen die geheel of gedeeltelijk geautomatiseerd worden uitgevoerd. Daarnaast is dit beleid van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. De betrokkenen kunnen onder andere inwoners van de gemeente zijn, maar ook de medewerkers van de gemeente en externe relaties.

1.8. Privacy van de inwoners van de gemeente Heumen

De gemeente Heumen heeft gegevens nodig om haar wettelijke verplichtingen en gemeentelijke taken uit te kunnen voeren.[1]De gemeente kan bijvoorbeeld geen paspoort verstrekken of een maatwerkvoorziening leveren zonder gegevens over de desbetreffende persoon te verwerken.

Betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig met persoonsgegevens omgaat, en dat de gemeente voorkomt dat er een onnodige of te vergaande inbreuk wordt gemaakt op de persoonlijke levenssfeer.

1.9. Privacy van de medewerkers van de gemeente Heumen

Naast het feit dat de gemeente Heumen persoonsgegevens van haar inwoners verzamelt, worden er ook gegevens van personeel verwerkt door de personeelsadministratie. Dit is noodzakelijk om onder andere iedere maand salaris te kunnen betalen aan de medewerker. Het kan ook voorkomen dat er privacygevoelige informatie van medewerkers verwerkt wordt. Ook het personeel moet erop kunnen vertrouwen dat er zorgvuldig met gegevens omgegaan wordt. Wat betreft de gegevens van het personeel gelden dan ook dezelfde waarborgen als voor de gegevens van inwoners.

[1] Artikel 6, lid 1, onder c en e AVG

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. Binnen de organisatie moet in kaart worden gebracht wie waarvoor verantwoordelijk is.

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. Binnen het college is een portefeuillehouder privacy aangewezen.

2.1.2. Portefeuillehouder

De wethouder van de gemeente Heumen is portefeuillehouder privacy en daarmee 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 wordt voor een aantal taken als gemeentelijk overheidsorgaan door de AVG als verwerkingsverantwoordelijke aangemerkt. 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 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. Als een afdelingshoofd twijfelt of het beleid goed uitgevoerd wordt of kan worden dan zal dit vraagstuk met de wethouder besproken worden, aangezien de wethouder als portefeuillehouder verantwoordelijk is voor de uitvoering van het gemeentelijk privacybeleid. Ten slotte zijn de afdelingshoofden ervoor verantwoordelijk dat hun teams de FG/privacy officer 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 dienen 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 dienen in staat te zijn situaties te herkennen waarin expertise nodig is van de FG, CISO of privacy Officer (PO). Als een medewerker twijfelt of het beleid goed uitgevoerd wordt of kan worden dan zal dit vraagstuk met de manager besproken worden, aangezien de manager verantwoordelijk is voor de verwerkingen van het betreffende team. Daarnaast heeft elke afdeling/team een aanspreekpunt privacy & informatiebeveiliging, die de communicatie, adviezen en informatie van de FG en CISO deelt met zijn of haar team.

2.1.6. Functionaris Gegevensbescherming (FG) en Privacy Officer (PO)

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 hij of zij desgevraagd advies over bijvoorbeeld het doen van een privacy impact assessment (PIA) en ziet hij of zij toe op de uitvoering van zijn advies. Tevens is de FG het contactpunt voor de AP.

De uitvoerende taken op het gebied van privacy zijn bij de PO belegd zodat de FG zijn adviserende en toezichthoudende rol vervult. De PO voert werkzaamheden uit zoals het actueel houden van het privacybeleid, de feitelijke implementatie van het beleid, het bijhouden van het register van verwerkingen en het coördineren van verzoeken van betrokkenen. De taken van de PO en de FG kunnen door één persoon worden ingevuld, afhankelijk van de beschikbaarheid aan budget en fte.

2.1.7. CISO

De Chief Information Security Officer (CISO) coördineert de informatiebeveiliging. De CISO is belast met het toezicht op de betrouwbaarheid van de informatievoorziening ter waarborging van de vertrouwelijkheid, integriteit beschikbaarheid van informatie binnen de organisatie. De CISO is de beleidsfunctionaris die taken uitvoert op het gebied van informatiebeveiliging en de spin in het web van de informatiebeveiliging. De CISO is verantwoordelijk voor de controle op 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/privacy officer en i-adviseur.

3. Werkprocessen

Om privacy te kunnen borgen zijn er verschillende werkprocessen ingericht. Deze processen zijn er op gericht om rechtmatig en gestructureerd persoonsgegevens te kunnen verwerken. Deze werkprocessen die voortvloeien uit de AVG worden in paragraaf 3.1. toegelicht. Daarnaast worden in de reguliere werkprocessen van de gemeente persoonsgegevens verwerkt. De wijze waarop privacy een rol speelt in deze werkprocessen en welke aandachtspunten hierbij gelden wordt toegelicht in paragraaf 3.2.

