Privacybeleid gemeente Heerenveen

Het college van burgemeester en wethouders

De burgemeester; en

De raad van de gemeente Heerenveen;

Ieder voor zover het zijn eigen bevoegdheden betreft,

gelet op de AVG, de Wpg en de UAVG,

overwegende dat het wenselijk is om beleid vast te stellen voor de wijze waarop de raad bij de uitoefening van haar bevoegdheden omgaat met de verwerking van persoonsgegevens,

hebben op respectievelijk 4 maart 2025 (College van B&W en burgemeester), en 17 april 2025 (de Raad van de gemeente Heerenveen) besloten het volgende vast te stellen met de ingangsdatum 1 mei 2025:

Privacybeleid Gemeente Heerenveen

1. Inleiding

1.1 Algemeen

De gemeente Heerenveen hecht veel waarde aan de bescherming van privacy bij het verwerken van persoonsgegevens van haar inwoners. Persoonsgegevens moeten veilig en rechtmatig worden verwerkt om een betrouwbare overheid en samenwerkingspartner te zijn en te blijven.

Binnen overheidsinstanties, dus ook binnen de gemeente Heerenveen, wordt voortdurend gewerkt met persoonsgegevens van inwoners, medewerkers, en (keten)partners. Dit is nodig voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken.

Inwoners moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met persoonsgegevens omgaat. Wij vinden het belangrijk om transparant te handelen en te laten zien hoe wij persoonsgegevens verwerken. Daarvoor is dit privacybeleid opgesteld. Alle medewerkers van de gemeente Heerenveen moeten zich hieraan houden.

Het privacybeleid draagt bij aan:

- het beschermen van de privacy van personen van wie de gemeente gegevens verwerkt of laat verwerken;
- het maatschappelijk vertrouwen en draagvlak;
- het beheersen van afbreuk- en aansprakelijkheidsrisico’s;
- het kunnen afleggen van verantwoording aan het college/de burgemeester/de raad, waar nodig de Autoriteit Persoonsgegevens of de rechter;
- het in kunnen spelen op wettelijke en technologische ontwikkelingen;

- de bewustwording op het gebied van verwerking van persoonsgegevens bij medewerkers.

1.2 Definities en afkortingen
In dit privacybeleid worden de volgende definities en afkortingen gehanteerd:

Algemene Verordening Gegevensbescherming (AVG)
Algemene Verordening Gegevensbescherming (EU 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens).

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens bevordert en bewaakt de bescherming van persoonsgegevens.

Betrokkene(n)
De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de persoonsgegevens worden verwerkt. Dit kan gaan om bijvoorbeeld een inwoner, ondernemer, ambtenaar of contactpersoon van een (keten)partner.

Chief Information Security Officer (CISO)
De CISO binnen de organisatie is verantwoordelijk voor het informatiebeveiligingsbeleid.

Datalek
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Data Protection Impact Assessment (DPIA) of Gegevensbeschermingseffectbeoordeling (GEB)
In het Nederlands is Data Protection Impact Assessment vertaald naar gegevensbeschermingseffectbeoordeling. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen. Een DPIA is een beoordeling over het effect van de (nieuwe of aangepaste) verwerking op de bescherming van de persoonsgegevens en is verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. De beoordeling bevat ten minste een inschatting van de risico's van de verwerking en de vereiste beheersmaatregelen om tekortkomingen op te lossen.

DPIA-checklist
Een checklist om te beoordelen of een DPIA verplicht is of niet.

Functionaris Gegevensbescherming (FG)
Een onafhankelijke en deskundige interne toezichthouder en adviseur met wettelijke taken en bevoegdheden. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van alle privacy wet- en regelgeving waaronder de AVG.

Persoonsgegevens
Informatie uit data die direct of indirect betrekking heeft op een levend persoon. Denk hierbij aan naam, adres, geboortedatum.

Bijzondere persoonsgegevens
Deze gegevens gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeur of gezondheid. Deze zijn door de wetgever extra beschermd. Het is verboden om bijzondere persoonsgegevens te verwerken, tenzij er een wettelijke uitzondering van toepassing is.

Privacy Adviseur (PA)
In iedere team zijn er Privacy Adviseurs die in de uitvoering helpen de AVG toe te passen. Zij zijn het eerste aanspreekpunt voor de collega's binnen de teams.

Privacy Officer (PO)
De Privacy Officers zijn adviseurs die de uitvoering van de privacywetgeving en het beleid doen. Zij bevorderen en adviseren onze gemeente over de bescherming van persoonsgegevens, stellen beleid op en ondersteunen de teams bij allerlei privacyzaken.

Verwerker
De organisatie, of persoon, die in opdracht en ten behoeve van de verwerkingsverantwoordelijke bepaalde onderdelen van of de gehele verwerking voor zijn rekening neemt.

Verwerkersovereenkomst
Een overeenkomst waarin de afspraken staan hoe een verwerker met de persoonsgegevens moet omgaan bij verwerkingen in opdracht en ten behoeve van de verwerkingsverantwoordelijke.

Verwerking
Alles wat je met persoonsgegevens kunt doen; 'het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen van gegevens.'

