



# Privacyreglement

2018-2021

## 1. Inleiding

In dit reglement laat gemeente Hilversum zien op welke manier zij dagelijks omgaat met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is. Privacy speelt een belangrijke rol in de relatie tussen de burger en de overheid en staat daarmee hoog op de bestuurlijke agenda. Gemeenten hebben de verantwoordelijkheid over persoonsgegevens en gegevensuitwisseling op alle terreinen waar ze actief zijn. Gemeenten zijn verplicht om zorgvuldig en veilig, proportioneel en betrouwbaar om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Goed en zorgvuldig omgaan met persoonsgegevens is een dagelijkse bezigheid van gemeenten. Het beschermen van de privacy is complex, en wordt steeds complexer door technologische ontwikkelingen, de decentralisaties, grote uitdagingen op het terrein van veiligheid en nieuwe Europese wetgeving. Daarom vinden wij het belangrijk om transparant te zijn over de manier waarop wij met persoonsgegevens omgaan, en de privacy waarborgen. Het privacyreglement laat zien op welke wijze de gemeente omgaat met de verwerking van persoonsgegevens. Een nadere invulling en specificatie van de verschillende verwerkingen wordt vastgelegd in het register van verwerken.

## 2. Wetgeving en definities

Op dit moment heeft elke lidstaat van de Europese Unie een eigen privacywet, gebaseerd op de Europese richtlijn van 1995. De Wet bescherming persoonsgegevens (Wbp) regelt het juridische kader voor de omgang met persoonsgegevens in Nederland. Op 25 mei 2018 vervalt de Wbp en treedt de Europese Verordening; de Algemene Verordening Gegevensbescherming (AVG), in werking, samen met de uitvoeringswet. De AVG bouwt voort op de Wbp en zorgt onder andere voor versterking en uitbreiding van de privacy rechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in de AVG gebruikt (Artikel 4, AVG):

*Betrokkene:* De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

*Verwerker:* De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

*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 (bijvoorbeeld; naam, adres, geboortedatum). Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, politieke voorkeuren of het Burgerservicenummer (BSN).

*Data Protection Impact Assessment (DPIA):* Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy.

*Verwerkingsverantwoordelijke:* Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

*Verwerking:* Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

*Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG):* De BIG is een normenkader met beveiligingsmaatregelen die een goed basis-beveiligingsniveau voor gemeenten neerlegt.

### 3. Reikwijdte

Het privacyreglement geldt voor iedereen (zowel intern als externe verwerkers) die gegevens verwerken voor of in opdracht van de gemeente Hilversum.

### 4. Verantwoordelijke

Het college van B&W, of de Burgemeester is eindverantwoordelijk, maar iedereen binnen de organisatie is verantwoordelijk voor de bescherming van de privacy van betrokkenen.

#### Het college van B&W/de Burgemeester

Is eindverantwoordelijk om te waarborgen dat persoonsgegevens worden beschermd in overeenstemming met wet- en regelgeving en op een behoorlijke en zorgvuldige manier. Er is een directe relatie met de beginselen van behoorlijk bestuur.

#### De directie

- De directie is verantwoordelijk voor de sturing;
- ziet toe op de juiste uitvoering van privacybeleid en -reglement en stuurt op (concern) risico's;
- borgt dat de functionaris voor gegevensbescherming (FG) zijn bevoegdheden ongehinderd kan uitvoeren;
- beoordeelt periodiek het privacybeleid en -reglement.

#### Afdelingsmanagers

- rapporteren jaarlijks aan de directie over naleving van wet- en regelgeving en het privacybeleid;
- zorgen dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- zijn verantwoordelijk voor de te nemen maatregelen, die n.a.v. een DPIA, moeten worden getroffen om de privacy van betrokkenen te beschermen.

#### Management

Hieronder vallen alle teammanagers, proceseigenaren, projectleiders en programmamanagers.

Zij zijn verantwoordelijk voor:

- het (laten) opstellen, indien nodig, van het betreffende organisatieonderdeel specifiek protocol en vragen hierover advies aan de privacyfunctionaris en FG en leggen het waar nodig aan het college voor ter vaststelling;
- het borgen van wet-, regelgeving, het privacybeleid en reglement;
- ziet er op toe dat, waar nodig, een DPIA wordt uitgevoerd;
- het tijdig betrekken van de FG bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- het maken van afspraken met andere organisatieonderdelen over het borgen van de privacy in geval van informatie die stroomt tussen verschillende organisatieonderdelen.

#### Medewerkers (inclusief inhuur/extern)

Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkenen. Dat betekent dat iedereen zorgt, binnen de kaders van zijn rol/functie, voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

#### Functionaris voor gegevensbescherming

- informeert en adviseert over de verplichtingen die de organisatie heeft met betrekking tot de bescherming van persoonsgegevens;

- ziet toe op de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens;
- ziet toe op het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van de organisatie op het gebied van de bescherming van persoonsgegevens;
- geeft advies over Data Protection Impact Assessment (DPIA);
- werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens;
- in samenspraak met de privacyfunctionaris evalueren van het privacybeleid, opstellen van voorstellen tot implementatie en aanpassingen van het privacybeleid,
- bewaakt en beheert samen met de privacyfunctionaris het verwerkingenregister,
- rechtstreeks rapporteren aan het college van B&W.

