Heemstede

GEMEENTEBLAD

Officiële uitgave van de gemeente Heemstede

Nr. 62040

12 februari

2026

Privacybeleid 2026-2029 Heemstede

Besluit B&W

1. Het privacybeleid Gemeente Heemstede, vastgesteld op 8 september 2020, voor zover zijn bevoegdheid strekt in te trekken;
2. Het Privacybeleid 2026-2029 Heemstede vast te stellen voor zover zijn bevoegdheid strekt;
3. De raad voor te stellen het privacybeleid Gemeente Heemstede, vastgesteld op 24 september 2020, voor zover zijn bevoegdheid strekt in te trekken;
4. De raad voor te stellen het Privacybeleid 2026-2029 Heemstede vast te stellen voor zover zijn bevoegdheid strekt;
5. Het voorstel en het Privacybeleid 2026-2029 Heemstede voor te leggen aan de commissie Samenleving om advies te geven aan de raad.

Besluit Burgemeester

1. Het privacybeleid Gemeente Heemstede, vastgesteld op 8 september 2020, voor zover zijn bevoegdheid strekt in te trekken;
2. Het Privacybeleid 2026-2029 Heemstede vast te stellen voor zover zijn bevoegdheid strekt.

Besluit raad

De raad van de gemeente Heemstede;

gelezen het voorstel van burgemeester en wethouders van 9 december 2025,

Besluit:

1. Het privacybeleid Gemeente Heemstede, vastgesteld op 24 september 2020, voor zover zijn bevoegdheid strekt in te trekken;
2. Het Privacybeleid 2026-2029 Heemstede vast te stellen voor zover zijn bevoegdheid strekt.

1. Inleiding

Het college van de gemeente Heemstede heeft op 10 december 2024 een strategisch informatiebeveiligings- en privacybeleid (IB&P-beleid) vastgesteld. Dit IB&P-beleid is richtinggevend en kaderstellend voor informatiebeveiliging en privacy en moet aangevuld worden met beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau. Dit document is het tactische privacybeleid, waarin achtereenvolgens aan de orde komen: een nadere definiëring van het beleid, privacymanagement, beleid voor rechtmatige en zorgvuldige verwerking van persoonsgegevens, privacyrechten, informatiebeveiliging, convenanten en verwerkersovereenkomsten, bewustwording, communicatie en evaluatie.

Dit privacybeleid geldt voor alle bestuursorganen van de gemeente. Waar de term ‘gemeente’ staat, betreft het alle bestuursorganen. Waar nodig wordt in de verschillende hoofdstukken ingegaan op specifieke punten voor een bepaald bestuursorgaan. Dit bestuursorgaan wordt dan bij naam genoemd.

1.1 Gemeentebreed en afdelingsspecifiek privacybeleid
Dit tactische privacybeleid is van toepassing op de hele organisatie en alle bestuursorganen, 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. Het beschrijft de kaders 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.

1.2 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.

In aanvulling daarop bevat andere wetgeving meer specifieke vereisten voor gegevensverwerking. Denk bijvoorbeeld aan de Jeugdwet, Wmo en Participatiewet, Wet basisregistratie personen, Wet politiegegevens, Wet justitiële en strafvorderlijke gegevens, de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Bibob) en de Archiefwet (voor bewaartermijnen). De bepalingen in deze specifieke (sectorale) wetgeving over de verwerking van persoonsgegevens gaan voor op de bepalingen van de AVG.

1.3 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 tactische privacybeleid hangt daarom samen met het tactische informatiebeveiligingsbeleid.

1.3.1 Gemeenteraad

Voor de gemeenteraad gelden ook de volgende raakvlakken:

Gedragscode Integriteit Volksvertegenwoordigers gemeente Heemstede

De gedragscode geeft richtlijnen voor het handelen van raadsleden. Deze gelden ook voor het verwerken van persoonsgegevens en het treffen van maatregelen om te voorkomen dat onbevoegden bij vertrouwelijke en geheime informatie kunnen komen.

Reglement van orde voor de vergaderingen en andere werkzaamheden van de raad van de gemeente Heemstede

Het Reglement van orde geeft aanwijzingen voor de raadsvergaderingen. Deze betreffen ook de verwerking van persoonsgegevens tijdens een raadsvergadering.