3.1.1. Basisregistratie Personen

Iedere gemeente beheert persoonsgegevens die in de Basisregistratie Personen (BRP) staan. De BRP is een centrale database waarin de basis gegevens van inwoners zijn opgenomen. De gemeente Heumen zal deze gegevens in sommige gevallen ook aan andere overheidsorganisaties verstrekken. De Belastingdienst bijvoorbeeld gebruikt persoonsgegevens om belastingen te heffen en het UWV om uitkeringen te verstrekken. De gemeente verstrekt de gegevens uit de BRP niet aan commerciële instellingen of aan particulieren.

3.1.2. 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 https://www.heumen.nl/inwoners/privacyverklaring_45179/ 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 moet het recht hebben om zijn of haar persoonsgegevens te laten rectificeren. Dit houdt in dat fouten hersteld moeten worden. Het kan bijvoorbeeld gaan om persoonsgegevens die in eerste instantie verkeerd zijn opgenomen: denk aan een naam die verkeerd is ingevoerd.

- **Gegevenswissing**

Een betrokkene heeft recht een verzoek te doen tot wissing van de persoonsgegevens. Denk hierbij aan een onrechtmatige gegevensverwerking of het intrekken van toestemming voor de gegevensverwerking waarbij er geen andere rechtsgrond meer overblijft.

- **Beperking**

Een betrokkene heeft het recht om een verzoek te doen tot beperking van de verwerking. Dit houdt in dat de verantwoordelijke de gegevens nog wel mag bewaren, maar dat hij de gegevens niet meer mag verwerken/gebruiken. Hiermee is dit recht minder verstrekkend dan het recht op het wissen van persoonsgegevens.

- **Bezwaar**

Een betrokkene heeft te allen tijde het recht om bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens. Als een betrokkene bezwaar maakt moet de verwerkingsverantwoordelijke de verwerking staken, tenzij dwingende gerechtvaardigde gronden anders bepalen.

- **Dataportabiliteit**

Betrokkenen hebben het recht om persoonsgegevens over te laten dragen. Dit heet het recht op dataportabiliteit. 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. In de praktijk kan van dit recht bij gemeenten niet of nauwelijks gebruik worden gemaakt.

3.1.3. 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. Het kan bijvoorbeeld gaan om een diefstal van een laptop, een in de trein vergeten usb-stick of een e-mail die naar de verkeerde persoon is verstuurd. Datalekken moeten worden gemeld bij de AP binnen 72 uur na ontdekking daarvan en in sommige gevallen ook bij de betrokkene.

De medewerker die een (mogelijk) beveiligingslek en/of datalek constateert, meldt dit zo snel mogelijk bij de FG/PO. De FG/PO schakelt met de CISO over de te nemen maatregelen en maakt de melding bij de autoriteit persoonsgegevens. Indien een datalek of beveiligingsrisico geconstateerd wordt, dient deze gemeld te worden zodat deze conform de geldende procedure voor het melden van beveiligingslekken en datalekken kan worden afgehandeld.

Het melden van eventuele beveiligingsrisico's of datalekken wordt aangemoedigd door de gemeente Heumen. Meldingen van beveiligingsrisico's worden gezien als een kans om het proces, de werkwijze en de dienstverlening van de gemeente Heumen te verbeteren.

3.1.4. Privacy Impact Assessment (PIA)

Wanneer er sprake is van een verhoogd risico bij het gebruik van persoonsgegevens, worden de privacy risico's in kaart gebracht door een PIA (ook wel Data Protection Impact Assessment (DPIA) genoemd) uit te voeren. Door middel van een PIA 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 PIA wordt bij voorkeur in een zo vroeg mogelijk stadium van het ontwerpproces uitgevoerd, zodat uitkomsten van de PIA meegenomen kunnen worden in het ontwerp en invulling gegeven kan worden aan 'privacy by design'. Een PIA 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 PIA wordt de FG advies gevraagd, maar zal de PIA niet zelf uitvoeren. Dat advies en wat met dat advies wordt gedaan, dient in de PIA te worden gedocumenteerd. Met de uitkomsten van een PIA 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. De gemeente Heumen gebruikt altijd hetzelfde format voor een PIA, deze is gemaakt door Safe Harbour B.V. en aan onze gemeente verstrekt.

Het is niet noodzakelijk om voor alle processen waarbij persoonsgegevens worden verwerkt een PIA uit te voeren. Er zullen enkel PIA'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 AP heeft een checklist opgesteld om te bepalen of een DPIA uitgevoerd moet worden. Pas nadat de PIA is uitgevoerd en de maatregelen zijn getroffen die nodig zijn om de risico's te beperken, verwerkt de gemeente de persoonsgegevens. Wanneer uit de PIA 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.