Verwerkingsverantwoordelijke
De organisatie of persoon die bepaalt waarom de verwerking van persoonsgegevens plaatsvindt en vaststelt met welke middelen dat gebeurt.

Wet politiegegevens (Wpg)
De Wet politiegegevens regelt de verwerking van persoonsgegevens voor de uitoefening van de politietaak door onder meer de politie en de bijzondere opsporingsdiensten (BOD), waaronder ook de buitengewone opsporingsambtenaren (boa's) vallen.

2. Privacy

2.1 Reikwijdte en afbakening
Het privacybeleid is van toepassing op:

- alle processen binnen de gehele organisatie waarbinnen persoonsgegevens worden verwerkt;
- digitale oplossingen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is;
- alle ruimten en digitale oplossingen die door bestuurders en medewerkers intern en extern worden gebruikt waar(op) persoonsgegevens worden verwerkt;
- alle geldende normen en regels op het gebied van privacy.

Voor het grootste deel van de verwerkingen is het college van burgemeester en wethouders (hierna: het college) de verwerkingsverantwoordelijke. Daar waar een specifieke taak is toebedeeld aan een ander bestuursorgaan, is dit bestuursorgaan ook de verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens. Daarom wordt dit privacybeleid niet alleen vastgesteld door het college, maar eveneens door de burgemeester als zelfstandig bestuursorgaan en door de gemeenteraad.

Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente gegevens verwerkt (of laat verwerken).

- De gemeente verwerkt bij het uitvoeren van haar taken alle mogelijke categorieën van persoonsgegevens, waaronder:
- Algemene persoonsgegevens:
    - Naam
    - Adres, postcode, woonplaats
    - Geboortedatum
    - Geslacht
    - Burgerlijke staat
- Bijzondere persoonsgegevens:
    - Burgerservicenummer
    - Ras en etnische afkomst
    - Politieke opvattingen
    - Gegevens met betrekking tot gezondheid
    - Strafrechtelijke veroordelingen en strafbare feiten

In deze tijd gaat ook de gemeente mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie en transparantie.

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. Het is het geheel aan maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie garanderen.

2.2 Wettelijk kader

De juridische grondslag voor privacy is terug te vinden in verschillende wet- en regelgeving. De bescherming van de privacy bij de verwerking van persoonsgegevens is een grondrecht. Dit is geregeld in:

- de Grondwet (artikel 10 Grondwet);
- het Handvest van de grondrechten van de Europese Unie (EHRM);
- het Europees Verdrag voor de Rechten van de Mens (EVRM);
- het Internationaal Kinderrechtenverdrag (IVRK).

De bescherming van de persoonsgegevens wordt ingevuld door wetten, namelijk:

- de Europese Algemene Verordening Gegevensbescherming (AVG);
- de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

De verwerking van strafrechtelijke persoonsgegevens wordt ingevuld door:

- Wet politiegegevens (Wpg).

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de privacy bij de verwerking van persoonsgegevens zoals in de volgende wetten:

- Wet maatschappelijke ondersteuning (Wmo 2015);
- Jeugdwet (Jw);
- Wet Basisregistratie Personen (Wet Brp);
- Participatiewet (Pw);
- Wet algemene bepalingen Burgerservicenummer (Wabb);
- Wet open overheid (Woo).

2.3 Uitgangspunten
Ook als de gemeente persoonsgegevens mag (of zelfs moet) verwerken, zijn er verschillende zaken om rekening mee te houden. Bijvoorbeeld: De gemeente moet altijd belangen afwegen, mag niet meer persoonsgegevens verwerken dan nodig en mag gegevens niet zomaar doorspelen aan andere instanties.

In deze paragraaf lichten we toe waar de gemeente Heerenveen rekening mee houdt.

a. Belangenafweging
Bij verwerking van persoonsgegevens zijn vaak diverse belangen gemoeid. Dat vraagt om een zorgvuldige belangenafweging tussen het belang van de betrokkene(n) en het publieke (algemeen) belang en de belangen van betrokkenen ten opzichte van elkaar. In een belangenafweging worden de uitgangspunten zoals beschreven in dit hoofdstuk meegewogen. De gemeente maakt een analyse, zodat de risico's van de verwerking vooraf inzichtelijk zijn. Na een onderbouwde belangenafweging wordt besloten of de gegevensverwerking kan plaatsvinden. Daarbij worden risico's zoveel mogelijk verkleind met de juiste maatregelen.

<u>Belang van de betrokkene</u>
Een betrokkene wil dat zijn persoonsgegevens veilig en betrouwbaar worden verwerkt. Transparantie over wat wij met de persoonsgegevens doen, wordt daarbij gewaarborgd. Aan de ene kant heeft de betrokkene er belang bij dat zo min mogelijk gegevens worden opgeslagen en niet langer worden bewaard dan noodzakelijk. Aan de andere kant verwacht de betrokkene efficiënte dienstverlening.

<u>Publiek belang</u>
De organisatie van de gemeente Heerenveen voert op diverse gebieden wettelijke- en

bestuurlijke taken uit. Om deze taken goed te volbrengen is het noodzakelijk dat er persoonsgegevens worden verwerkt.