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 burgers. 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 met derden. Daarnaast maakt de gemeente op een aantal terreinen aparte samenwerkingsafspraken met haar partners.

Door dit privacybeleid uit te voeren:

1. beschermt de gemeente de burgers tegen risico's van de informatiemaatschappij;
2. draagt de gemeente bij aan maatschappelijk vertrouwen en draagvlak;
3. kunnen het college en de burgemeester met vertrouwen verantwoording afleggen aan de gemeenteraad, en de gemeente waar nodig aan de Autoriteit Persoonsgegevens of de rechter;
4. kan de gemeente op een betrouwbare manier samenwerken met partners;
5. beheerst de gemeente gemeentelijk afbreuk- en aansprakelijkheidsrisico's;
6. speelt de gemeente adequaat in op de technologische en wettelijke ontwikkelingen.

2.3 Uitgangspunten privacy
De gemeente Heemstede heeft in haar strategische IB&P-beleid de volgende uitgangspunten opgenomen:
- Persoonsgegevens worden rechtmatig en zorgvuldig verwerkt.
- De betrokkene heeft inzicht in de gegevens die de gemeente verwerkt en (rechtmatig) deelt met derden.
- Persoonsgegevens worden alleen voor specifieke, vastgestelde, uitdrukkelijk omschreven en gerechtvaardigde doelen verwerkt.
- Bij het verwerken van persoonsgegevens gaat de gemeente uit van de principes van subsidiariteit en proportionaliteit.
- De gemeente gaat uit van minimale gegevensverwerking.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk.
- Medewerkers van de gemeente hebben een geheimhoudingsplicht voor de verwerkte persoonsgegevens.
- Voor het delen van persoonsgegevens met derden worden afspraken gemaakt.
- De gemeente honoreert de privacyrechten van betrokkene.

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
In het strategische IB&P-beleid zijn vanuit de uitgangspunten op het gebied van informatiebeveiliging en privacy de verantwoordelijkheden uitgewerkt. Op basis hiervan zijn de leidinggevenden van de afdelingen proceseigenaar[1]. Proceseigenaren voeren regie over hun proces(sen). Bij teamoverstijgende processen kan een coördinerend domeinmanager of een andere functionaris worden aangewezen.
De proceseigenaar kan verantwoordelijkheden beleggen bij medewerkers.
Wet- en regelgeving legt veelal de verantwoordelijkheid voor de verwerking van persoonsgegevens bij een specifiek bestuursorgaan neer. Vaak is dat het college van burgemeester en wethouders. Het aangewezen bestuursorgaan is dan verwerkingsverantwoordelijke in de zin van de AVG en is eindverantwoordelijk voor de privacybestendigheid van de betreffende processen.

3.1.1 Gemeenteraad
Gemeenteraadsleden voeren hun werkzaamheden aan de ene kant namens de gemeenteraad uit en aan de andere kant namens de politieke partij die zij vertegenwoordigen in de gemeenteraad. Dit privacybeleid gaat alleen over hun werkzaamheden namens de gemeenteraad en daarmee de werkzaamheden waarbij de griffie is betrokken; voor de werkzaamheden namens de politieke partij is de partij verwerkingsverantwoordelijke. Dit privacybeleid geldt niet voor de werkzaamheden namens de politieke partij.

3.2 Uitwerking van de privacy governance
In bijlage 1 is voor de specifieke processen de privacy governance van de gemeente Heemstede uitgewerkt. De hiervoor genoemde verantwoordelijkheden zijn hierin geïmplementeerd.

1) Afhankelijk van de afdeling kan het bijvoorbeeld gaan over de domeinmanager, de teammanager, de teamleider en de coördinator.

4. Beleid voor rechtmatige en zorgvuldige verwerking van persoonsgegevens

Uit de AVG vloeit een aantal verplichtingen voort voor de gemeente als verwerkingsverantwoordelijke. De belangrijkste verplichtingen worden nader beschreven in dit hoofdstuk.

4.1 Register van verwerkingen

Conform artikel 30 van de AVG heeft de gemeente Heemstede een register van verwerkingen opgesteld en op de website gepubliceerd. Jaarlijks wordt dit register geactualiseerd. De volgende gegevens zijn in het register van verwerkingen opgenomen:

- 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.

