Privacybeleid
Gemeente Heemstede

Inhoudsopgave

1. Inleiding

Binnen de gemeente Heemstede wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met zijn persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. Het dataverkeer neemt toe en er worden meer gegevens verzameld en gedeeld. De hoeveelheid gevoelige informatie van personen neemt toe (bijvoorbeeld jeugdzorg, maatschappelijke ondersteuning en de zorg voor chronisch zieken, ouderen en gehandicapten), net als de risico's van bijvoorbeeld cybercrime. De samenleving wordt steeds kritischer en de burgers hebben een grotere behoefte aan rechten om inzicht te krijgen in de verwerking van hun persoonsgegevens.

Op 25 mei 2018 is de Algemene verordening gegevensbescherming in werking getreden. Het doel van de verordening is met name een nog betere bescherming van persoonsgegevens te verzekeren en het vrije verkeer van persoonsgegevens binnen de Europese Unie te waarborgen.

In dit beleid wordt uitgewerkt hoe de gemeente Heemstede met privacy omgaat. Achtereenvolgens komen aan de orde een nadere definiëring van het beleid, privacymanagement, beleid voor rechtmatige en zorgvuldige verwerking van persoonsgegevens, privacyrechten, informatiebeveiliging, convenanten en verwerkersovereenkomsten, bewustwording, communicatie en evaluatie.

1.1 Wat houdt het verwerken van persoonsgegevens in?

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de 'betrokkene'). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is.

Er is al snel sprake van verwerken van persoonsgegevens. Onder andere verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, combineren, afschermen, wissen of vernietigen van gegevens valt allemaal onder het verwerken van persoonsgegevens.

1.2 Wie verwerken persoonsgegevens?

In de gehele gemeentelijke organisatie worden persoonsgegevens verwerkt. Dit varieert van het gebruik van een beperkte gegevensset door bijvoorbeeld de afdeling Uitvoering openbare ruimte tot grote gegevenssets zoals bij de afdeling Publiekszaken (basisregistratie personen (BRP)) en de Intergemeentelijke afdeling Sociale Zaken (IASZ). Deze laatste afdeling verwerkt ook veel gevoelige

gegevens zoals gegevens over de gezondheid van aanvragers van een voorziening op grond van de Wet maatschappelijke ondersteuning (Wmo).

De gegevens worden deels in eigen administratiesystemen verwerkt, maar voor een groot deel ook direct of indirect via het centrale gegevensmagazijn. In het centrale gegevensmagazijn zitten gegevens die afkomstig zijn uit de BRP.

1.3 Opstellen privacybeleid

Het bestuur en de medewerkers van de gemeente Heemstede hechten veel waarde aan het zorgvuldig, rechtmatig en veilig verwerken van persoonsgegevens. Het bestuur en het management spelen daarbij een cruciale rol bij het waarborgen van de privacy. Het college van de gemeente Heemstede heeft daarom besloten een algemeen privacybeleid te formuleren over hoe om te gaan met de verwerking van persoonsgegevens. De gemeente Heemstede geeft middels dit beleid een duidelijke richting aan privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft.

Dit beleid is van toepassing op de hele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente. Het is in lijn met het algemene beleid van de gemeente en de relevante lokale, nationale en Europese wet- en regelgeving.

In dit algemene privacybeleid staan kaders beschreven voor het verwerken van persoonsgegevens, de bescherming van deze gegevens en de omgang met deze gegevens. De kaders gelden voor de gemeente, samenwerkingsverbanden die zijn of worden aangegaan en derden die zijn of worden ingeschakeld. Dit beleid dient als kapstok waaraan voor een specifiek vakgebied een afdelingsspecifiek privacybeleid gehangen kan worden. Verder worden er naar aanleiding van dit beleid werkprocessen opgesteld, die als handvat fungeren om het beleid in de dagelijkse praktijk toe te passen.

1.4 Juridisch kader

Bij de verwerking van persoonsgegevens staat respect voor de persoonlijke levenssfeer van de betrokkene(n) voorop. De Algemene verordening gegevensbescherming (AVG) biedt hiervoor het wettelijk kader, samen met de Uitvoeringswet algemene verordening gegevensbescherming.

Als algemene regel geldt dat persoonsgegevens op behoorlijke en zorgvuldige wijze moeten worden verwerkt. De verantwoordelijke van de gegevensverwerking moet daarbij transparant zijn. De AVG bepaalt verder dat persoonsgegevens alleen voor een specifiek omschreven doel mogen worden verwerkt en niet voor andere doelen mogen worden gebruikt dan waarvoor zij verzameld zijn. Daarbij bepaalt de AVG dat deze gegevens alleen mogen worden verwerkt als dat noodzakelijk is om het specifiek beschreven doel te bereiken, en dat zo min mogelijk gegevens worden verwerkt. Dat houdt ook in dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk.

In aanvulling daarop bevat andere wetgeving meer specifieke vereisten voor gegevensverwerking. Voor het sociaal domein zijn dat de verschillende materiële wetten (zoals de Jeugdwet, Wmo en Participatiewet). Zowel in de Wmo als in de Participatiewet zijn bepalingen opgenomen over het verwerken van persoonsgegevens. Voor BIG-geregistreerden speelt de Wet geneeskundige behandelingsovereenkomst een rol, met daarin het medisch beroepsgeheim. Andere relevante wetten waarin privacybepalingen zijn opgenomen zijn onder andere:

- Wet basisregistratie personen;
- Wet politiegegevens;
- Wet justitiële en strafvorderlijke gegevens;
- Archiefwet (voor bewaartermijnen).

De bepalingen in deze specifieke (sectorale) wetgeving over de verwerking van persoonsgegevens gaan voor op de bepalingen van de AVG.

1.5 Raakvlakken en overlap met andere beleidsthema's

Het privacybeleid van de gemeente Heemstede heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Integriteitsbeleid

Privacybeleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid.

Kwaliteitsbeleid

Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratie is randvoorwaardelijk voor een klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteits- en risicomanagement

Privacybeleid gaat afbreuk- en aansprakelijkheidsrisico's tegen en voorkomt dat werkprocessen spaak lopen als de bijbehorende gegevensverwerking een schending van het recht op privacy inhoudt (onrechtmatige daad).

Informatiebeveiliging

Het beschermen van persoonsgegevens kan niet geborgd worden zonder adequate informatiebeveiliging. Het privacybeleid hangt daarom samen met het Informatiebeveiligingsbeleid.

2. Privacybeleid

2.1 Visie op gegevensbescherming

De gemeente Heemstede wil dicht bij de burger staan. Zij wil de burger begrijpen en waar mogelijk zorgen voor maatwerk. Er is sprake van wederzijds begrip en vertrouwen. Ze creëert ruimte voor initiatieven vanuit de burgers en is omgevingsbewust.