Belang van betrokkenen ten opzichte van elkaar
De bescherming van de rechten van de ene betrokkene kan ingrijpende gevolgen hebben voor de belangen en de rechten van de ander.

b. Rechtmatig, behoorlijk, en transparant
Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken:

- rechtmatig: de hoofdregel is dat de verwerking van persoonsgegevens alleen toegestaan is in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze;
- behoorlijk: persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene(n) zelf. De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden;
- transparant: de gemeente is transparant over de manier waarop de gemeente met persoonsgegevens omgaat. De gemeente praat niet over de betrokkene(n), maar met de betrokkene(n). De betrokkenen worden op heldere en laagdrempelige wijze geïnformeerd over de manier waarop met hun persoonsgegevens om wordt gegaan.

De gemeente houdt zich hierbij ook aan de volgende uitgangspunten:

c. Verantwoording
De gemeente treft passende en organisatorische maatregelen om te zorgen dat er voor het hele gegevensverwerkingsproces en alle daarbij betrokken partijen aan de AVG wordt voldaan. Dat betekent bijvoorbeeld dat we een verwerkingsregister bijhouden, een data protection impact assessment (DPIA) uitvoeren bij gegevensverwerkingen met een hoog privacyrisico en een datalekregister bijhouden.

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar is extern en intern toezicht op. De Autoriteit Persoonsgegevens (hierna: AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (hierna: FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. De gemeente stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

d. Verdere verwerking
Het uitgangspunt is dat persoonsgegevens alleen worden verwerkt voor het doel waarvoor ze zijn verkregen (bijvoorbeeld persoonsgegevens in een vergunningaanvraag). Persoonsgegevens kunnen echter in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, en er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. De gemeente voert, voordat de verwerking start, eerst een toets uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

e. Dataminimalisatie, bewaartermijn en opslagbeperking
De gemeente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. Niet meer dan dat. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk, worden minder of geen persoonsgegevens verwerkt. Ook hebben alleen de medewerkers voor wie dit noodzakelijk is, toegang tot de gegevens.

Onderdeel van dataminimalisatie is ook dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verwerkt. De bewaartermijnen van persoonsgegevens lopen hierdoor uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Deze komen ook terug in de vastgestelde selectielijsten die voortvloeien uit de Archiefwet, welke aangeven hoe lang informatie bewaard moet worden. De Archiefwet en de AVG hebben dus verschillende uitgangspunten. Hierdoor moet in de praktijk soms het belang van archivering worden afgewogen tegen het belang van bescherming van persoonsgegevens.

Als registratie van de persoonsgegevens niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd. Alleen als de bewaartermijn niet op basis van wettelijke bepalingen of de selectielijsten kan worden vastgesteld, stelt de gemeente de bewaartermijn vast op basis van noodzakelijkheid. Er is een uitzondering op dit principe voor wat betreft gegevensverwerking ten aanzien van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

f. Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. De persoonsgegevens zijn overeenkomstig het classificatieniveau beveiligd door middel van passende technische en organisatorische maatregelen.

g. Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken met de derden over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. Ook de derden moet zich houden aan de privacyregelgeving en aan het privacybeleid van de gemeente. De AVG verplicht gemeenten tot het maken van contractuele afspraken met derden in de vorm van verwerkersovereenkomsten of gegevensuitwisselingsovereenkomsten.

h. Subsidiariteit
De verwerking van persoonsgegevens is alleen toegestaan wanneer het doel niet op een andere manier kan worden bereikt. Als dit doel ook bereikt kan worden met geen of minder (belastende) persoonsgegevens, dan wordt daarvoor gekozen.

i. Proportionaliteit
De persoonsgegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel.
Het doel van de verwerking van persoonsgegevens moet in verhouding staan tot de inbreuk op privacy van de betrokkene. Dit betekent onder andere dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk.

j. Technische en organisatorische veiligheid
Voor de opgeslagen gegevens, bijvoorbeeld in een database, register of bestand, zijn passende technische en organisatorische veiligheidsmaatregelen getroffen. We kunnen binnen de gemeente nog zo zorgvuldig met persoonsgegevens omgaan – als die gegevens (te) gemakkelijk in de handen van onbevoegden kunnen komen, dan bereiken we ons doel niet. De gemeente Heerenveen maakt daarom gebruik van de Baseline Informatiebeveiliging Overheid (BIO) en het daarbij horende niveau van informatiebeveiliging.

Verder zijn uitsluitend geautoriseerde gebruikers bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

k. Transparantie en informatieplicht
De gemeente is transparant over de manier waarop zij met persoonsgegevens omgaat. De gemeente praat niet over de betrokkenen, maar met de betrokkenen. De gemeente informeert de betrokkene over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt en waarom en voor welk doel dat gebeurt.

Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

2.5 Rechtsgrondslagen
Persoonsgegevens mogen niet zomaar worden verwerkt. Dat mag alleen als hiervoor een grondslag uit de wet (de AVG) is en op een behoorlijke en zorgvuldige wijze. Dit betekent onder andere dat verwerkingen alleen plaatsvinden als hier een rechtmatige verwerkingsgrondslag bestaat. Meestal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

De gemeente verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De gegevensverwerking moet een specifiek doel dienen. Nog voordat er wordt begonnen met het verwerken van persoonsgegevens moet een doel worden afgesproken. Bij deze doeleinden kan worden gedacht aan het voorzien in informatiebehoeften van verzoekers, het beoordelen van een subsidieaanvraag of het behandelen van klachten. De verwerkingsdoeleinden staan opgenomen in het verwerkingsregister.