Voor de verwerking van politiegegevens is er een apart register van verwerkingen opgesteld en gepubliceerd. Los van de bovengenoemde gegevens zijn hierin ook de volgende gegevens opgenomen:

- de rechtsgrondslag voor de verwerking vanuit de Wet politiegegevens;
- het antwoord op de vraag of profilering plaatsvindt;
- de persoon/instantie die de medewerkers met toegang tot de politiegegevens autoriseert.

In de privacyverklaring, waaronder dit register valt, zijn de contactgegevens van de functionaris voor gegevensbescherming opgenomen.

4.2 Transparantie

De gemeente Heemstede is transparant over hoe ze persoonsgegevens verwerkt. Hierdoor weten burgers 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 persoonsgegevens zijn:

- het geven van algemene informatie op de website;
- het geven van aanvullende informatie bij het vragen naar persoonsgegevens;
- 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:

- 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.

Heemstede

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 gemeente zorgt ervoor dat de persoonsgegevens alleen voor deze doelen worden verwerkt. Wanneer de wens ontstaat om persoonsgegevens voor andere doelen te verwerken, wordt hierover eerst advies ingewonnen bij de privacybeheerder of FG. Daar waar nodig wordt een 'Data Protection Impact Assessment' (DPIA) uitgevoerd om de vraag te beantwoorden of de verwerking 'niet onverenigbaar' is met het oorspronkelijke doel.

4.4 Rechtmatige grondslag
De gemeente Heemstede verwerkt alleen persoonsgegevens als voldaan wordt aan een van de grondslagen uit de AVG. Gegevensverwerking gebeurt 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, op basis van toestemming of voor het eigen gerechtvaardigde belang.
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 van de AVG en artikel 46 van de Uitvoeringswet AVG.

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.
Om hieraan te kunnen voldoen worden twee stappen genomen. Bij de aanbesteding van nieuwe software waarin persoonsgegevens worden verwerkt, wordt een vooronderzoek uitgevoerd. Dit vooronderzoek leidt tot het definiëren van eisen op het gebied van informatiebeveiliging en privacy waaraan de nieuwe software moet voldoen. Ook neemt de proceseigenaar voor het opstarten van een nieuwe verwerking van persoonsgegevens of een verandering van een bestaande verwerking van persoonsgegevens voor advies contact op met de privacybeheerder of de FG. Tevens wordt een pre-DPIA uitgevoerd om te kijken of de verwerking op de gewenste manier mogelijk is en of er vervolgens een Data Protection Impact Assessment (DPIA) nodig is (zie 4.9).

4.6 De hoeveelheid te verwerken gegevens
De gemeente Heemstede streeft naar minimale gegevensverwerking. Ook dit is een onderdeel van 'privacy by design'. Het 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). Hiervoor wordt gebruik gemaakt van een pre-DPIA (zie 4.9).
Als burgers zelf meer gegevens aanbieden dan nodig is voor het doel, dan worden de overbodige gegevens vernietigd. De burger wordt hiervan op de hoogte gebracht.

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 genomen:
- 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 Basisregistratie personen (BRP), zodat de gemeente altijd 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.

4.8 Bewaartermijn
Als de gemeente Heemstede de gegevens niet meer nodig heeft voor het doel waarvoor ze verzameld zijn, 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 Selectielijst 2020 behorende bij 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 2020 is afgelopen.

4.9 Gegevensbeschermingseffectbeoordeling / Data Protection Impact Assessment (DPIA)
Voordat een nieuwe gegevensverwerking wordt gestart of een bestaande verwerking wijzigt, voert de gemeente Heemstede een pre-DPIA uit. Met deze pre-DPIA wordt onderzocht of de geplande verwerking of wijziging wettelijk gezien mogelijk is en of er een DPIA uitgevoerd moet worden.
Bij de bepaling of een DPIA nodig is, maakt de gemeente Heemstede gebruik van de bepalingen in de AVG en van de beoordelingscriteria die hiervoor zijn opgesteld door de Europese privacytoezichthouders en de Autoriteit Persoonsgegevens.
Elke drie jaar wordt een DPIA opnieuw bekeken, waar nodig aangepast en beoordeeld. Ten slotte 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 Anonimiseren van persoonsgegevens
In het kader van de openbaarheid van het bestuur is de gemeente verplicht om bepaalde documenten openbaar te maken. Daarnaast kan een inwoner documenten opvragen onder de Wet open overheid (Woo) en Wet hergebruik van overheidsinformatie (Who). Bij het openbaar maken van informatie zorgt de gemeente voor het anonimiseren van de persoonsgegevens. Voor de bepaling welke informatie geanonimiseerd moet worden, wordt gebruikgemaakt van de 'Checklist anonimiseren Wep[2]'.