Om de burger te kunnen helpen, is het verwerken van gegevens nodig. Bij het verwerken van persoonsgegevens gaat de gemeente op een veilige manier met deze gegevens om en respecteert zij de privacy van de betrokkenen. Daarbij zorgt ze ervoor dat de burgers hun privacyrechten kunnen uitoefenen.

2.2 Doel en reikwijdte privacybeleid

Het verwerken van persoonsgegevens moet in overeenstemming met de wet en op behoorlijke wijze gebeuren. Dit privacybeleid geeft daar de richtlijnen voor. Het privacybeleid heeft betrekking op de persoonsgegevens van personen van wie de gemeente Heemstede gegevens verwerkt of laat verwerken en is van toepassing op alle taken en processen waar de gemeente verantwoordelijk voor is. Hieronder valt ook de uitwisseling van persoonsgegevens door de gemeente. Daarnaast maakt de gemeente op een aantal terreinen aparte samenwerkingsafspraken met haar partners.

Door dit privacybeleid uit te voeren:

1. beschermt het college haar inwoners tegen risico's van de informatiemaatschappij;
2. draagt het college bij aan maatschappelijk vertrouwen en draagvlak;
3. kan het college met vertrouwen verantwoording afleggen aan de raad, waar nodig de Autoriteit Persoonsgegevens of de rechter;
4. beheerst het college gemeentelijk afbreuk- en aansprakelijkheidsrisico's;
5. speelt het college adequaat in op de technologische en wettelijke ontwikkelingen.

2.3 Uitgangspunten privacy

De gemeente Heemstede houdt zich bij het verwerken van persoonsgegevens aan de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid en transparantie
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. De gemeente zorgt ervoor dat burgers inzicht kunnen hebben in de gegevens die de gemeente verwerkt.

Grondslag en doelbinding

De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt. De rechtmatige grondslagen zijn:

- verwerking op basis van toestemming;
- verwerking voor de uitvoering van een overeenkomst;
- verwerking voor het nakomen van een wettelijke verplichting;
- verwerking voor een taak met een algemeen belang of uitoefening van openbaar gezag;
- verwerking voor de behartiging van een gerechtvaardigd belang;
- verwerking voor een vitaal belang van de betrokkene.

Dataminimalisatie

De gemeente verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

Bewaartermijn

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de gemeentelijke taken goed uit te kunnen voeren of om wettelijke verplichtingen te kunnen naleven.

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 zijn verzameld. Daarbij zorgt de gemeente voor een passende beveiliging van de persoonsgegevens. Deze beveiliging is vastgelegd in het informatiebeveiligingsbeleid.

Delen met derden

In het geval van samenwerking met externe partijen waarbij sprake is van verwerking van persoonsgegevens maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente controleert deze afspraken jaarlijks.

Integrale dienstverlening

Als het in het belang van de burger is, wordt individueel bekeken of delen van de gegevens met anderen (binnen en buiten de organisatie) nodig is. Hierdoor is integraal werken mogelijk. De burger wiens gegevens het betreft, wordt van deze gegevensdeling en van de achterliggende motivatie voor de gegevensdeling op de hoogte gebracht.

Subsidiariteit

Vóór het verwerken van de gegevens bepaalt de gemeente of het doel van de verwerking niet op een andere manier bereikt kan worden dan met het verwerken van de persoonsgegevens. Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.

Proportionaliteit

De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot, en met het doel van, de verwerking.

Rechten van betrokkenen

De gemeente honoreert alle rechten van betrokkenen.

Deze aandachtspunten worden verder uitgewerkt in de volgende hoofdstukken.

3. Privacymanagement

Voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens in overeenstemming met de wet is goed privacymanagement van de gemeente noodzakelijk. Het gaat hierbij om vragen als ‘Hoe is privacy ingebed in de organisatiestructuur?’ en ‘Bij wie ligt het proceseigenaarschap en wie houdt toezicht op de naleving?’.
Waar het bij privacymanagement uiteindelijk om gaat is dat er een bedrijfsvoering ontstaat waarbij privacy op een natuurlijke manier bij de organisatie is gaan behoren (‘privacy by design). Daarbij is het uitgangspunt dat de standaard zo privacybestendig mogelijk is (‘privacy by default’).

3.1 Taken en verantwoordelijkheden

Het college van burgemeester en wethouders is eindverantwoordelijk voor de naleving van privacywetgeving met de burgemeester als portefeuillehouder. Het hoogste management en het lijnmanagement hebben de ambtelijke verantwoordelijkheid om een proactief privacybeleid te voeren op basis van afweging van belangen en risico’s bij de verwerking van persoonsgegevens, zodat dit behoorlijk, zorgvuldig en in overeenstemming met de wet plaatsvindt.
Het college legt over de privacybeleidsuitvoering verantwoording af aan de gemeenteraad. Het college zorgt ook voor een zodanige documentatie van beleid en maatregelen dat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak.
Onderstaande tabel brengt de verantwoordelijkheden in beeld aan de hand van het RASCI-model:

Verantwoordelijk	**Rol**
R Responsible / feitelijk verantwoordelijk	1e lijn - Gemeentesecretaris - Domeinmanagers - Teammanagers - Operationeel leidinggevenden - Alle medewerkers (incl. inhuur en externen)
A Accountable / eindverantwoordelijk	1e lijn - College van burgemeester en wethouders
S Supporting / ondersteunend	2e lijn - Privacybeheerder - Juristen
C Consulted / controlerend	3e lijn - FG - CISO - Controller - Accountant
I Informed / geïnformeerd	Belanghebbenden - Inwoners - Medewerkers - Gemeenteraad - Autoriteit Persoonsgegevens

3.2 Proceseigenaarschap

De teammanager is er verantwoordelijk voor dat de gemeentelijke taakuitoefening binnen de grenzen van dit privacybeleid plaatsvindt en rapporteert hierover aan het hoogste management, dat op zijn beurt rapporteert aan het college. Het college legt verantwoording af aan de gemeenteraad.
De teammanager is proceseigenaar. Proceseigenaren voeren regie over hun proces(sen). Bij teamoverstijgende processen kan een coördinerend teammanager of een andere functionaris, bijvoorbeeld een domeinmanager, worden aangewezen.
De proceseigenaar kan verantwoordelijkheden mandateren aan medewerkers (‘subproceseigenaren’). Het college van burgemeester en wethouders is in de meeste gevallen ‘verwerkingsverantwoordelijke’ in de zin van de AVG en blijft dus eindverantwoordelijk voor de privacybestendigheid van de gemeentelijke processen.