<u>Grondslag en doelbinding</u>

- De gemeente verwerkt alleen persoonsgegevens indien hiervoor een rechtmatige grondslag bestaat:

- voor de uitvoering van een taak in het algemeen belang of voor de uitoefening van het openbaar gezag (deze grondslag is het meest voorkomend i.v.m. uitvoeren publiekrechtelijke taken);

- om te voldoen aan een wettelijke verplichting (ook deze grondslag wordt veel gebruikt door de gemeente. Hierbij staat de verplichting om persoonsgegevens te verwerken letterlijk in de landelijke wetgeving, bijvoorbeeld de Participatiewet);

- voor de uitvoering van een overeenkomst met de betrokkene (bijvoorbeeld het verwerken van persoonsgegevens in de administratie bij een koopovereenkomst);

- bij uitzondering: ter bescherming van vitale belangen (situaties van leven of dood);

- bij uitzondering: betrokkene heeft toestemming gegeven voor de verwerking (let op: betrokkene moet een vrije keuze hebben en dus ook kunnen weigeren. Daarom kan toestemming in het publiekrecht bijna nooit worden gebruikt als grondslag).

- De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt.

De gemeente werkt hierbij vanuit de bedoeling. Dit betekent dat als er onduidelijkheid is over het wel of niet mogen verwerken, het doel waarvoor gegevens worden verwerkt doorslaggevend is. De gemeente zorgt ervoor dat de motivatie of de belangenafweging hiervan schriftelijk wordt vastgelegd.

2.5 Risico's

Bij schending van de privacywet- en regelgeving is de gemeente wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:

- het betalen van een schadevergoeding. Een benadeelde kan hier soms aanspraak op maken
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de AP als landelijk toezichthouder een boete opleggen. Onder de AVG kunnen de (zeer) forse boetes oplopen tot maximaal € 20 miljoen.

Binnen bepaalde domeinen en ketens worden bijzondere persoonsgegevens, zoals medische gegevens of strafrechtelijke gegevens verwerkt. Voorbeelden zijn het sociaal domein en de keten openbare orde en veiligheid. Aan de verwerking van deze persoonsgegevens zijn aanvullende voorwaarden gesteld (artikel 9 en 10 AVG), omdat er sprake is van (zeer) gevoelige informatie over personen. De gemeente zorgt voor adequate oplossingen en maatregelen voor het veilig overdragen van deze gegevens wanneer dit noodzakelijk is, bijvoorbeeld naar externe partijen zoals de politie.

De risico’s van schending van de privacy voor personen variëren van ongemak, stigmatisering, en uitsluiting tot identiteitsfraude of chantage.

Om de risico’s te beperken moeten maatregelen worden getroffen. Leidend daarbij is dat privacy-eisen zoveel mogelijk worden geïntegreerd in regulier en/of al bestaand beleid en vertaald worden naar processtappen die worden geïntegreerd in het reguliere werkproces.

3. Verantwoordelijkheden en taken

3.1 Overzicht

De afzonderlijke bestuursorganen zijn ieder verantwoordelijk voor een zorgvuldige gegevensverwerking bij de uitvoering van zijn of haar taken. Binnen het privacy-werkveld hebben deze verschillende bestuursorganen te onderscheiden rollen. Ook zijn er binnen de ambtelijke organisatie van de gemeente taken belegd bij een aantal specifieke personen en functies. We lichten de taakverdeling hieronder toe.

	Verantwoordelijk	
R	Responsible/ Feitelijk verantwoordelijk	• Teammanagers en Concerndirecteuren • De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/ Eindverantwoordelijk	• Het college van B&W
C	Consulted/ Adviserend	• Chief Privacy Officer en Privacy Officers • Privacy Adviseurs • CISO • Functionaris Gegevensbescherming
I	Informed/ Geïnformeerd	• Gemeenteraad (privacyrechtelijk geen controlerende taak, maar op basis van de Gemeentewet en de decentralisatiewetgeving een bestuurlijke toezichttaak) • Functionaris Gegevensbescherming • Belanghebbende(n)/Betrokkene(n)

Team	Betrokkenheid
Communicatie	In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van team communicatie betrokken.

Audit / Concern Control	Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).

3.2 Het college
Het college:

- Is belast met de waarborging van de bescherming van persoonsgegevens, op een manier die in overeenstemming is met de geldende wet- en regelgeving en de zorgvuldigheidsvereisten. Er is een directe relatie met de beginselen van behoorlijk bestuur;
- stelt kaders voor de bescherming van de privacy op basis van wet- en regelgeving;
- evalueert de toepassing en werking van het privacybeleid op basis van rapportage van de FG;
- rapporteert/legt verantwoording af aan de raad over de uitvoering/realisatie van het privacybeleid;
- stelt het privacybeleid vast.

