Gemeente Helmond

GEMEENTEBLAD

Officiële uitgave van de gemeente Helmond

Nr. 193754

23 april

2026

Privacy beleid Gemeente Helmond 2026 – 2029

Het college van burgemeester en wethouders van de gemeente Helmond
De burgemeester van de gemeente Helmond

Gelet op de Algemene verordening gegevensbescherming en de Wet politiegegevens.

BESLUITEN

vast te stellen:

Het Privacy beleid Gemeente Helmond 2026-2029

1. Inleiding

De gemeente werkt met gegevens van inwoners, ondernemers, medewerkers, bezoekers en (keten)partners. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Helmond is zich hiervan bewust en met dit privacybeleid legt zij uit wat ze doet met deze gegevens.

2. Context

De gemeente Helmond wil met haar beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG) en de Wet Politiegegevens (hierna te noemen Wpg). Het document maakt onderdeel uit van een pakket aan maatregelen en documenten waarmee de gemeente voldoet aan haar verantwoordingsplicht.

De visie, missie en ambities van de gemeente Helmond op het gebied van de AVG en de Wpg heeft de gemeente Helmond vastgelegd in haar Strategische informatiebeveiligings- en privacybeleid 2025-2028. Dit strategische beleid is richtinggevend en bevat de kapstok voor dit aanvullende privacybeleid. Het privacybeleid wordt, daar waar relevant, aangevuld met onderwerp- of domeinspecifieke beleidsdocumenten op tactisch niveau en werkinstructies op operationeel niveau.

Daarnaast heeft de gemeente Helmond:
- In werkprocessen, procedures en instructies beschreven hoe er in de praktijk wordt gewerkt. Bijvoorbeeld over hoe inwoners en medewerkers hun rechten kunnen uitoefenen;
- Twee registers van verwerkingen waarin onder andere duidelijk wordt beschreven wat de grondslag van de verwerkingen is, het doel, welke gegevens worden verwerkt en welke partijen hierbij zijn betrokken;
- Een privacyverklaring gepubliceerd.

3. Geldigheidsduur

Dit privacybeleid is op 31 maart 2026 door het college van B&W en door de burgemeester. Het beleid geldt voor vier jaar. Indien hier aanleiding toe is (bijvoorbeeld bij grote veranderingen) kunnen het college en de burgemeester besluiten tot een tussentijdse herziening. Jaarlijks wordt daarom beoordeeld of het beleid nog passend is. Voor zover deze beleidsnota verder reikt dan alleen een beschrijving van een wettelijk voorschrift, heeft de nota het karakter van een beleidsregel als bedoeld in artikel 1:3, van de Algemene wet bestuursrecht.

4. Versiebeheer

Dit privacybeleid, vervangt het privacybeleid 2020-2024 en het privacyreglement 2018.

Naam	Gepubliceerd
Privacybeleid	Gemeenteblad 2018, 168572
Privacybeleid 2020-2024	Gemeenteblad 2020 nr 355399
Privacyreglement 2018	Gemeenteblad 2018 nr 111634