3.3 Uitwerking van de privacy governance

In bijlage 1 is de privacy governance van de gemeente Heemstede uitgewerkt. De hiervoor genoemde verantwoordelijkheden zijn hierin geïmplementeerd. De proceseigenaar is verantwoordelijk voor het voldoen aan de vereisten vanuit de AVG en wordt daarbij ondersteund door de Privacy Beheerder en in sommige gevallen door de CISO. De Functionaris gegevensbescherming controleert of er conform de AVG wordt gewerkt.

4. Beleid voor rechtmatige en zorgvuldige verwerking van persoonsgegevens

Uit de AVG vloeit een aantal verplichtingen voort voor de gemeente als verwerkingsverantwoordelijke. Deze uitgangspunten werden in paragraaf 2.3 al kort gemeld en de voornaamste verplichtingen worden nader beschreven in dit hoofdstuk.

4.1 Register van verwerkingen

Artikel 30 van de AVG vereist dat de gemeente een register opstelt en bijhoudt van alle verwerkingsactiviteiten die onder verantwoordelijkheid van de gemeente plaatsvinden. Hierdoor hebben burgers inzicht in welke gegevens de gemeente verwerkt. De gemeente Heemstede heeft dit register opgesteld en op de website gepubliceerd en houdt dit actueel. De volgende gegevens zijn in het register van verwerkingen opgenomen:

- de naam en contactgegevens van de verwerkingsverantwoordelijke;
- de (gemeentelijke) afdeling die de gegevens verwerkt;
- de verwerkingsdoeleinden;
- de grondslag die aan de basis van de verwerking ligt, inclusief eventuele uitleg;
- de categorieën van betrokkenen;
- de categorieën van (bijzondere) persoonsgegevens;
- de categorieën van ontvangers van de persoonsgegevens aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de bewaartermijnen van de gegevens;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen;
- de herkomst van de gegevens;
- de naam en contactgegevens van de functionaris voor de gegevensbescherming.

4.2 Transparantie

De gemeente Heemstede is transparant over hoe ze persoonsgegevens verwerkt. Hierdoor weten burgers en personen die benaderd worden wie de gemeente Heemstede is, dat de gemeente Heemstede persoonsgegevens verwerkt, waarom dit gebeurt en welke maatregelen de gemeente Heemstede neemt om zorgvuldig met de gegevens om te gaan.
De belangrijkste manieren om betrokkenen te informeren over de verwerking van persoonsgeggevens zijn:

- het geven van algemene informatie bij inschrijven en op de website;
- het geven van aanvullende informatie bij het aanvragen van specifieke diensten;
- indien vereist, het geven van een cookiemelding op alle gemeentelijke websites en het hebben van een privacyverklaring, inclusief cookiebepaling;
- het bieden van laagdrempelige mogelijkheden om inzage te krijgen in de verwerking van persoonsgegevens. Zie hiervoor ook hoofdstuk 5.

Betrokkenen worden in ieder geval geïnformeerd over:

- de identiteit en contactgegevens van de verantwoordelijke en van de functionaris voor gegevensbescherming;
- de doeleinden en rechtsgrond(en) van de gegevensverwerking;
- indien van toepassing: de ontvangers;
- indien van toepassing: nadere informatie met betrekking tot eventuele doorgifte van persoonsgegevens naar een derde land of internationale organisatie;
- de bewaartermijnen;
- de rechten van betrokkenen.

Als de gegevens niet van de betrokkene zelf zijn verkregen, wordt ook informatie gegeven over de categorieën van persoonsgegevens die worden verwerkt.

De betrokkene wordt geïnformeerd voordat deze zijn gegevens verstrekt. Als de gegevens niet van de betrokkene zelf zijn verkregen, dan wordt de betrokkene hierover geïnformeerd op het moment dat de gemeente Heemstede deze gegevens vastlegt.

4.3 Doelbinding

Met doelbinding wordt bedoeld dat gegevens alleen worden verwerkt voor het doel waarvoor ze zijn verzameld. En als gegevens toch voor andere doelen worden gebruikt, wordt beoordeeld of dit nieuwe doel niet te ver afstaat van het oorspronkelijke doel van verzamelen van de gegevens.

De gemeente Heemstede verwerkt alleen gegevens voor de doelen waarvoor ze van de burgers verkregen zijn. In paragraaf *4.2 Transparantie* is aangegeven hoe en wanneer personen op de hoogte worden gesteld van de verwerking van persoonsgegevens. De organisatie zorgt ervoor dat de persoonsgegevens alleen voor deze doelen worden verwerkt. Wanneer de wens ontstaat om persoonsgegevens voor andere doelen te verwerken, wordt daar waar nodig een ‘Data Protection impact analysis’ (DPIA) uitgevoerd om de vraag te beantwoorden of de verwerking ‘niet onverenigbaar’ is met het oorspronkelijke doel.

4.4 Rechtmatige grondslag

De gemeente Heemstede mag alleen persoonsgegevens verwerken wanneer hier een grondslag voor bestaat. De gemeente Heemstede verwerkt gegevens van haar burgers, medewerkers, (keten)partners en bezoekers van haar websites veelal op basis van wettelijke taken, in het kader van de vervulling van taken van algemeen belang en in het kader van de uitoefening van openbaar gezag. In sommige gevallen verwerkt zij gegevens ter uitvoering van een overeenkomst of op basis van toestemming.
Zodra een persoon is ingeschreven in de gemeente worden de gegevens verwerkt conform de wettelijke bepalingen vanuit de Basisregistratie personen (BRP). Ook voor andere publiekrechtelijke taken is de gemeente verplicht de gegevens uit de BRP te gebruiken. Ten aanzien van de onlineactiviteiten verwerkt de gemeente Heemstede persoonsgegevens ter uitvoering van wettelijke

verplichtingen (informatievoorziening aan het publiek), of op basis van een gerechtvaardigd belang. In sommige gevallen gebeurt dit op basis van toestemming (bijvoorbeeld voor het plaatsen van toestemmingsplichtige cookies).
De gemeente Heemstede verwerkt vanuit haar wettelijke taken ook bijzondere persoonsgegevens, zoals gegevens over de gezondheid voor de aanvraag van een hulpmiddel in het kader van de Wmo. Dit is opgenomen in het register van verwerkingsactiviteiten. De gemeente is ook wettelijk verplicht om het Burgerservicenummer (BSN) te verwerken, onder meer uit hoofde van de Wet algemene bepalingen burgerservicenummer (Wabb) en de Wet basisregistratie personen (Wet BRP). Dit is in overeenstemming met het bepaalde in artikel 87 AVG en artikel 46 van de Uitvoeringswet AVG. Verwerking van het BSN moet altijd proportioneel zijn.