3.3 De concerndirectie
De concerndirecteur(en) en de algemeen directeur zijn verantwoordelijk voor kaderstelling en sturing. Deze zorgen ervoor:

- dat er gestuurd wordt op concernrisico's;
- dat er gecontroleerd wordt of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkene(n) te beschermen;
- dat de FG, de CISO en de PO naar behoren en tijdig worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.4 De teammanagers
De teammanager is verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar team plaatsvindt. Dit betekent onder meer de verantwoordelijkheid voor:

- het bijhouden en actualiseren van verwerkingen voor het verwerkingsregister;
- het ondertekenen van verwerkersovereenkomsten;
- het ondertekenen van brieven naar betrokkenen en ontvangers bij datalekken;
- bewustwording creëren rondom informatieveiligheid en privacy bij de medewerkers;
- het invullen van de DPIA checklist en de uitvoering van de DPIA;
- de inhoudelijke behandeling van privacyklachten;
- de inhoudelijke behandeling van verzoeken van rechten van betrokkenen.

De teammanager wordt in de uitvoering van zijn verantwoordelijkheid ondersteund door de PA (zie 3.9) binnen het team.

3.5 De Functionaris Gegevensbescherming (FG)

De FG is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG heeft in ieder geval de volgende verantwoordelijkheden:

- het monitoren, informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- het toezien op naleving van de AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming namens de Autoriteit Persoonsgegevens;
- het toezien op naleving van het gemeentelijke beleid en de verwerker met betrekking tot de bescherming van persoonsgegevens;
- het toezien op naleving van de Wpg;
- het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- het geven van advies met betrekking tot de DPIA/GEB en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- het inzetten van controle- en monitoringsbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- het samenwerken met de AP;
- het optreden als contactpunt voor de AP;
- het in samenspraak met de CISO adviseren over digitale oplossingen en de informatiebeveiliging van gegevensverwerking;
- het toezien op het verwerkingsregister;
- het bij inbreuk persoonsgegevens (meldplicht datalekken) adviseren over de ernst en omvang ervan;
- het adviseren over privacyklachten
- het adviseren over de afhandeling van verzoeken van betrokkenen met betrekking tot de verwerking van hun gegevens en het uitoefenen van hun rechten (zoals o.a. recht op inzage).

3.6 Chief Information Security Officer (CISO)

De CISO is op organisatieniveau onder meer verantwoordelijk voor:

- het adviseren over informatiebeveiligingsbeleid;
- de toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens;
- het coördineren van de uitvoering van het beleid;
- het adviseren over informatiebeveiliging;
- het tijdig melden van informatiebeveiligingsincidenten bij PO/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident;
- het beheersen van risico’s;
- het opstellen van rapportages met betrekking tot informatiebeveiligingsbeleid.

3.7 *Chief Privacy Officer (CPO)*
De CPO heeft een aansturende, monitorende, en ondersteunende rol voor de taken van de PO's (zie paragraaf 3.8).

3.8 De Privacy Officer (PO)
De PO werkt nauw samen met de PA's, de FG, de CISO en de CPO en voert onder andere de volgende taken uit:

- bevordert bewustwording op het gebied van privacy en informatieveiligheid binnen de organisatie;
- adviseert over de verwerkingsgrondslag;
- adviseert de organisatie over de bescherming van persoonsgegevens (inclusief scholing);
- stelt algemeen privacybeleid (inclusief verklaringen, reglementen en procedures) op;
- stelt privacymodellen (waaronder brieven en overeenkomsten) op;
- stelt jaarlijks een privacyplanning op;
- ondersteunt het team bij het opstellen van specifiek privacybeleid per team;
- adviseert over de juridische aspecten in de verwerkersovereenkomsten;
- controleert verwerkersovereenkomsten;
- heeft een coördinerende en adviserende rol bij het verwerkingsregister;
- is verantwoordelijk voor het vullen van het verwerkingsregister;
- adviseert over compliance-vraagstukken binnen de organisatie;
- adviseert bij klachtprocedures;
- heeft een coördinerende en adviserende rol bij veiligheidsincidenten en datalekken;
- houdt een intern datalekregister bij;
- heeft een ondersteunende en adviserende rol bij verzoeken van betrokkenen die gebruik maken van hun rechten;
- coördineert en adviseert de teams bij het uitvoeren van DPIA's;
- ondersteunt en adviseert de PA's op de teams bij privacyvraagstukken.

3.9 De Privacy Adviseur (PA)
De PA werkt nauw samen met de FG en de PO's en voert onder andere de volgende taken uit:

- bevordert bewustwording op het gebied van privacy en gegevensbescherming binnen hun team;
- adviseert het team over de bescherming van persoonsgegevens;
- heeft een uitvoerende rol bij privacyvraagstukken binnen hun team en sturen deze indien nodig of gewenst naar een PO;
- ondersteunt de PO's;
- is verantwoordelijk voor het aanleveren van gegevens voor het verwerkingsregister aan de PO's;
- ondersteunt bij de uitvoering van een DPIA.

3.10 De medewerkers
Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen bij de uitvoering van hun werkzaamheden. Dat betekent dat iedereen zorgt voor een veilige, rechtmatige, behoorlijke en transparante verwerking

van persoonsgegevens. De medewerkers kunnen hiervoor gebruik maken van het stroomschema dat bijgevoegd is in bijlage A. “Afwegingskader zorgvuldig verwerken en delen van persoonsgegevens”.