5. Definitie en begripsbepaling

a. AP: de Autoriteit Persoonsgegevens. Dit is de landelijke toezichthouder die toeziet of persoonsgegevens op een juiste manier worden verwerkt (voorheen: College bescherming persoonsgegevens).
b. AVG: Algemene verordening gegevensbescherming.
c. Betrokkene: de persoon op wie de gegevensbetrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt. Dit kunnen persoons- of politiegegevens zijn.
d. Bevoegd functionaris: zorgt ervoor dat politiegegevens bij een artikel 9 verwerking op een rechtmatige en juiste wijze wordt verwerkt.
e. Chief Information Security Officer (CISO) verantwoordelijk voor de coördinatie van informatiebeveiliging.
f. Data Protection Impact Assessment (DPIA) is een instrument om de privacyrisico's van gegevensverwerking in kaart te brengen en maatregelen te nemen om deze risico's te verminderen. Het wordt ook wel de Gegevensbeschermingseffectbeoordeling genoemd.
g. FG: Functionaris voor gegevensbescherming, toezichthouder op de verwerking van persoonsgegevens.
h. Geautomatiseerd vergelijken: het met een binaire zoeksleutel van (een) trefwoord(en) zoeken van bepaalde politiegegevens. Het resultaat van deze gerichte zoekslag is een uitkomst van hit/no hit.
i. Gecombineerd verwerken: zonder binaire zoeksleutel binnen (een selectie van) beschikbare politiegegevens zoeken naar verbanden. Het resultaat van deze vrije zoekslag is een verzameling van gegevens die voldoen aan bepaalde gemeenschappelijke kenmerken. Deze gemeenschappelijke kenmerken kunnen een profiel van indicatoren of bepaalde kenmerken (trefwoorden) inhouden
j. Gerichte verwerking (artikel 9-verwerking): het verwerken van politiegegevens die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen.
k. Persoonsgegevens: alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijv. naam, adres, geboortedatum). Naast gewone persoonsgegevens zijn er ook bijzondere persoonsgegevens. Die gaan over gevoelige onderwerpen, bijvoorbeeld etnische achtergrond, politieke voorkeuren en de gezondheid.
l. Politiegegevens: een persoonsgegeven dat verwerkt wordt in het kader van de opsporingstaak. Hiervoor geldt de Wet politiegegevens. Een politiegegeven is een specifieke versie van een persoonsgegeven.
m. Proceseigenaar: de afdelingsmanager, verantwoordelijk voor de processen op zijn of haar afdeling.
n. Risicoanalyse: in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen wat de privacy en informatiebeveiligingsrisico's zijn en welke maatregelen getroffen dienen te worden aan de hand van de geconstateerde risico's.
o. Security en privacy officers: ondersteunt de organisatie bij het borgen van informatiebeveiliging en bescherming van persoons-en politiegegevens.
p. SPO team: het centrale team van security en privacy officers.
q. Ter beschikking stellen van politiegegevens: het uitwisselen van politiegegevens met organisaties of medewerkers binnen het Wpg domein.
r. Verstrekken van politiegegevens: Het uitwisselen van politiegegevens met organisaties of medewerkers buiten het Wpg-domein.
s. Verwerkingsverantwoordelijke: een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
t. Verwerker: de persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
u. Verwerking: een verwerking is alles wat met een persoonsgegeven wordt gedaan, zoals vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, vernietigen en lezen.
v. Wpg: Wet politiegegevens.
w. Wpg domein: Alle personen en instanties die gegevens verwerken volgens het regime van de Wpg. Binnen de gemeente zijn dit de BOA's voor zover zij opsporingsgegevens verwerken.

6. Reikwijdte

Het beleid is van toepassing op alle taken en processen waar de gemeente voor verantwoordelijk is. Het heeft betrekking op de persoonsgegevens van personen van wie de gemeente Helmond gegevens verwerkt (of laat verwerken).

Een politiegegevens is een specifieke versie van een persoonsgegeven. Waar in dit beleid wordt gesproken over een persoonsgegeven, wordt daarom ook een politiegegeven bedoeld. Alleen wanneer het beleid specifiek betrekking heeft op een politiegegeven, wordt deze term gebruikt.

7. Uitgangspunten

Geen persoonsgegevens, tenzij die nodig zijn.
Privacy begint bij het niet verzamelen van persoonsgegevens en gaat ook niet alleen over het delen van persoonsgegevens. Bij het inrichten of veranderen van een werkproces is de eerste vraag, of het überhaupt noodzakelijk is om persoonsgegevens te gebruiken. Alleen persoonsgegevens die nodig zijn worden gebruikt.