4.5 Privacy by design

De gemeente Heemstede zorgt er vóór de start van een gegevensverwerking voor dat zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens afgedwongen wordt. Dit is ‘privacy by design’. Hierbij wordt onder andere gekeken of de gegevens nodig zijn voor het te behalen doel en naar de benodigde beveiliging van de persoonsgegevens. Een onderdeel van privacy by design is ‘privacy by default’: hiermee wordt ervoor gezorgd dat de standaard instellingen zo privacyvriendelijk mogelijk zijn.

4.6 De hoeveelheid te verwerken gegevens

De gemeente Heemstede streeft naar minimale gegevensverwerking. Ook dit is een onderdeel van privacy by design en houdt in dat alleen die gegevens verwerkt worden die noodzakelijk zijn voor het doel waarvoor ze verzameld zijn. Voordat begonnen wordt met de verzameling van de gegevens wordt beoordeeld of het doel van de verwerking niet op een andere manier bereikt kan worden dan met het verwerken van persoonsgegevens (subsidiariteit). Ook wordt beoordeeld of de inbreuk op de privacy van de burgers/cliënten wel in verhouding staat tot het doel van de verwerking (proportionaliteit).
Als burgers zelf meer gegevens aanbieden dan nodig is voor het doel, dan worden de overbodige gegevens vernietigd.

4.7 Kwaliteit van gegevens

De gemeente Heemstede treft maatregelen om de kwaliteit van gegevens te borgen. Onder kwaliteit wordt verstaan dat de gegevens juist, nauwkeurig en actueel zijn. Voordat gegevens worden verwerkt vinden (geautomatiseerde) controles plaats om te voorkomen dat personen niet goed benaderd worden (denk aan het versturen van brieven naar een oud adres, het versturen van brieven met een verkeerde tenaamstelling of het versturen van een brief naar een overledene).
In ieder geval zijn de volgende maatregelen getroffen:

- Bij de invoer van gegevens vindt een kwaliteitscontrole plaats door het verifiëren van gegevens.
- ICT-systemen valideren gegevens door middel van invoercontroles en validaties.

- ICT-systemen zijn daar waar persoonsgegevens worden gebruikt veelal direct of indirect gekoppeld aan de BRP, zodat altijd wordt beschikt over actuele gegevens. Als deze koppeling niet mogelijk is, worden de gegevens in de BRP geverifieerd, voordat zij worden gebruikt.
- Betrokkenen hebben de mogelijkheid gegevens in te zien en te laten corrigeren indien nodig.

4.8 Bewaartermijn

Als de gemeente Heemstede de gegevens niet meer nodig heeft, dan vernietigt zij de gegevens, tenzij er een wettelijke verplichting is om de gegevens langer te bewaren. Soms worden bewaartermijnen genoemd in specifieke wetten waarvoor de gegevensverwerking nodig is; in andere gevallen bepaalt de Archiefwet de bewaartermijnen. De gemeente Heemstede vernietigt in die gevallen –indien technisch mogelijk- de gegevens zodra de wettelijke bewaartermijn en/of de termijn uit de selectielijst van de VNG is afgelopen.

4.9 Gegevensbeschermingseffectbeoordeling

Vanuit de AVG is de gemeente verplicht om in een aantal gevallen vóór de verwerking van de gegevens een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren. Het uitvoeren van een DPIA is alleen verplicht als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de gemeente Heemstede gegevens verwerkt. Bij de beoordeling hiervan maakt de gemeente Heemstede gebruik van de beoordelingscriteria die hiervoor zijn opgesteld door de Europese Privacytoezichthouders.
Naast het uitvoeren van een DPIA voor de aanvang van een gegevensverwerking voert de gemeente Heemstede elke drie jaar een beknopte DPIA uit op de bestaande gegevensverwerkingen. Hierin wordt gecontroleerd of nog steeds aan alle voorwaarden wordt voldaan of dat er extra beveiligingsmaatregelen genomen moeten worden (als de gegevensverwerking grotere privacyrisico's heeft, wordt de beknopte DPIA uitgebreid). Indien nodig wordt er in dergelijke gevallen een volledige DPIA uitgevoerd. Daarnaast wordt een DPIA over bestaande gegevensverwerkingen uitgevoerd als bijvoorbeeld de gegevens voor een ander doel gebruikt gaan worden of als men nieuwe technologie gaat gebruiken.

4.10 Samenwerkingsverbanden

De gemeente Heemstede werkt samen in regionaal verband. Zo kent de gemeente Heemstede onder andere samenwerkingen op het gebied van zorg en van veiligheid, zoals het Veiligheidshuis. De gemeente Heemstede zorgt ervoor dat zij afdoende afspraken maakt met deze samenwerkingspartners om de privacy te waarborgen. Vóór de deelname in een samenwerkingsverband voert de gemeente Heemstede een DPIA uit om de risico's van deelname aan het samenwerkingsverband te analyseren en hierop maatregelen te nemen.

5. Privacyrechten

De AVG bepaalt niet alleen de plichten van degenen die persoonsgegevens verwerken, maar ook de rechten van personen van wie de gegevens worden verwerkt.

5.1 Recht op inzage en correctie van persoonsgegevens

Iedere betrokkene kan de gemeente met redelijke tussenpozen vragen welke persoonsgegevens van hem/haar worden verwerkt. Als de gegevens niet juist of onvolledig zijn, kan de betrokkene de gemeente verzoeken zijn of haar gegevens te verbeteren, te verwijderen of aan te vullen. Dit verzoek kan mondeling en schriftelijk worden ingediend. De gemeente voldoet binnen één maand na ontvangst aan het inzageverzoek. Als het inzageverzoek erg complex is of als er tegelijkertijd veel verzoeken binnenkomen, wordt deze termijn –indien nodig- met twee maanden verlengd.

Als er persoonsgegevens worden verwerkt, dan worden de volgende gegevens vermeld:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens;
- de (categorieën van) ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- indien mogelijk: de periode gedurende welke de persoonsgegevens naar verwachting zullen zijn opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- dat de betrokkene recht heeft de verwerkingsverantwoordelijke te verzoeken de persoonsgegevens te verbeteren of te wissen of de verwerking van hem betreffende persoonsgegevens te beperken en het recht tegen die verwerking bezwaar te maken;
- dat de betrokkene recht heeft een klacht in te dienen bij een toezichthoudende autoriteit;
- als de persoonsgegevens niet bij de betrokkene zelf worden verzameld, alle beschikbare informatie over de bron van die gegevens.