3.1.5. Register van verwerkingsactiviteiten

In het register van verwerkingsactiviteiten wordt bijgehouden welke verwerkingen van persoonsgegevens de gemeente heeft. Een register dient te voldoen aan bepaalde eisen. De PO beheert het actuele register van verwerkingsactiviteiten van de gemeente Heumen. Daarnaast hebben de teams bij het verwerken van persoonsgegevens de verantwoordelijkheid om in beeld te brengen welke verwerkingen er plaats vinden en nieuwe verwerkingen te melden bij de PO.

3.1.6. 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 en de verwerker. De gemeente Heumen maakt in beginsel gebruik van de standaard Verwerkersovereenkomst Gemeenten van de VNG.

3.1.7. 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. Voor de gemeente zal in de meeste gevallen de grondslag '*vervulling van een taak van algemeen belang of uitoefening van openbaar gezag*' en '*uitvoeren wettelijke taak*' van toepassing zijn. Er zijn echter situaties denkbaar waarbij deze grondslag 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[2] heeft gegeven. Hierbij moet wel de kanttekening worden geplaatst dat de gemeente Heumen zo min mogelijk gebruik maakt van deze grondslag. Dit heeft te maken met het feit dat tussen de gemeente en haar inwoners een afhankelijkheidsrelatie bestaat. Dit houdt in dat de betrokkene niet altijd vrijelijk kan kiezen. 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.

3.2. Privacy binnen werkprocessen

Gemeentebreed worden allerlei werkprocessen uitgevoerd. Bij veel processen worden ook persoonsgegevens verwerkt. Het is daarom van belang dat er binnen de gemeentelijke werkprocessen zowel voorafgaand als tijdens het proces aandacht besteed wordt aan privacy. De gemeente dient op een zorgvuldige, transparante en veilige manier met de persoonsgegevens van de inwoners en de medewerkers om te gaan. Om bij de uitvoering van bestaande processen en bij de invoering van nieuwe processen de privacy van de betrokkene te kunnen waarborgen, zijn de volgende aandachtspunten van belang:

- Nieuwe processen waarbij persoonsgegevens betrokken zijn, worden vooraf getoetst aan de eisen die de AVG stelt.
- Persoonsgegevens mogen alleen worden verwerkt indien hier een grondslag voor is zoals genoemd in paragraaf 1.3.
- Binnen een werkproces worden persoonsgegevens alleen verwerkt voor het realiseren van het doel waarvoor de persoonsgegevens zijn verzameld.
- Binnen een werkproces worden geen persoonsgegevens verwerkt die niet noodzakelijk zijn.
- Wanneer een nieuw werkproces ingericht wordt, dient voor aanvang vermelding te komen in het register van verwerkingsactiviteiten.
- Indien bij een nieuw werkproces een andere partij betrokken is, dient beoordeeld te worden of tussen de gemeente en deze partij een verwerkersovereenkomst opgesteld moet worden.

[2] Artikel 6,lid 1, onder a, AVG

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. Het gaat om bewustwording bij iedere medewerker. De meeste inbreuken worden namelijk nog steeds veroorzaakt door menselijke fouten. 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/privacy officer zodat zij hun controlerende en adviserende taken kunnen vervullen. Bewustwording vereist onderhoud. Dit houdt in dat privacy met regelmaat onder de aandacht dient te worden gebracht in onder andere werkoverleggen en bijvoorbeeld tijdens kennissessies of trainingen.

De gemeente Heumen creëert bewustwording op verschillende manieren. Om de bewustwording te vergroten worden periodiek bewustwordingsacties georganiseerd. Concreet houdt dat in dat de gemeente een terugkerende bewustwordingscampagne heeft. De gemeente Heumen wil hiermee onder andere het risico op datalekken en veiligheidsincidenten beperken. Daarnaast wordt informatieveiligheid en privacy periodiek onder de aandacht gebracht tijdens werkoverleggen en wordt belangrijke informatie over deze onderwerpen op het intranet geplaatst.

5. Beheer & 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. De wijze waarop hiermee omgegaan wordt, wordt weergegeven in het Informatiebeleidsplan. Deze bevat de visie en strategie op informatievoorziening.

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.
- 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.

Hoe lang blijven gegevens bewaard

- De AVG geeft geen concrete bewaartermijnen voor persoonsgegevens.
- Uitgangspunt van de gemeente Heumen is dat persoonsgegevens niet langer bewaard worden dan noodzakelijk is.
- De gemeente maakt gebruik van een geldige selectielijst. Dit is een lijst van werkprocessen met de bijbehorende bewaartermijnen.
- De bewaartermijnen in de selectielijst zijn veelal afgeleid van andere wetten waarin een bewaarplicht voor gegevens staat.
- In het register van verwerkingen worden de bewaartermijnen van persoonsgegevens weergegeven. Deze bewaartermijnen zijn gebaseerd op de bewaartermijnen uit selectielijsten.