Het doel voor de verwerking is duidelijk.
Persoonsgegevens worden slechts gebruikt of verzameld voor een van te voren bepaald, concreet omschreven doel (doelbinding). Dat doel bepaalt ook de omvang en de reikwijdte van de te verwerken persoonsgegevens. Er wordt niet meer gebruikt dan strikt nodig is voor dat doel (proportionaliteit). Ook wordt er niet verzameld of gebruikt als er andere mogelijkheden zijn die minder inbreuk maken op de privacy van betrokkenen (subsidiariteit). We treffen alle redelijke maatregelen om te zorgen dat alleen persoonsgegevens worden gebruikt die nodig zijn om het doel te bereiken. Ook treffen we maatregelen om te zorgen dat de persoonsgegevens niet voor een ander doel worden gebruikt.

Er is altijd een grondslag.
Het gebruik van persoonsgegevens is altijd gebaseerd op een (rechts)grondslag uit de AVG of de Wpg. We houden ons daarbij aan de voorwaarden die bij deze grondslag horen. Zie ook de privacyverklaring.

De kwaliteit van de persoonsgegevens is in orde.
De verwerkte persoonsgegevens moeten juist en actueel zijn. Het verwerken van onjuiste persoonsgegevens kan vervelende gevolgen hebben voor betrokkenen. Ook kan het een goede dienstverlening in de weg staan. We treffen maatregelen om te zorgen dat de persoonsgegevens juist zijn en blijven.

De beveiliging van persoonsgegevens is geregeld.
We treffen alle redelijke maatregelen om te zorgen dat op het juiste moment de juiste persoonsgegevens beschikbaar zijn voor de juiste personen. De gemeente houdt zich daarbij aan de BIO en de specifieke eisen uit het Besluit politiegegevens buitengewoon opsporingsambtenaren. Hoe de gemeente dit doet, staat in het strategisch informatiebeveiligings- en privacybeleid 2025-2029 van de gemeente. De basis voor dit beleid is Baseline Informatiebeveiliging Overheid (BIO).

We verwijderen persoonsgegevens zodra het kan.
De gemeente bewaart de persoonsgegevens niet langer dan nodig. De meeste termijnen hiervoor liggen vast in de Archiefwet en de "Selectielijst archiefbescheiden Gemeenten en intergemeentelijke organen 2020". Welke bewaartermijn van toepassing is op een verwerking is terug te vinden in het register van verwerkingen.

Ook voor politiegegevens geldt dat ze worden verwijderd als ze niet langer nodig zijn. Om hiervoor te zorgen worden politiegegevens gelabeld in respectievelijk artikel 8, 9 en 13 informatie. Aan elk label is de wettelijke bewaartermijn ingericht. Politiegegevens, worden na verwijdering nog maximaal vijf jaar bewaard. Daarna worden ze pas vernietigd.

Persoons- en politiegegevens zijn gescheiden.
Voor de politiegegevens die onder de Wpg worden verwerkt gelden (deels) andere regels dan voor de persoonsgegevens die onder de AVG worden verwerkt. Voor politiegegevens die wij onder de Wpg verwerken, gelden bijvoorbeeld andere verwerkingstermijnen en andere regels voor het delen van politiegegevens. De gegevenshuishouding, systemen en werkprocessen voor de Wpg zijn daarom anders ingericht dan bij de overige processen. Voor de Boa's geldt dat zij vaak meerdere taken hebben en verschillende soorten persoonsgegevens verwerken. Persoonsgegevens die een Boa verwerkt in zijn rol als toezichthouder vallen onder de AVG. De politiegegevens die de Boa als opsporingsambtenaar verwerkt, vallen onder de Wpg. Hij of zij heeft dus een 'twee-petten-uitdaging' en is zich daar bewust van.

We verstrekken politiegegevens niet, tenzij dit nodig is.
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen voltrekt zich binnen het Wpg-domein.
Bij het verstrekken van politiegegevens gaat het om het delen van deze gegevens buiten het Wpg-domein. Het gaat dan bijvoorbeeld om verstrekking aan de burgemeester, een toezichthouder, of een functionaris in het kader van de Wet bibob. We verstrekken politiegegevens alleen als dit past binnen de doeleinden van de Wpg en het Besluit. We documenteren de verstrekking en vragen daar waar nodig toestemming van het bevoegd gezag.