#### De privacyfunctionaris

Er kunnen meerdere privacyfunctionarissen werkzaam zijn binnen de organisatie, zoals een organisatie brede privacyfunctionaris, maar ook specifiek gericht op een vakgebied.

De privacyfunctionaris:

- bevordert en adviseert de organisatie gevraagd en ongevraagd over de bescherming van persoonsgegevens,
- controleert en evalueert de naleving van wet- en regelgeving en het door het college vastgestelde beleid met betrekking tot de bescherming van persoonsgegevens,
- verzorgt rapportages over de status,
- evalueert, in samenspraak met de FG, het privacybeleid, doet voorstellen tot implementatie en aanpassingen van het privacybeleid,
- rapporteert rechtstreeks aan de FG en de directie.

#### Businesscontroller

rapporteert aan de directie over naleving van wet- en regelgeving en het privacybeleid, richtlijnen en processen.

## **5. Verwerkingen (Artikel 4, AVG)**

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat je met een persoonsgegeven doet een verwerking is.

#### **Doeleinden (Artikel 5, AVG)**

Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Het doel moet uitdrukkelijk omschreven en gerechtvaardigd zijn. De gegevens mogen niet voor andere doelen verwerkt worden. Voor de uitvoering van sommige wetten, zoals bijvoorbeeld de Jeugdwet, zijn de doelen voor het verwerken in de wet al vastgelegd, net als de persoonsgegevens die gevraagd en verwerkt mogen worden.

#### **Rechtmatige grondslag (Artikel 6, AVG)**

De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Dat betekent dat de verwerking alleen mag plaatsvinden:

- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden
- Voor de goede vervulling van de gemeentelijke taak
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking

### **Wijze van verwerking**

De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De wet gaat uit van subsidiariteit. Dit betekent dat verwerking alleen is toegestaan wanneer het doel niet op een andere manier kan worden bereikt. In de wet wordt ook gesproken over proportionaliteit. Dit betekent dat persoonsgegevens alleen mogen worden verwerkt als dit in verhouding staat tot het doel. Wanneer met geen, of minder (belastende), persoonsgegevens hetzelfde doel bereikt kan worden moet daar altijd voor gekozen worden.

De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. Deze gegevens worden alleen verwerkt door personen met een geheimhoudingsplicht. Daarnaast beveiligd de gemeente alle persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. De kaders hiervoor zijn vastgelegd in het informatieveiligheidsbeleid van de gemeente. Uitwerkingen hiervan liggen vast in procedures en protocollen, gebaseerd op de BIG, die jaarlijks worden geëvalueerd.

### **Doorgifte (Artikel 44 t/m 50, AVG)**

De gemeente geeft alleen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie op grond van goedgekeurde afspraken door de Europese Commissie.

### **Data Protection Impact Assessment (DPIA) (Artikel 35, AVG)**

Met een data protection impact assessment worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De gemeente voert deze uit wanneer er een geautomatiseerde verwerking, een grootschalige verwerking, of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

### **Privacy by design/default (Artikel 23 AVG)**

Privacy by design houdt in dat al tijdens de ontwikkeling van producten en diensten aandacht wordt besteedt aan privacy verhogende maatregelen. De gemeente voert dit uit in een vroegtijdig stadium om mogelijke kostbare en tijdrovende aanpassingen te voorkomen. Privacy by default houdt in dat de gemeente technische en organisatorische maatregelen neemt om alleen persoonsgegevens te verwerken die noodzakelijk zijn voor het specifieke doel.

Door de uitvoering van een DPIA kan tijdig bij privacy by design/default worden gezien en bepaald welke maatregelen moeten worden genomen.

## **6. Transparantie en communicatie**

Via de Wet openbaarheid van bestuur (Wob) kun je een verzoek om informatie indienen bij de gemeente. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

Wet hergebruik van overheidsinformatie De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

#### **Vestrekking op basis van open data.**

De gemeente Hilversum verzamelt verschillende soorten gegevens om haar werk zo goed mogelijk te kunnen doen. Geografische data, bezoekersaantallen, productinformatie (aantallen verstrekte reisdocumenten of aantal uitkeringsgerechtigden e.d.) of allerlei gegevens over de stad. Deze informatie kan waardevol en interessant zijn voor bedrijven, organisaties, journalisten, onderzoekers en bewoners. Zij kunnen hiermee bijvoorbeeld applicaties en websites ontwikkelen. Daarom stelt de gemeente deze data zo veel en zo gemakkelijk mogelijk beschikbaar. Bij open data gaat het alleen over informatie die openbaar gemaakt mag worden en dus nooit over gegevens die herleidbaar zijn tot een persoon.

#### **Informatieplicht (Artikel 13,14, AVG)**

De gemeente Hilversum informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan.