Archivering

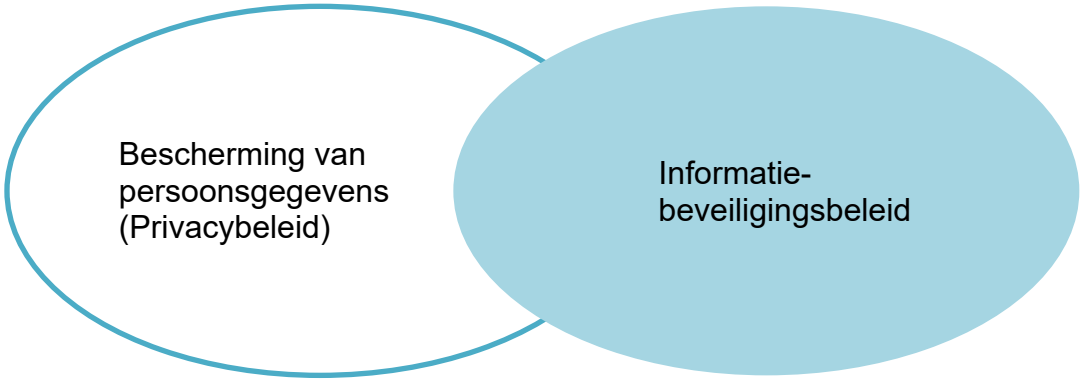
- Het bewaren van persoonsgegevens is alleen toegestaan zolang ze van belang zijn voor het doel waarvoor ze zijn verzameld.
- Voor sommige verwerkingen van persoonsgegevens geldt dat persoonsgegevens op grond van de Archiefwet of andere materiële wetten gedurende een minimale termijn bewaard moeten blijven.
- De Archiefwet houdt daarbij rekening met de privacy door zo nodig van persoonsgegevens de openbaarheid te beperken.
- Indien het onmogelijk is gebleken archiefbescheiden (met persoonsgegevens) direct te vernietigen na het verlopen van de bewaartermijn wordt dit niet gezien als een datalek of beveiligingsincident. Wel streven we er als gemeente naar om ons zo goed als mogelijk aan de bewaartermijn te houden.

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 multifactor authenticatie, autorisaties en controle hierop door middel van logging.
- De gemeente voorkomt hierbij ongeoorloofde toegang tot het gebruik van persoonsgegevens.

5.1. Informatiebeveiligingsbeleid

Informatiebeveiliging en privacy zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacy zijn echter twee verschillende begrippen. Ze hebben wel een gemeenschappelijk raakvlak.



Informatiebeveiliging heeft een bredere scope dan de bescherming van enkel persoonsgegevens. Informatiebeveiliging draait om de bescherming van alle gevoelige informatie tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Bijvoorbeeld ook de beveiliging van politiek gevoelige of financiële gegevens. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn.

Een adequate informatiebeveiliging (van persoonsgegevens) is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de Algemene Verordening Gegevensbescherming (AVG), de Europese privacywet. Artikel 32 van de AVG schrijft voor dat:

“Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen”.

Informatiebeveiliging maakt daarmee een onderdeel uit van de AVG. De AVG laat de inschatting van risico’s en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Wel geeft de AVG voorbeelden van mogelijke risico’s en maatregelen. Normenkaders als de BIO helpen de gemeente om de risico’s goed in te schatten en de benodigde maatregelen te treffen.

BIG - BIO

Sinds 2013 hebben de Nederlandse gemeenten gewerkt aan informatiebeveiliging op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Deze gold tot 1 januari 2020 en is vervangen worden door de Baseline Informatiebeveiliging Overheid (BIO). De BIO is in tegenstelling tot de BIG verplicht voor gemeenten. De aanpak van informatiebeveiliging in de BIO verschilt niet fundamenteel van die in de BIG. Het werk dat de gemeente Heumen de afgelopen jaren in de implementatie van de BIG heeft gestoken vormt dan ook de basis om de BIO te gaan implementeren.

ENSIA

ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer

overzicht over de stand van zaken van de informatieveiligheid en de gemeente hier ook beter op sturen.

Bijlage 1 Afkortingen en Begrippen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
Awb	Algemene wet bestuursrecht
BIG	Baseline Informatiebeveiliging Nederlandse Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BRP	Basisregistratie Personen
CISO	Chief Information Security Officer
ENSIA	Eenduidige Normatiek Single Information Audit
FG	Functionaris voor gegevensbescherming
OBDO	Overheidsbreed Beleidsoverleg Digitale Overheid
DPIA	Data Protection Impact Assessment
VNG	Vereniging van Nederlandse gemeenten