8. Het register van verwerkingen

De gemeente heeft in het register van verwerkingen een overzicht gemaakt van de verschillende verwerkingsactiviteiten die onder haar verantwoordelijkheid plaatsvinden. Er is een register van verwerkingen voor de Wpg en een register van verwerkingen voor de AVG. Het verwerkingenregister bevat alle verplichte onderdelen. Dat betekent dat iedere afzonderlijke verwerking nadere informatie bevat over onder meer:

- de herkomst van de persoonsgegevens;
- waarom we de persoonsgegevens gebruiken (doel, -rechts-grondslag);
- welke persoonsgegevens we gebruiken;
- wie de persoonsgegevens ontvangt;
- hoe de persoonsgegevens zijn beveiligd;
- hoe lang de persoonsgegevens worden bewaard.
- De toekenning van autorisaties[1]

Het register is op te vragen bij het SPO-team door te mailen naar SPO@helmond.nl.

9. Risico beperkende maatregelen

9.1 De risicoanalyse

Risicobeheer is de kern van informatiebeveiliging en privacy en sluit aan bij onze architectuurprincipes. We zorgen ervoor dat van al onze processen, diensten en producten en informatiesystemen de risico's bekend zijn. We zoeken goede oplossingen en regelen deze in zodat privacy problemen zich niet of nauwelijks voordoen. We starten pas als de restrisico's voor betrokkenen laag zijn.

Een risicoanalyse heeft betrekking op zowel privacy- als informatiebeveiligingsaspecten. Bij de prioritering van de uit te voeren maatregelen houden we daarom zowel rekening met de risico's voor betrokkenen als de risico's voor de organisatie. Hoe hoger het risico voor betrokkenen hoe hoger de prioriteit.

Een DPIA is onderdeel van de uit te voeren risicoanalyse. De proceseigenaar is verantwoordelijk voor het uitvoeren van een risicoanalyse, het treffen van mitigerende maatregelen en het accepteren van de restrisico's. Hij of zij wordt daarbij ondersteund door medewerkers van zijn eigen afdeling én het SPO-team. Hij of zij vraagt daarnaast advies aan de FG en CISO. De processen zijn beschreven. We hebben daarnaast instructies en procedures. Deze sluiten aan bij de landelijke standaarden van de Vereniging Nederlandse Gemeenten (VNG).

9.2 Privacy by design

Het is van groot belang om aan de voorkant te bedenken welke vragen en problemen vanuit privacy-oogpunt (kunnen) gaan spelen. Door dan al oplossingen te bedenken en toe te passen, zorgen we er al bij het ontwerp voor dat persoonsgegevens goed worden beschermd. Dit noemen we privacy by design.

Uitgangspunt is daarom dat risicomanagement onderdeel is van de besluitvorming. We voeren een risicoanalyse uit bij nieuwe ontwikkelingen en veranderingen:

1. binnen een proces (onderdeel van resultaat van deze procesaanpassing);
2. die leiden tot een project (onderdeel van het projectresultaat; projectfase:
   a. bij opstellen startnotitie: op hoofdlijnen;
   b. tijdens het opstellen van het plan van aanpak: uitvoeren van deze richtlijn;
3. bij beleid (onderdeel van beleidsaanpassing);
4. bij inkoop van producten of diensten.

9.3 Privacy by default

We hanteren het uitgangspunt dat de instellingen van een programma, app, website of dienst zo privacy-vriendelijk mogelijk zijn. Ook dienen de verplichtingen uit de Wpg zoveel als mogelijk te zijn geborgd binnen de applicatie. Dat noemen we privacy by default. Privacy by default is een onderdeel van privacy by design.

1) Alleen voor de Wpg

10. Datalekken

De gemeente gaat zorgvuldig om met persoonsgegevens. Toch kan het voor komen dat onbevoegde personen toegang krijgen tot persoonsgegevens, we persoonsgegevens zijn kwijtgeraakt of persoonsgegevens onterecht worden veranderd. In dat geval spreken we van een datalek. Wanneer er een datalek heeft plaatsgevonden, wordt direct actie ondernomen aan de hand van onze procedure datalekken.