Bij de verstrekking van gegevens houdt het recht van privacy op waar dat van een ander begint. In sommige gevallen is het recht van inzage beperkt door rechten van anderen. Denk hierbij bijvoorbeeld aan een inzageverzoek dat tot onevenredige administratieve lasten leidt voor de verwerkingsverantwoordelijke. Of aan gegevens waarin ook gegevens van andere personen zijn opgenomen. In dat geval worden de gegevens van de andere personen geanonimiseerd.

Bij een verzoek tot correctie deelt de gemeente binnen vier weken na ontvangst van het verzoek aan de betrokkene mee of zijn/haar verzoek gegrond is. De gemeente verbetert de gegevens als deze onjuist, niet volledig of niet ter zake dienend waren. Bovendien worden derden aan wie de persoonsgegevens voor de correctie zijn verstrekt van deze correctie op de hoogte gebracht. De verzoeker mag opgave verzoeken van degene(n) aan wie de gemeente deze mededeling heeft gedaan.

5.2 Recht van bezwaar en op het indienen van een klacht

Iedere betrokkene heeft het recht om bezwaar te maken tegen de verwerking van gegevens. Dit kan als de verwerking gebeurt op grond van een taak van algemeen belang of een gerechtvaardigd belang.
Als een betrokkene bezwaar maakt tegen het verwerken van de gegevens en het betreft een van de genoemde belangen, dan stopt de gemeente met het verwerken van deze gegevens. Als de gemeente dwingende gerechtvaardigde redenen voor de verwerking heeft die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of als er sprake is van een rechtsvordering, dan stopt de gemeente de verwerking niet. Zo lang niet duidelijk is of de gronden van de gemeente zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene wordt de verwerking beperkt.
De gemeente informeert de betrokkene over het recht op bezwaar. Dit gebeurt uiterlijk op het moment van het eerste contact met de betrokkene. Deze informatie wordt duidelijk en gescheiden van andere informatie aangeboden.

Als iemand een klacht heeft over de verwerking omdat hij vindt dat de gemeente Heemstede niet zorgvuldig omgaat met zijn gegevens, dan kan hij een klacht indienen bij het college van burgemeester en wethouders. Deze klacht wordt serieus behandeld. Als de klacht terecht is, dan wordt de manier van omgaan met de persoonsgegevens aangepast en de betrokkene hierover geïnformeerd.

5.3 Recht op beperking van de verwerking

De betrokkene heeft in de volgende gevallen recht op beperking van de verwerking van de gegevens:

- *De gegevens zijn mogelijk onjuist*: als iemand aangeeft dat de gegevens mogelijk niet juist zijn, dan gebruikt de gemeente deze gegevens niet zolang niet gecontroleerd is of de gegevens kloppen.
- *De verwerking is onrechtmatig*: als de gemeente bepaalde gegevens niet mag verwerken, maar de betrokkene wil niet dat de gegevens worden gewist, dan bewaart de gemeente deze gegevens wel maar gebruikt ze niet.
- *De gegevens zijn niet meer nodig*: als de gemeente de gegevens niet meer nodig heeft voor het doel waarvoor ze zijn verzameld, maar de betrokkene heeft de gegevens wel nog nodig voor een rechtsvordering, dan bewaart de gemeente deze gegevens wel maar gebruikt ze niet.
- *Betrokkene maakt bezwaar*: als de betrokkene bezwaar heeft gemaakt tegen de verwerking, dan stopt de gemeente met het verwerken van deze gegevens, tenzij de gemeente gerechtvaardigde gronden voor de verwerking heeft die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene. Zolang niet duidelijk is of de gronden van de gemeente zwaarder wegen, verwerkt de gemeente deze gegevens niet.

Als de gemeente de gegevens ook aan andere partijen heeft verstrekt, dan laat de gemeente weten dat ze het gebruik van de gegevens beperkt heeft en verzoekt deze organisatie de verwerking van de

gegevens ook te beperken. Als de betrokkene hierom vraagt, geeft de gemeente aan welke organisaties hierover zijn geïnformeerd.

5.4 Recht op vergetelheid

In de volgende gevallen wist de gemeente de gegevens als de betrokkene erom vraagt en er geen sprake is van een uitzondering (zie onder):

- de gemeente heeft de gegevens niet meer nodig;
- de betrokkene heeft de eerder gegeven toestemming voor de verwerking van de gegevens ingetrokken (en dit is de enige grondslag voor de verwerking van de gegevens);
- de betrokkene heeft bezwaar gemaakt tegen de verwerking van de gegevens en dit bezwaar is ingewilligd;
- de gegevens worden onrechtmatig verwerkt;
- de wettelijke bewaartermijn van de gegevens is verlopen.

Uitzonderingen

In de volgende gevallen wist de gemeente de gegevens niet:

- de gemeente verwerkt de gegevens omdat de verwerking wettelijk verplicht is;
- de gemeente verwerkt de gegevens op grond van haar openbaar gezag of (wettelijk vastgelegde) taak van algemeen belang;
- de gemeente verwerkt de gegevens voor een taak van algemeen belang op het gebied van volksgezondheid;
- de gemeente moet de gegevens in het algemeen belang archiveren;
- de gegevens zijn noodzakelijk voor een rechtsvordering;
- de verwerking van de gegevens is noodzakelijk om het recht op vrijheid van meningsuiting en informatie uit te oefenen.

5.5 Recht op dataportabiliteit

In het voorkomende geval dat de gemeente persoonsgegevens verwerkt op grond van toestemming van de betrokkene of voor de uitvoering van een overeenkomst en de betrokkene wil de gegevens overdragen aan een andere organisatie, dan verstrekt de gemeente de gegevens aan de betrokkene. Het gaat hierbij alleen om digitale gegevens.

5.6 Algemene uitzonderingen privacyrechten

De gemeente geeft geen gehoor aan verzoeken van de betrokkene als dat noodzakelijk is voor het waarborgen van:

1. de nationale veiligheid;
2. de landsverdediging;
3. de openbare veiligheid;

4. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Hieronder valt ook de bescherming tegen en de voorkoming van gevaren van de openbare veiligheid;
5. andere belangrijke doelen van algemeen belang van Nederland of van de Europese Unie, vooral als het gaat om belangrijke economische of financiële belangen;
6. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
7. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor beroepen met een beroepscode;
8. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag in de in punten 1 tot en met 5 en punt 7 genoemde gevallen;
9. de bescherming van de betrokkene of van rechten en vrijheden van anderen;
10. de inning van civielrechtelijke vorderingen.