4. Rechten van betrokkenen

De AVG is voor een heel groot deel gericht op het verbeteren van de privacyrechten van de betrokkene(n). Dit betekent dat er meer aandacht is voor de rechten van de betrokkene(n) en dat een procedure daarvoor van groot belang is. Daarom worden de rechten van betrokkene(n) en hoe de gemeente verzoeken op grond van deze rechten behandelt, hierna beschreven.

4.1 Welke rechten kunnen betrokkenen uitoefenen?

4.1.1 Recht op informatie
De gemeente moet de betrokkene(n), op het moment dat de verwerking van persoonsgegevens plaatsvindt, hierover informeren. Dit recht vangt aan bij het vragen van persoonsgegevens (aan betrokkene(n)) of bij de eerste verwerking van de persoonsgegevens (bij gegevens verkregen van anderen). Het informeren van de betrokkene(n) kan op individueel niveau plaatsvinden, maar ook in de vorm van een algemene informatievoorziening door bijvoorbeeld het verwerkingsregister openbaar te maken en beschikbaar te houden voor betrokkenen. Op zijn/haar verzoek verstrekt de gemeente informatie aan de betrokkene(n).

4.1.2 Recht op inzage
Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, hun gegevens worden verwerkt. Wanneer gegevens verwerkt worden, hebben zij het recht om inzage te verkrijgen in de persoonsgegevens die verwerkt worden.

4.1.3 Recht op rectificatie
Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren. Met inachtneming van de doeleinden van de verwerking, heeft de betrokkene het recht onvolledige persoonsgegevens aan te (laten) vullen.

4.1.4 Recht op gegevenswissing (vergetelheid)
In gevallen waar de betrokkene toestemming heeft gegeven aan de gemeente om gegevens te verwerken, dan heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen. Hierbij vindt een belangenafweging plaats.

4.1.5 Recht van beperking van de verwerking
Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken. Bijvoorbeeld als de betrokkene heeft gevraagd om gegevens te wijzigen, maar de gemeente dit verzoek nog moet beoordelen.

4.1.6 Recht op overdraagbaarheid (dataportabiliteit)
Betrokkenen kunnen op basis van de AVG gegevens die hem/haar zelf betreffen opvragen in gestructureerde, gangbare en digitaal leesbare vorm. Ook heeft hij/zij het

recht deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen.

Dit recht kan alleen uitgeoefend worden ten aanzien van digitale gegevens en als de gegevensverwerking heeft plaatsgevonden op basis van een overeenkomst of door toestemming. Dit komt bij de gemeente niet tot zeer weinig voor. Het recht op dataportabiliteit bij de gemeente is daarom sterk beperkt.

4.1.7 Recht van bezwaar (verzet)
Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens als gegevensverwerking plaatsvindt op grond van een algemeen belang of een gerechtvaardigd belang. De gemeente zal de verwerking van de gegevens dan staken, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Wanneer een beroep wordt gedaan op het recht van bezwaar is er automatisch, gedurende de periode die nodig is om een besluit te nemen, sprake van een beperking van de verwerking van de persoonsgegevens. Het recht op bezwaar zoals hier genoemd is niet hetzelfde als het indienen van bezwaar op grond van de Algemene wet bestuursrecht.

4.1.8 Recht op menselijke blik bij besluiten
Betrokkenen hebben het recht op een menselijke blik bij besluiten. Dit betekent dat mensen een nieuw, door een persoon genomen besluit, kunnen vragen als zij een geautomatiseerd besluit van een organisatie hebben ontvangen.

4.2 Hoe oefenen betrokkenen hun rechten uit

4.2.1 Controle identiteit
De betrokkene kan het verzoek via het webformulier, schriftelijk of mondeling indienen. Na ontvangst van een verzoek tot uitoefening van de in paragraaf 4.1 genoemde rechten, stuurt de gemeente een bevestigingsbrief. Hierin kan worden verzocht dat de betrokkene zich identificeert. Voordat de gemeente het verzoek namelijk in behandeling kan nemen, wordt de identiteit van de betrokkene altijd gecontroleerd. De betrokkene kan hiervoor een afspraak maken en zich identificeren bij Burgerzaken. Indien het verzoek gaat over een kind onder de 16 jaar, dan is het noodzakelijk dat de verzoeker ouderlijk gezag heeft. De gemeente controleert dat in het gezagsregister.

4.2.2 Behandeling van het verzoek
De gemeente handelt het verzoek binnen één maand af. Als het verzoek complex is of als veel verzoeken tegelijkertijd behandeld moeten worden, dan kan de termijn verlengd worden tot drie maanden nadat de gemeente het verzoek heeft ontvangen.

Als het verzoek om veel gegevens gaat of als het verzoek onduidelijk is, dan kan de gemeente de betrokkene verzoeken om zijn/haar verzoek te specificeren.

4.2.3 Beslissing op verzoek
In de beslissing laat de gemeente weten of en hoe aan het verzoek zal worden voldaan. Indien verlenging van de beslistermijn noodzakelijk is, dan zal binnen de beslistermijn dit worden bericht aan de betrokkene.