11. Transparantie en communicatie

De gemeente informeert betrokkenen over het verwerken van persoonsgegevens door middel van een privacyverklaring op de website. Wanneer betrokkenen persoonsgegevens aan de gemeente verstrekken, worden zij op de hoogte gesteld op welke manier de gemeente met persoonsgegevens omgaat. Dit kan bijvoorbeeld via een formulier gebeuren. De betrokkene wordt niet nogmaals geïnformeerd als hij of zij al weet dat de gemeente persoonsgegevens verzamelt en verwerkt en weet waarom en voor welk doel dat gebeurt. Daar is sprake van als in wet- of regelgeving de verwerking van persoonsgegevens is opgenomen[2].

12. Rechten van betrokkenen

Privacywetgeving geeft naast verplichtingen voor de gemeente ook diverse rechten aan betrokkenen:

1. **Het recht van inzage**
   Betrokkenen hebben het recht om bij het college te informeren of hun persoons- of politiegegevens worden gebruikt. Is dit het geval dan heeft hij of zij recht op inzage.
2. **Het correctierecht**
   Betrokkenen hebben het recht om persoons- of politiegegevens die onjuist of onvolledig zijn, te laten aanpassen of aanvullen.
3. **Het verwijderingsrecht.**
   Soms hebben betrokkenen toestemming gegeven om uw persoonsgegevens te verwerken. Bijvoorbeeld als men zich heeft aangemeld voor een nieuwsbrief. In die gevallen heeft betrokkene het recht om deze gegevens te laten verwijderen. Betrokkenen hebben ook het recht om hun persoons- of politiegegevens te laten verwijderen als we ze ten onrechte hebben gebruikt. In andere gevallen kunnen persoons- of politiegegevens niet worden verwijderd.
4. **Beperking van de verwerking**
   Betrokkenen kunnen daarnaast vragen om tijdelijk het gebruik van hun persoonsgegevens te "bevriezen". De gegevens kunnen dan tijdelijk niet worden gebruikt of verwijderd. Betrokkenen kunnen in de volgende gevallen vragen om beperking van de verwerking:
   a. **Persoonsgegevens zijn mogelijk onjuist**
      Is betrokkene van mening dat wij onjuiste persoonsgegevens gebruiken? Dan mogen wij deze gegevens niet gebruiken zolang wij ze nog niet hebben gecontroleerd of de gegevens wel kloppen.
   b. **Betrokkene is het niet eens met de verwerking**
      Betrokkene vindt dat wij de persoonsgegevens niet mogen gebruiken en heeft bezwaar gemaakt tegen het gebruik. We mogen de gegevens niet gebruiken tijdens het onderzoek.
   c. **De verwerking is onrechtmatig**
      Wij mogen bepaalde persoonsgegevens niet verwerken. Betrokkene wil niet wat wij de gegevens wissen en vraagt ons om de verwerking te beperken in plaats van te wissen. Wij bewaren de persoonsgegevens, maar mogen ze niet meer gebruiken
   d. **Gegevens zijn niet meer nodig**
      Wij hebben de persoonsgegevens niet meer nodig voor het doel waarvoor we ze hebben verzameld, maar betrokkene heeft de gegevens nog wel nodig voor een rechtsvordering. Bijvoorbeeld een juridische procedure. Wij bewaren de gegevens, maar mogen ze niet meer gebruiken.

12.1 Privacyrechten gebruiken

Betrokkenen kunnen online een verzoek rechten van betrokkene indienen.

Om er zeker van te zijn dat betrokkene is wie hij of zij zegt dat hij of zij is, identificeren wij hem of haar altijd. Inloggen via DigiD is daarom verplicht. Beschikt men niet over DigiD of dient men het verzoek niet online in? Dan stellen we de identificatie altijd vast aan de hand van persoonlijk contact en een origineel identiteitsbewijs. Hiervoor kunnen betrokkenen een afspraak maken met het klantencontact centrum.