Voorwaarde hiervoor is wel dat het niet gehoor geven aan het verzoek geen effect heeft op de wezenlijke inhoud van de grondrechten en fundamentele vrijheden van de betrokkene.

6. Informatiebeveiliging

Om zorgvuldig met persoonsgegevens om te kunnen gaan moeten passende beschermende maatregelen worden getroffen. Deze maatregelen moeten de geheimhouding en beveiliging van de gegevens borgen. De maatregelen gelden voor allen die onder verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Heemstede werken: interne medewerkers, verwerkers en subverwerkers. De maatregelen gelden ook voor diensten en goederen die onderdeel zijn van de beveiliging, zoals de beveiliging van het pand, de schoonmaak of de leveranciers van de hardware.
Uit hoofde van de meldplicht datalekken (artikel 33 AVG) meldt het college van burgemeester en wethouders van de gemeente Heemstede een beveiligingsincident bij de Autoriteit Persoonsgegevens, tenzij het niet aannemelijk is dat de inbreuk op de beveiliging een privacyrisico inhoudt. De procedure rond de meldplicht van datalekken is uitgewerkt in een handleiding voor de medewerkers van de gemeente Heemstede. In dit hoofdstuk wordt verder ingegaan op de onderwerpen:

- geheimhouding;
- informatiebeveiliging.

6.1 Geheimhouding

Alle personen die onder het gezag van het college van burgemeester en wethouders werken zijn geheimhouding verplicht. Dit zijn niet alleen medewerkers van de interne organisatie, maar ook verwerkers en inhuurkrachten.
Elke werknemer in vaste dienst legt een eed of belofte af bij indiensttreding als onderdeel van de arbeidsovereenkomst. Daarnaast wordt een geheimhoudingsverklaring getekend. Inhuurkrachten tekenen in ieder geval een geheimhoudingsverklaring. Afhankelijk van de duur en de aard van de inhuur wordt ook de eed/belofte afgelegd.
Daarnaast worden de medewerkers in een apart document gewezen op de geheimhoudingsplicht en op het belang van een zorgvuldige omgang met de gegevens. Voor een aantal aparte functies worden medewerkers specifiek op hun geheimhoudingsplicht gewezen, zoals bij het gebruik van Suwinet en van de Basisregistratie personen.

Verwerkers en externen worden door middel van verwerkersovereenkomsten en contracten verplicht tot geheimhouding. Dit is opgenomen in de model verwerkersovereenkomst. In alle contracten met leveranciers, verwerkers en overige externen die toegang krijgen tot het pand of tot de systemen is een bepaling over de geheimhouding opgenomen.

6.2 Informatiebeveiliging

Voor de informatiebeveiliging geldt de norm van de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG). Per 1 januari 2020 wordt deze norm vervangen door de Baseline Informatiebeveiliging Overheid (BIO), waarbij 2019 als overgangsjaar geldt.

Voor de informatiebeveiliging is een strategisch en tactisch informatiebeveiligingsbeleid opgesteld, dat iedere vier jaar herzien en opnieuw vastgesteld wordt.

7. Convenanten en verwerkersovereenkomsten

Voor het realiseren van bepaalde (beleids)doelstellingen kan de gemeente Heemstede samenwerken met externe partijen. Met deze partijen wordt een convenant afgesloten. Ook kan de gemeente Heemstede verwerkers inschakelen om bepaalde gemeentelijke taken uit te voeren. Hiervoor sluit de gemeente een verwerkersovereenkomst af.

7.1 Convenanten

De gemeente kan met externe partijen samenwerken om beleidsdoelen te realiseren. Dit gebeurt bijvoorbeeld op het gebied van veiligheid. Voor deze samenwerking worden afspraken opgesteld over onder andere de verdeling van de taken, de verantwoordelijkheden en de werkwijze. Als het voor het bereiken van de beleidsdoeleinden nodig is om persoonsgegevens te verwerken, dan worden hierover uitdrukkelijk afspraken opgenomen in het convenant. Het gaat hier in ieder geval om afspraken over:

- wie de verantwoordelijke is;
- het onderwerp, de aard, het doel en de duur van de uit te voeren verwerking van persoonsgegevens, met een nadere beschrijving van de soorten persoonsgegevens en de categorieën van betrokkenen;
- de manier van verwerken van de persoonsgegevens;
- wie verantwoordelijk is voor het beheer van de gegevens;
- technische en organisatorische beveiligingsmaatregelen;
- geheimhouding en vertrouwelijkheid;
- bij wie de betrokkene moet zijn om zijn privacyrechten te kunnen uitoefenen;
- wie verantwoordelijk is voor het voldoen aan andere verplichtingen, zoals het melden van datalekken, het uitvoeren van DPIA's en bij voorafgaande raadpleging;
- het teruggeven of vernietigen van de gegevens na beëindiging van het convenant;
- wie verantwoordelijk is voor de uitvoering van audits en controle van de gegevens;
- doorgifte van de gegevens naar het buitenland.

Jaarlijks wordt gecontroleerd of de convenanten nog actueel zijn en waar nodig aangepast.

7.2 Verwerkersovereenkomsten

Verwerkers verwerken persoonsgegevens in opdracht van de gemeente Heemstede. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd. Met alle verwerkers wordt een verwerkersovereenkomst gesloten.

In de verwerkersovereenkomst maakt de gemeente Heemstede in ieder geval afspraken over:

- het onderwerp, de aard, het doel en de duur van de uit te voeren verwerking van persoonsgegevens, met een nadere beschrijving van de soorten persoonsgegevens en de categorieën van betrokkenen;
- het verwerken van de persoonsgegevens door de verwerker op instructie van de verantwoordelijke;

- het door de verwerker inhuren van andere verwerkers (subverwerkers);
- technische en organisatorische beveiligingsmaatregelen;
- geheimhouding en vertrouwelijkheid;
- het assisteren van de verantwoordelijke bij het voldoen aan de plichten als betrokkenen hun privacyrechten uitoefenen;
- het assisteren van de verantwoordelijke bij het voldoen aan andere verplichtingen, zoals het melden van datalekken, het uitvoeren van DPIA's en bij voorafgaande raadpleging;
- het teruggeven of vernietigen van de gegevens na beëindiging van de overeenkomst;
- het meewerken aan audits en controles om te kunnen vaststellen of de verwerker zich houdt aan de in de verwerkersovereenkomst genoemde verplichtingen;
- doorgifte van de gegevens naar het buitenland;
- de aansprakelijkheid.