In het geval de gemeente niet – of gedeeltelijk – aan het verzoek voldoet, wordt dit altijd gemotiveerd in het besluit. Het kan bijvoorbeeld zijn dat bepaalde gegevens vanwege de openbare orde en veiligheid niet gedeeld mogen worden. Ook is het niet toegestaan om gegevens van andere personen in te zien.

5. Verplichtingen AVG

5.1 Register van verwerkingsactiviteit

De gemeente houdt een register van de verwerkingsactiviteiten bij. Het register bevat onder andere:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, indien van toepassing, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van de soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Indien van toepassing: een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

5.2 Datalekken

Een datalek is een beveiligingsincident waarbij persoonsgegevens in onbevoegde handen komen. Dat kan een grote impact hebben op betrokkenen en op de gemeente als organisatie. Een datalek zit in een klein hoekje en het is niet mogelijk om datalekken volledig buiten de deur te houden. De gemeente heeft daarom meerdere processen, systemen en acties ingezet om datalekken te voorkomen. Zo worden medewerkers op het intranet en via bijeenkomsten voorgelicht over het voorkomen, herkennen en melden van een datalek. Verder maakt de gemeente afspraken met derden die werkzaamheden voor de gemeente uitvoeren over het melden van datalekken.

De gemeente zet zich in voor het realiseren van een omgeving waarin het snel melden van mogelijke datalekken wordt gestimuleerd. Een datalek met een hoog risico wordt daardoor binnen 72 uur gemeld worden door de FG bij de AP en/of betrokkenen. Naast een morele verplichting heeft de gemeente ook te maken met een financieel risico als niet aan de meldplicht wordt voldaan. Bij het niet of niet tijdig melden loopt de gemeente een risico op een boete van de AP.

Medewerkers melden een (potentieel) datalek via het intranet. De PO’s en de CISO ontvangen de melding. In overleg met de medewerker beoordelen de PO’s en/of CISO het datalek en de mogelijkheden tot het herstel of stoppen van het datalek. Ook wordt de FG betrokken bij de afhandeling van het datalek. De FG kan dan bijvoorbeeld adviseren over het informeren van de slachtoffers.

De PO’s houden een intern datalekregister bij waarin de gemelde datalekken worden geregistreerd. In het register wordt een omschrijving, de vervolgstappen en een evaluatie opgenomen. Dit register wordt door de FG geraadpleegd voor het opstellen van het jaarverslag.

5.3 Data protection impact assessment

Is de gemeente van plan persoonsgegevens te verwerken, maar levert dat waarschijnlijk een hoog privacyrisico op? Dan is de gemeente verplicht eerst een 'data protection impact assessment' (DPIA) uit te voeren. Dit is een instrument om vooraf de privacyrisico's in kaart te brengen, zodat de gemeente maatregelen kan nemen om risico's te verkleinen. Bij het uitvoeren van een DPIA worden de voor *Gegevensbescherming door ontwerp* en *Gegevensbescherming door standaardinstellingen* noodzakelijke aspecten (bijvoorbeeld dataminimalisatie en bewaartermijnen) meegenomen in de voorgenomen verwerking. Zo worden in bijvoorbeeld formulieren geen gegevens gevraagd die overbodig zijn. Dit helpt tevens mee aan het principe van dataminimalisatie. Op deze manier wordt gewaarborgd dat nieuwe verwerkingen conform de normen van *Gegevensbescherming door ontwerp* en *Gegevensbescherming door standaardinstellingen* worden ingericht.

De gemeente is constant in ontwikkeling op onder andere het gebied van technologie, voorzieningen en digitale dienstverlening. Door ontwikkeling kan er sprake zijn van een nieuwe verwerking of een wijziging van een bestaande verwerking. Bij dit soort veranderingen moeten de privacyrisico's in kaart worden gebracht zodat een juiste belangenafweging kan plaatsvinden. Het in kaart brengen van de privacyrisico's gebeurt aan de hand van een DPIA-checklist en de lijst van de AP.

Op basis van de DPIA-checklist die binnen de gemeente wordt gehanteerd, wordt bepaald of er sprake is van een hoog privacyrisico. Als er geen sprake is van een hoog risico, dan kan een advies van de PO en/of FG volstaan. Als er wel sprake is van een hoog risico, dan moet een DPIA worden uitgevoerd. Een DPIA geeft inzicht in welke maatregelen nodig zijn om het risico te verkleinen naar een minimaal en acceptabel niveau. Hiermee wordt invulling gegeven aan een juiste belangenafweging. Een advies hierop van de FG is verplicht.

Voor het uitvoeren van een DPIA wordt gebruik gemaakt van een modelformulier, die gebaseerd is op het model van de Informatiebeveiligingsdienst (IBD).

Processen kunnen regelmatig worden aangepast met mogelijke effecten op de verwerking van persoonsgegevens. Bij een wijziging in een proces is het noodzakelijk om een eerder uitgevoerde DPIA te herzien om te beoordelen of de wijziging nieuwe risico's met zich meebrengt. Wijzigingen in een proces kunnen kleine risico's vergroten en grote risico's verkleinen. Dit wordt meegenomen bij het herzien van een DPIA.