Naast het anonimiseren van de persoonsgegevens in het document zelf worden ook de persoonsgegevens uit de metadata verwijderd. Dit geldt voor zowel documenten die door een gemeentemedewerker zijn opgesteld als voor ingekomen documenten.

4.11 Datagedreven werken
De gemeente Heemstede beschikt over veel data. Deze kunnen worden samengevoegd en vervolgens getoond in dashboards om zo doelmatiger, efficiënter en transparanter te kunnen werken, dienstverlening te optimaliseren en te kunnen sturen op cijfers.
Voor de ontwikkeling van een specifiek dashboard stelt – afhankelijk van welke data in een dashboard getoond moeten worden - de proceseigenaar of het managementteam een doel voor het dashboard vast. Alleen die gegevens worden verwerkt die nodig zijn voor het doel van het dashboard. Na beveiligde ontvangst van de betreffende data worden deze door de data-analisten getransformeerd en waar mogelijk geanonimiseerd naar data voor het dashboard. Alleen die personen die belang hebben bij toegang tot een dashboard worden geautoriseerd.

4.12 Samenwerkingsverbanden
De gemeente Heemstede werkt samen met derden. Zo kent de gemeente Heemstede onder andere samenwerkingen op het gebied van zorg en veiligheid, zoals het Zorg- en Veiligheidshuis. De gemeente Heemstede zorgt ervoor dat zij afdoende afspraken maakt met deze samenwerkingspartners om de privacy te waarborgen (zie 7.1). 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.
Als een (deel van een) gegevensverwerking wordt uitbesteed aan een verwerker, dan wordt voor de overdracht van de gegevens een verwerkersovereenkomst afgesloten (zie 7.2).

4.13 Gemeenteraad
Voor de gemeenteraad gelden de volgende specifieke punten:

4.13.1 Ingezonden stukken
Inwoners kunnen stukken sturen aan de raad. Deze komen binnen bij de griffie. Bij de verwerking van de ingekomen stukken aan de raadsleden worden de regels uit dit beleid gehanteerd.

2) Wep = Wet elektronische publicaties.

4.13.2 Opname van raadsvergaderingen
Raadsvergaderingen zijn openbaar. In het kader van de transparantie worden de raadsvergaderingen opgenomen. Dit wordt bij de ingang van de raadszaal bekend gemaakt. Insprekers worden ervan op de hoogte gebracht, dat hun inspraak wordt opgenomen. Conform de Selectielijst 2020, die hoort bij de Archiefwet, worden deze beelden met de verslaglegging permanent bewaard.

4.14 Burgemeester en politiegegevens
De burgemeester kan in zijn verantwoordelijkheid voor de openbare orde van de politie persoonsgegevens krijgen. Op het moment dat de burgemeester deze gegevens ontvangt, vallen ze niet meer onder de Wet politiegegevens, maar onder de AVG. De burgemeester verwerkt deze gegevens met alle waarborgen vanuit de AVG en conform dit privacybeleid.

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 mag 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 wordt bij voorkeur schriftelijk 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 - gemotiveerd met maximaal twee maanden verlengd. Hiervan wordt de betrokkene op de hoogte gebracht.

Als er persoonsgegevens worden verwerkt, dan worden bij de reactie op het verzoek de volgende gegevens vermeld:
- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens die worden verwerkt;
- de (categorieën van) ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- indien mogelijk: de vermoedelijke bewaartermijn van de persoonsgegevens 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 documenten 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 terecht is en de gegevens verbeterd worden. 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 alleen als de verwerking gebeurt op grond van een taak van algemeen belang of een gerechtvaardigd belang van de betrokkene.
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 van bezwaar. Dit gebeurt uiterlijk op het moment van het eerste contact met de betrokkene.