Het afsluiten van de verwerkersovereenkomst wordt -indien mogelijk- meegenomen bij het afsluiten van de hoofdovereenkomst en is daarmee een integraal onderdeel van de hoofdovereenkomst. Als de verwerkersovereenkomst later wordt gesloten, dan wordt gebruik gemaakt van de Heemsteedse modelovereenkomst. Deze wordt voorgelegd aan de verwerker; mocht deze onderdelen van de overeenkomst aangepast willen zien, dan wordt dat in goed onderling overleg bepaald, waarbij de vereisten vanuit de AVG niet uit het oog verloren worden. Vanaf 1 januari 2020 wordt de modelverwerkersovereenkomst van de Vereniging Nederlandse Gemeenten (VNG) verplicht voor de nieuw af te sluiten verwerkersovereenkomsten.

Jaarlijks wordt gecontroleerd of de bestaande verwerkersovereenkomsten nog actueel zijn en waar nodig aangepast.

8. Bewustwording, communicatie en evaluatie

Privacybeleid moet niet beperkt blijven tot het formuleren van uitgangspunten en door het college na te streven doelen. Alle medewerkers van de gemeente Heemstede dragen in de praktijk zorg voor de eerbiediging van de persoonlijke levenssfeer bij de verwerking van persoonsgegevens. Privacy is daarmee voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur en personeel moeten zich bij de uitoefening van hun werk voortdurend bewust zijn van het belang van het waarborgen van de rechten van de burgers.

Naast het inrichten van het privacybeleid en werkprocessen is het belangrijk dat personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Daarom is het belangrijk dat de professionals in het veld en binnen de gemeente zich bewust zijn van de regels en gedragsnormen rondom privacy. De gemeente Heemstede ondersteunt dit proces door het ontwikkelen van bijvoorbeeld privacyprotocollen en afwegingskaders. Richting de burger is communicatie over de privacy van belang. De burger heeft het recht te weten wat er met zijn of haar gegevens gebeurt.

Om ervoor te zorgen dat de professionals zich bewust zijn van het belang van privacy en weten hoe zij persoonsgegevens op een zorgvuldige manier moeten verwerken, wordt jaarlijks een awarenessplan opgesteld. Hierin worden verschillende aandachtspunten voor de bewustwording en -blijving van de personen die met de persoonsgegevens werken opgenomen. Omdat het veilig omgaan met persoonsgegevens een direct verband houdt met informatiebeveiliging wordt het oppakken van awareness op het gebied van privacy gecombineerd met de bewustwording op het gebied van informatiebeveiliging. Binnen het awarenessprogramma wordt aandacht besteed aan bijvoorbeeld trainingen en opschoondagen.
De gemeente Heemstede streeft een cultuur na waarin professionals elkaar in alle openheid aanspreken op het eigen gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijk randvoorwaarden voor het realiseren van een optimaal privacybeleid.

8.1 Evaluatie

Aan het einde van elk jaar wordt geëvalueerd wat de opbrengst was van het awarenessprogramma, zodat bij het opstellen van het awarenessprogramma voor het volgende jaar hiermee rekening gehouden kan worden.
Daarnaast evalueert de functionaris gegevensbescherming jaarlijks hoe de privacy was gewaarborgd in het afgelopen jaar en rapporteert hierover aan het college van burgemeester en wethouders.

Dit privacybeleid treedt in werking na vaststelling door het college van burgemeester en wethouders. Het beleid wordt iedere vier jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via de website van de gemeente. De meest actuele versie van het beleid is te vinden op <link>.

.Aldus vastgesteld door burgemeester en wethouders van de gemeente Heemstede op <datum>.

Bijlage 1: Privacy governance van de gemeente Heemstede

Op de volgende pagina's is de privacy governance van de gemeente Heemstede voor de processen op het gebied van privacy opgenomen.

1. Beheer van het register van verwerkingen

Vanuit de AVG is het verplicht een register van verwerkingen op te stellen en actueel te houden van alle gegevensverwerkingen binnen de organisatie. In het register moeten minimaal de volgende gegevens opgenomen worden: van wie gegevens worden verwerkt, welke gegevens worden verwerkt en voor welke doeleinden, hoe lang de gegevens bewaard worden, wie de gegevens ontvangen, of er gegevens naar buiten de EU worden verstrekt, hoe de gegevens worden beveiligd en de naam en contactgegevens van de verantwoordelijke en van de Functionaris gegevensbescherming.

	Eigenaar	Privacybeheerder	CISO	FG
Actieve aanlevering van nieuwe verwerkingen bij de privacybeheerder en de FG	X			
Zorgdragen voor de actualiteit van verwerkingen(register)	X			
Coördinatie van de actualisatie van het register van verwerkingen		X		
Beheer van het register van verwerkingen		X		
Toetsing op kwaliteit, actualiteit, juistheid en volledigheid van (register van) verwerkingen				X

2. Registratie, beheer en actualisatie van verwerkersovereenkomsten

Als de verantwoordelijke een andere organisatie inschakelt om persoonsgegevens voor hem te verwerken, dan moet met deze organisatie een verwerkersovereenkomst afgesloten worden. In deze overeenkomst moeten de volgende elementen opgenomen worden:
- omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking;
- het soort persoonsgegevens, de categorieën van betrokkenen en de rechten en plichten van de verantwoordelijke;
- verwerking vindt alleen plaats op basis van de schriftelijke instructies van de verantwoordelijke;
- geheimhoudingsplicht voor personen in dienst van of werkzaam voor de verwerker;
- het treffen van passende technisch en organisatorische maatregelen om de verwerking te beveiligen;
- er worden geen subverwerkers ingeschakeld zonder voorafgaande schriftelijke toestemming van de verantwoordelijke;
- de verwerker helpt de verantwoordelijke bij het voldoen van de plichten als betrokkenen hun privacyrechten uitoefenen en voor het nakomen van andere verplichtingen, zoals het melden van datalekken en het uitvoeren van een data protection impact assessment (DPIA);
- na afloop van de verwerkingsdiensten verwijdert de verwerker de gegeven of geeft deze terug (inclusief eventuele kopieën);
- de verwerker werkt mee aan audits.

De gemeenten Heemstede heeft een standaard verwerkersovereenkomst die in principe gebruikt wordt. Mocht een verwerker onoverkomelijke bezwaren hebben tegen deze overeenkomst, dan kan na een goede motivatie hiervoor en goedkeuring van de overeenkomst door de privacybeheerder eventueel gebruik gemaakt worden van de overeenkomst van de verwerker.