2) Bijvoorbeeld in hoofdstuk 5 van de Wet maatschappelijke ondersteuning

Een kopie van een identiteitsbewijs wordt niet geaccepteerd. Er kan namelijk niet worden gecontroleerd of het identiteitsbewijs echt is. Bovendien is een kopie gemakkelijk te vervalsen., zeker met de huidige digitale technieken. Een kopie zorgt dan ook per definitie voor twijfel over de identiteit van betrokkene.

Voor medewerkers geldt dat zij ook een beroep kunnen doen op deze rechten voor zover de organisatie gegevens over hen verwerkt. Omdat zij al bekend zijn bij de organisatie hoeven zij zich niet te identificeren. Zij kunnen hun verzoek daarom rechtstreeks indienen bij het SPO team. Indien nodig kan het SPO team wel aanvullend onderzoek doen om de identiteit van een medewerker vast te stellen.

Betrokkenen mogen alleen hun eigen persoonsgegevens inzien. Anderen mogen alleen persoonsgegevens inzien als zij hier schriftelijk voor zijn gemachtigd. Dit geldt ook voor een curator of mentor, een vertegenwoordiger of belangenbehartiger. Uit de machtiging moet blijken welke informatie mag worden verstrekt, aan wie de informatie mag worden verstrekt en met welk doel. Ook voor gemachtigden geldt er een identificatieplicht.

De verzoeken worden, in samenspraak met de afdeling, afgehandeld door het SPO team. De wijze waarop dit gebeurt is vastgelegd in procedures.
Verzoekt een betrokkene om inzage in al zijn persoonsgegevens, dan volstaan wij met een algemene zoekslag. Betrokkene krijgt op dat moment (alleen) een overzicht van bijvoorbeeld zaken en meldingen waar de persoonsgegevens over betrokkene in voorkomen. Men krijgt dan nog niet de persoonsgegevens zelf. Wil betrokkene die persoonsgegevens wel ontvangen, dan kan hij of zij met behulp van het overzicht een nieuw, gespecificeerd, verzoek indienen.

13. De organisatie van de bescherming van persoonsgegevens

13.1 Wie is bestuurlijk verantwoordelijk?
De bestuursorganen van de gemeente zijn allemaal verwerkingsverantwoordelijken voor de verwerkingen die door hen of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn de burgemeester, het college van B&W en de Gemeenteraad.

13.2 Wie is ambtelijk verantwoordelijk?
De gemeentesecretaris is verantwoordelijk voor het realiseren van de privacydoelstellingen uit dit beleid.

13.3 We hebben een interne toezichthouder.
De gemeente heeft een FG aangesteld. Afspraken over de taken en positie zijn vastgelegd in een reglement.

13.4 Naleving
We sturen op het zorgvuldig en rechtmatig omgaan met persoonsgegevens. Het lijnmanagement houdt actief toezicht op de naleving van het beleid door medewerkers en inhuurkrachten binnen hun verantwoordelijkheidsgebied en corrigeert waar nodig. Middels interne en/of externe audits wordt aangetoond dat wordt voldaan aan de AVG en de Wpg, dat de beveiligingsdoelstellingen van de organisatie worden gehaald en dat de benodigde beheersmaatregelen getroffen en effectief zijn.

De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de richtlijnen op het gebied van privacy. Er zijn verschillende momenten waarop de FG rapporteert over de werkzaamheden en resultaten van de organisatie rondom privacy en informatiebeveiliging. In ieder geval legt de FG eenmaal per jaar een jaarverslag voor aan het dagelijks bestuur.

14. Inwerkingtreding

Dit beleid treedt in werking met ingang van de dag na de datum van haar bekendmaking.

Aldus besloten in de vergadering van het college van burgemeester en wethouders van gemeente Helmond van 31 maart 2026

Burgemeester en wethouders van Helmond,

mr. S.C.C.M. Potters
burgemeester

E.P.H. Koop, MSc
Gemeentesecretaris

Burgemeester van Helmond,

mr. S.C.C.M. Potters
burgemeester