Als iemand een klacht heeft over de verwerking omdat hij vindt dat de gemeente Heemstede niet zorgvuldig omgaat met zijn gegevens, dan kan hij deze 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 nog wel 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 andere partijen de verwerking van de gegevens ook te beperken. Als de betrokkene hierom vraagt, geeft de gemeente aan welke andere partijen hierover zijn geïnformeerd.

5.4 Recht op vergetelheid
In de volgende gevallen wist de gemeente de gegevens als de betrokkene erom vraagt en 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 de verwerking van de gegevens is hierdoor gestaakt;
- de gegevens worden onrechtmatig verwerkt;
- de wettelijke bewaartermijn van de gegevens is verlopen.

<u>Uitzonderingen</u>
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 partij, 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 voor 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. Beveiliging van de gegevens

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, de burgemeester en de gemeenteraad 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 gebouw, de schoonmaak of de leveranciers van de hardware.
In het strategisch IB&P-beleid zijn de tien bestuurlijke principes voor informatiebeveiliging opgenomen. Deze principes helpen mede de persoonsgegevens te beschermen.
Als sprake is van een datalek, dan meldt de gemeente Heemstede dit bij de Autoriteit Persoonsgegevens, tenzij het niet aannemelijk is dat het datalek 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;
- vooronderzoeken;
- 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 (sub)verwerkers en inhuurkrachten.
Elke werknemer in vaste dienst legt een eed of belofte af bij indiensttreding als onderdeel van de arbeidsovereenkomst. Daarnaast wordt bij de ondertekening van de arbeidsovereenkomst een geheimhoudingsverklaring getekend. Inhuurkrachten tekenen in ieder geval bij de ondertekening van de inhuurovereenkomst een geheimhoudingsverklaring. Afhankelijk van de duur en de aard van de inhuur wordt ook de eed of belofte afgelegd.
Daarnaast worden de medewerkers op het intranet op de geheimhoudingsplicht en op het belang van een zorgvuldige omgang met de gegevens gewezen. 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 Vooronderzoeken

Bij de aanschaf van nieuwe software wordt een vooronderzoek uitgevoerd. Door het invullen van het vooronderzoek worden de eisen duidelijk waaraan de software op het gebied van informatiebeveiliging en privacy moet voldoen. Deze eisen worden meegenomen bij de aanbesteding van de software.

6.3 Informatiebeveiliging

Voor de informatiebeveiliging geldt met ingang van 2026 de Cyberbeveiligingswet en de norm van de Baseline Informatiebeveiliging Overheid (BIO2).
Naast het strategisch IB&P-beleid wordt er op het gebied van informatiebeveiliging ook 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 beleidsdoelstellingen te realiseren. Dit gebeurt bijvoorbeeld op het gebied van veiligheid. Voor deze samenwerking worden afspraken opgesteld over onder andere de verdeling van taken, verantwoordelijkheden en werkwijze. Als het voor het bereiken van de beleidsdoelstellingen 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 verwerkingsverantwoordelijke 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 worden deze 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 verwerkingsverantwoordelijke;
- het door de verwerker inhuren van andere verwerkers (subverwerkers);
- technische en organisatorische beveiligingsmaatregelen;
- geheimhouding en vertrouwelijkheid;
- het assisteren van de verwerkingsverantwoordelijke bij het voldoen aan de plichten als betrokkenen hun privacyrechten uitoefenen;
- het assisteren van de verwerkingsverantwoordelijke 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.

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

8. Bewustwording, communicatie en evaluatie

Bestuur en medewerkers 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 daarom belangrijk dat personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. 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 'Bewustwordingsplan informatiebeveiliging en privacy' opgesteld. Hierin worden verschillende bewustwordingsactiviteiten geagendeerd. Omdat het veilig omgaan met persoonsgegevens een direct verband houdt met informatiebeveiliging betreft de bewustwording zowel privacy als informatiebeveiliging.
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 belangrijke randvoorwaarden voor het realiseren van een optimaal privacybeleid.

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. Zie hiervoor 4.2 Transparantie.