Omdat de teammanager verantwoordelijk is voor de privacy binnen zijn of haar team, is hij/zij verantwoordelijk voor het (laten) uitvoeren van de DPIA en het nemen van de in de DPIA genoemde maatregelen. De PO ondersteunt en adviseert bij het maken van een DPIA, die uitgevoerd wordt door een team collega's met een diversiteit aan deskundigheid (zoals een proceseigenaar, een PA, een technisch en/of functioneel beheerder).

5.4 Gegevensbescherming door ontwerp en standaardinstellingen

<u>Gegevensbescherming door ontwerp</u>

Gegevensbescherming door ontwerp (ook wel 'privacy by design') houdt in dat er vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:

- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens;
- de technische en organisatorische maatregelen die hiervoor nodig zijn.

Privacy wordt aan het begin van de uitvoer van projecten meegenomen. Dit wordt gewaarborgd door een PO mee te laten kijken in de voorfase van een project. De FG ziet erop toe dat dit gebeurt.

Gegevensbescherming door standaardinstellingen
Gegevensbescherming door standaardinstellingen (ook wel 'privacy by default') houdt in dat de standaardinstellingen van een programma zodanig worden ingesteld dat de privacybescherming maximaal wordt gewaarborgd.

5.5 Verwerkersovereenkomsten met derden
Bij veel gemeentelijke processen worden gegevens verwerkt door derden. Denk hierbij aan uitbestede werkzaamheden of samenwerkingsverbanden. Het college blijft verantwoordelijk voor de verwerking van de gegevens. Zij moet er daarom op toezien dat gegevens juist verwerkt en beveiligd worden.

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensverwerking en -uitwisseling aan moet voldoen.

Er worden bijvoorbeeld afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt;
- hoe de verwerker met de persoonsgegevens moet omgaan;
- welke beveiligingsmaatregelen moeten worden genomen;
- melden van een datalek aan de verantwoordelijke;
- welke vormen van toezicht de verantwoordelijke mag uitoefenen;
- de geheimhoudingsplicht;
- inschakeling van derden en onderaannemers door de verwerkers;
- locatie van de data;
- aansprakelijkheid in geval van schade door het niet naleven van regelgeving.

Als voor deze afspraken een verwerkersovereenkomst wordt afgesloten, gebruikt de gemeente de standaardovereenkomst van de IBD/VNG.

De teammanager dat een dergelijke uitbesteding, samenwerking of uitwisseling aangaat, ziet toe op de totstandkoming van deze afspraken en ondertekent de overeenkomst. De PO en de CISO worden bij de totstandkoming betrokken.

De gemeente geeft in beginsel geen persoonsgegevens door aan (organisaties in) een land dat buiten de Europese Economische Ruimte ligt of internationale organisaties. Als zij dit toch gaat doen, dan zal dit onder de voorwaarden uit de AVG zijn.

6. Bewustwording
Voor het borgen van privacy is het vooral van belang dat er bewust met persoonsgegevens wordt omgegaan. Het is noodzakelijk om het bewustzijn van alle medewerkers voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en

veilig en verantwoord gedrag wordt aangemoedigd. De gemeente zorgt ervoor dat hier voortdurend aandacht voor is.

Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies en tijdens de introductiebijeenkomst. De gemeente verwacht van elke medewerker een adequaat niveau van bewustwording op het gebied van privacy en informatiebeveiliging. Er worden diverse (online) middelen ingezet om dit te bereiken.

Via e-learnings, digitale awareness tools, organisatiebrede (fysieke) bijeenkomsten en interne informatiepagina's wordt bewustwording op het gebied van privacy en informatiebeveiliging gestimuleerd. Onder andere komen de volgende thema's komen hierbij aan bod:

- Herkennen en melden van een datalek;
- De informatiebewuste medewerker;
- Het kwalificeren van persoonsgegevens en overige informatie;
- Het uitvoeren van een DPIA.

Door één of meerdere PO's wordt jaarlijks een planning opgesteld om de bewustwording binnen de gehele organisatie op peil te houden. De FG heeft hierbij een adviserende en toezichthoudende rol.

7. Slotbepalingen

7.1 Uitwerking privacybeleid

Om de bescherming van (het werken met) persoonsgegevens binnen de gemeente Heerenveen te optimaliseren, kan dit privacybeleid nader worden uitgewerkt in domeinspecifieke of onderwerpspecifieke uitwerkingskaders. Indien hiertoe wordt overgegaan, dan worden deze uitwerkingskaders als bijlagen bij dit privacybeleid gevoegd. De uitwerkingskaders worden vastgesteld door het college.

7.2 Evaluatie

We evalueren het privacybeleid eens per drie jaar. Indien daartoe aanleiding bestaat, wordt het privacybeleid (eerder) beoordeeld en zo nodig bijgesteld.

7.2 Inwerkingtreding

Dit privacybeleid treedt in werking op de dag na bekendmaking.

7.3 Intrekken privacyreglement

Bij de inwerkingtreding van dit privacybeleid wordt het privacyreglement gemeente Heerenveen, vastgesteld op 28 januari 2021, ingetrokken.