De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt en weet voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

#### **Verwijdering**

De gemeente bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van gemeentelijke taken, of zoals vastgelegd in de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren.

#### **Rechten van betrokkenen (Artikel 13 t/m 20, AVG)**

De wet bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden ook wel de rechten van betrokkenen genoemd, en bestaan uit de volgende rechten:

##### *Recht op informatie*

Betrokkenen hebben het recht om aan de gemeente te vragen of zijn/haar persoonsgegevens worden verwerkt.

##### *Inzagerecht*

Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt.

##### *Correctierecht*

Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren.

##### *Recht van verzet*

Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken.

### *Recht om vergeten te worden*

In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.

### *Recht op bezwaar*

Betrokkenen hebben het recht om bezwaar aan te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

### **Indienen van verzoek**

Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via de e-mail ingediend worden. De gemeente heeft vier weken de tijd, vanaf de ontvangst van het verzoek, om te beoordelen of het verzoek gerechtvaardigd is. Binnen vier weken zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Als het verzoek niet wordt opgevolgd is er de mogelijkheid om bezwaar te maken bij de gemeente, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

### **Geautomatiseerde verwerkingen, profilering (Artikel 22, AVG)**

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van de persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering.

Op grond van de AVG is het niet toegestaan om profilering te gebruiken. In Artikel 22.2 worden de uitzonderingen opgesomd:

1. Noodzakelijk voor de uitvoering van een overkomst tussen de betrokkene en verwerkingsverantwoordelijke.
2. Toegestaan door Nederlands/EU recht.
3. Na toestemming van de betrokkene.

Gemeente Hilversum maakt geen gebruik van profilering.

### **Big data en tracking**

De gemeente Hilversum maakt ook gebruik van nieuwe technologieën, zoals Big data en tracking. Voor het optimaal uitvoeren van bepaalde taken kan het nodig zijn om Big data en tracking te gebruiken. Hierbij kunt u bijvoorbeeld denken aan:

- het volgen van de aanwezig mobiele telefoons om grote publieksstromen of verkeersstromen te monitoren en in goede banen te leiden (bijvoorbeeld tijdens grote evenementen) om de veiligheid van de burgers te vergroten.
- tracking om fietsstromen (aantallen) in kaart te brengen en daarop eventuele regulerende maatregelen te kunnen treffen. Denk aan het bieden fietsparkeervoorzieningen.

Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon en mag echter niet leiden tot schending van de privacy. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen toegankelijk voor hiervoor geautoriseerde personen. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het

behalen van het doel gebruikt zullen worden. Daarnaast worden de persoonsgegevens geanonimiseerd zodat zij niet herleidbaar zijn tot een persoon.

### **Inzet van camera's**

Binnen gemeente Hilversum wordt er onderscheid gemaakt tussen twee vormen van cameratoezicht. Cameratoezicht van gemeentelijke gebouwen (beveiliging) en cameratoezicht ten behoeve van toezicht in de openbare ruimte (openbare orde of veiligheid). Dit laatste vindt plaats namens de gemeente, na een daartoe strekken besluit van de burgemeester en wordt gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden, daarom werkt de gemeente hiervoor samen met de politieorganisatie. Om de privacy zo goed mogelijk te waarborgen zijn de afspraken hierover gewaarborgd in een procedure. Alleen politieambtenaren of hiertoe door de Burgemeester aangewezen Buitengewoon opsporingsambtenaren hebben toegang tot de camerabeelden.

Cameratoezicht voor gemeentelijke gebouwen is een ondersteunend middel bij de bescherming van medewerkers en bezoekers alsmede bij de beveiliging van de eigendommen van de medewerkers en bezoekers. De bepalingen zijn opgenomen in het reglement cameratoezicht beveiliging gemeentelijke gebouwen. Bij inzet van camera's voor andere gemeentelijke doeleinden dient voorafgaand aan deze inzetadvies te worden gevraagd aan de functionaris voor de gegevensbescherming.

## **7. Plichten van de gemeente Hilversum**

Register van verwerken (Artikel 30, AVG) De gemeente is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de gemeente de verwerkingsverantwoordelijke is. Elk register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt, en welke gegevens daarvoor worden gebruikt, namelijk:

- De verwerkingsverantwoordelijke en/of de gezamenlijk verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisaties;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;

### **Datalekken (Artikel 33, 34, AVG)**

We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden meldt de gemeente dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan het AP. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval meldt de gemeente dit aan de betrokkenen in duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

### **Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)**

De gemeente heeft een FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van het AP. Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen overneemt. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG

gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke richtlijnen op het gebied van privacy.

**Contactgegevens FG**

Voor vragen over privacy of over deze toelichting kunt u contact opnemen met de functionaris voor gegevensbescherming van gemeente Hilversum via email: [fg@hilversum.nl](mailto:fg@hilversum.nl)

**Afsluiting**

Als de gemeente een wettelijke verplichting niet nakomt kan de betrokkene een klacht indienen. Deze zal via de klachtenregeling van de gemeente worden behandeld. In gevallen waar het reglement niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.