8.1 Evaluatie

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

Dit privacybeleid treedt voor elk bestuursorgaan in werking na vaststelling door het betreffende bestuursorgaan. Het beleid wordt iedere vier jaar geëvalueerd en indien nodig herzien. Aanpassingen van dit beleid worden aangekondigd via de website van de gemeente.

Vastgesteld bij besluit van de burgemeester van 9 december 2025

Vastgesteld bij besluit van het college van 9 december 2025

Vastgesteld bij besluit van de raad van 5 februari 2026

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.

	Proceseigenaar	**Privacybeheerder**	**ISO**	**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 gemeente 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.

	Proceseigenaar	**Privacybeheerder**	**ISO**	**CISO**	**FG**

Afsluiten van verwerkersovereenkomsten	X				
Actualiseren en beheren van de modelverwerkersovereenkomst		X	X	X	
Advies aan de organisatie ten aanzien van werken met verwerkers en verwerkersovereenkomsten		X	X	X	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.				
	Proceseigenaar	**Privacybeheerder**	**ISO**	**CISO**	**FG**
Voorzitten privacyoverleg					X
Deelnemen aan privacyoverleg		X	X	X	X
Uitnodigen privacyspecialisten voor bijwonen overleggen met privacyvraagstukken	X				
Deelnemen aan project-, team- en themaoverleggen met betrekking tot privacyvraagstukken		X	X	X	X

4. Afhandeling datalekken

	Een beveiligingsincident kan een datalek zijn. Als een beveiligingsincident ook een datalek betreft, worden het beveiligingsincident en het datalek naast elkaar afgehandeld. Hier wordt ingegaan op de afhandeling van datalekken. 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 datalekken melden. Het meldingsformulier staat opgenomen op Intranet.				
	Proceseigenaar	**Privacybeheerder**	**ISO**	**CISO**	**FG**
Inventariseren van feiten en omstandigheden en opstellen verslag van feiten en omstandigheden	X	X	X	X	
Uitvoeren analyse	X	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 datalek		X	X	X	

Afstemmen datalek en resultaten analyse met secretaris		X	X	X	
Controle rapportage datalek				X	X
Melden datalek bij Autoriteit persoonsgegevens		X		X	X
Melden datalek aan betrokkenen	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.

	Proceseigenaar	Privacybeheerder	ISO	CISO	FG
Gevraagd en ongevraagd advies geven aan bestuur, management en medewerkers met betrekking tot privacyvraagstukken.		X	X	X	X
Voorlichting en communicatie over privacy aan de organisatie (bewustwording), inclusief het opstellen van een bewustwordingsplan.		X	X	X	X
Continue aandacht voor privacy op de afdeling	X				

6. Uitvoering risicoanalyse en 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. De basis voor de risicoanalyse is een vastgesteld risicokader. Ook moet er sprake zijn van een risicomanagementbeleid, waarin ook de 'Risk Appetite' is opgenomen: welke risicoscore is de organisatie bereid om te accepteren bij het nastreven van haar doelstellingen.

	MT	Proceseigenaar	Privacybeheerder	ISO	CISO	FG
Opstellen risicokader en -beleid	X					
Jaarlijkse controle op naleving risicokader en -beleid					X	X
Rapporteren uitkomst jaarlijkse controle aan MT en opnemen resultaten in Information Security Management System (ISMS)					X	

Initiëren / aanvragen DPIA		X				
Uitvoeren DPIA, inclusief uitvoeren risicoanalyse		X	X	X		
Inhoudelijke en procedurele ondersteuning van de eigenaar bij het doorlopen van de DPIA			X	X	X	
Adviseren over de DPIA					X	X
Opstellen verslag inclusief aanbevelingen, verwerken en archiveren van de resultaten van de DPIA			X	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.

	Proceseigenaar	**Privacybeheerder**	**ISO**	**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, inclusief het eventueel anonimiseren van de documenten	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.

	Proceseigenaar	Privacybeheerder	ISO	CISO	FG
De ontwikkeling, de optimalisatie en de interne en externe communicatie rond gemeentebrede procedures, formats en beleid met betrekking tot privacy		X	X	X	X
Vertalen van het gemeentebrede beleid en procedures naar de afdelingsspecifieke situatie (zoals het schrijven van het afdelingsspecifieke privacybeleid en opstellen van afdelingsspecifieke privacyprocedures).	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