	Eigenaar	Privacybeheerder	CISO	FG
Afsluiten van verwerkersovereenkomsten	X			
Actualiseren en beheren van de modelverwerkersovereenkomst		X	X	
Advies aan de organisatie ten aanzien van werken met verwerkers en verwerkersovereenkomsten		X		
Coördinatie registratie verwerkers en archivering van verwerkersovereenkomsten		X		
Toezicht op registratie verwerkers en verwerkersovereenkomsten				X

3. Deelname aan overleg over privacy

Er is een regulier privacyoverleg waaraan de privacybeheerder, de CISO en de FG deelnemen. Daarnaast nemen deze personen deel aan overleggen van afdelingen, projectgroepen en werkgroepen waarin privacyvraagstukken aan de orde komen.				
	Eigenaar	**Privacybeheerder**	**CISO**	**FG**
Voorzitten privacyoverleg				X
Deelnemen aan privacyoverleg		X	X	X
Uitnodigen privacyspecialisten voor bijwonen overleggen met privacyvraagstukken	X			
Deelnemen aan project-, team- en themaoverleggen met betrekking tot privacyvraagstukken		X	X	X

4. Afhandeling veiligheidsincidenten

Een datalek is een inbreuk op de beveiliging van persoonsgegevens. Dit is heel breed. Het kan bijvoorbeeld gaan over een hacker die toegang heeft gekregen tot persoonsgegevens of een brand waarmee de serverruimte wordt vernietigd, een verloren usb-stick met persoonsgegevens of zelfs het versturen van een brief naar een verkeerd adres, waarbij de bewoner de brief ook geopend heeft.

Elke medewerker binnen Heemstede moet veiligheidsincidenten melden. Het meldingsformulier staat opgenomen in Hoegle.

	Eigenaar	Privacybeheerder	CISO	FG
Inventariseren van feiten en omstandigheden en opstellen verslag van feiten en omstandigheden	X	X	X	
Uitvoeren analyse	X	X	X	
Verstrekken advies			X	X
In geval van dilemma's in analyse en / of advies afstemmen met respectievelijk de eigenaar, gemeentesecretaris en bestuurder			X	X
Opstellen en versturen rapportage veiligheidsincident		X	X	
Afstemmen incident en resultaten met secretaris		X	X	
Controle rapportage veiligheidsincident			X	X
Melden datalek bij Autoriteit persoonsgegevens				X
Melden datalek aan betrokkenen	X	X	X	X
Implementeren adviezen uit rapportages	X			
Toetsing op implementatie adviezen				X

5. Advies en voorlichting aan de organisatie

Het goed omgaan met de privacy staat of valt met het gedrag van de personen die de persoonsgegevens verwerken. Het is daarom belangrijk dat alle medewerkers, het management en het bestuur goed op de hoogte zijn van wat kan en mag; zij moeten zich bewust zijn van de risico's die het verwerken van persoonsgegevens met zich mee brengen.

	Eigenaar	Privacybeheerder	CISO	FG
Gevraagd en ongevraagd advies geven aan bestuur, management en medewerkers met betrekking tot privacyvraagstukken.		X	X	X
Voorlichting en communicatie over privacy aan de organisatie (bewustwording)		X	X	X
Continue aandacht voor privacy op de afdeling	X			

6. Uitvoering data protection impact assessment (DPIA)

De AVG verplicht de verantwoordelijke in bepaalde gevallen voor het beginnen van het verwerken van gegevens voor een bepaald doel een DPIA uit te voeren. Dit is nodig als de gegevensverwerking een hoog privacyrisico oplevert voor de mensen van wie de gegevens verwerkt worden. Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking oplevert voor betrokkenen en in de maatregelen die de verantwoordelijke moet nemen om de risico's af te dekken. Daarnaast is het soms ook nodig om een DPIA uit te voeren voor een bestaande gegevensverwerking, bijvoorbeeld als er nog nooit een onderzoek heeft plaatsgevonden of als er veranderingen zijn ten opzichte van de vorige DPIA, zoals het gebruiken van een nieuwe technologie of als de gegevens voor een ander doel gebruikt worden. Dit is ook nodig als het risico of de omgeving verandert.

	Eigenaar	Privacybeheerder	CISO	FG
Initiëren / aanvragen DPIA	X	X		
Uitvoeren DPIA	X	X		
Inhoudelijke en procedurele ondersteuning van de eigenaar bij het doorlopen van de DPIA		X	X	
Adviseren over de DPIA				X
Opstellen verslag inclusief aanbevelingen, verwerken en archiveren van de resultaten van de DPIA		X		
Uitvoeren acties / implementeren maatregelen voortkomend uit de DPIA	X			
Toetsen uitgevoerde acties / geïmplementeerde maatregelen				X
Toetsen op de procedure, de resultaten, de effectuering en de naleving van de resultaten uit de DPIA				X

7. Afhandeling verzoek rechten van betrokkenen met betrekking tot persoonsgegevens

Onder de AVG heeft de betrokkene een aantal rechten om controle te houden over hun persoonsgegevens. Het gaat hierbij om:
1. recht op inzage;
2. recht op vergetelheid;
3. recht op rectificatie en aanvulling;
4. recht op dataportabiliteit;
5. recht op beperking van verwerking;
6. recht om bezwaar te maken;
7. recht op een menselijke blik bij besluiten;
8. recht op duidelijke informatie over wat met hun persoonsgegevens gebeurt.

Het gaat hier om de rechten 1 tot en met 6.

	Eigenaar	Privacybeheerder	CISO	FG
Verantwoordelijk voor het opstellen van procedures voor afhandeling verzoeken			X	X
Ontvangen verzoek, uitzetten vraag binnen de organisatie, verzamelen informatie en terugkoppeling naar aanvrager bij afdelingsoverstijgend verzoek		X		
Verzoek uitvoeren	X			
Procedureel en inhoudelijk ondersteunen bij de procedures verzoek rechten van betrokkenen		X		
Optimalisatie van de procedure, verzorgen van communicatie en voorlichting en verkrijgen van draagkracht binnen de organisatie rond de procedures over verzoeken rechten van betrokkenen			X	X
Toezicht op doorlopen procedures verzoek rechten van betrokkenen				X

8. Ontwikkelen en beheer van procedures, formats en beleid

Om ervoor te zorgen dat de medewerkers op een uniforme en goede manier met privacy omgaan moeten procedures, formats en beleid ontwikkeld en beheerd worden.				
	Eigenaar	**Privacybeheerder**	**CISO**	**FG**
De ontwikkeling, de optimalisatie en de interne en extern communicatie rond procedures, formats en beleid met betrekking tot privacy		X	X	X
Ten uitvoer brengen van het beleid	X			
Het beheer en de archivering van procedures, formats en beleid met betrekking tot privacy		X		
Toezicht op de kwaliteit, archivering, communicatie en toepassing van de procedures, formats en beleid				X