



Privacyreglement

Inhoud

Privacyreglement gemeente Meerijstad	3
1. Wetgeving en definities	3
2. Reikwijdte	4
3. Verantwoordelijke	4
4. Verwerkingen	4
4.1 Doeleinden	5
4.2 Rechtmatige grondslag	5
4.3 Wijze van verwerking	5
4.4 Doorgifte	5
5. Transparantie en communicatie	5
5.1 Informatieplicht	5
5.2 Verwijdering	5
5.3 Rechten van betrokkenen	5
5.4 Indienen van verzoek	6
6. Plichten van de gemeente	6
6.1 Register van verwerkingen	6
6.2 Verwerkersovereenkomsten	6
6.3 Privacy bij design en privacy by default	6
6.4 Privacy impact assessments (PIA's)	7
6.5 Aanstellen van een Functionaris voor gegevensbescherming en Privacy officer (PO)	7
6.6 Meldplicht datalekken	7
Afsluiting	7

Privacyreglement gemeente Meierijstad

Het privacyreglement is een verdieping van het privacybeleid en laat zien hoe gemeente Meierijstad 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 vertrouwelijk om te gaan met het verzamelen, bewaren en beheren van persoonsgegevens van burgers. Dat geldt o.a. voor taken op het gebied van basisadministraties, openbare orde en veiligheid en het sociaal domein. 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.

1. Wetgeving en definities

Tot 25 mei 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 privacyrechten met meer verantwoordelijkheden voor organisaties.

De volgende begrippen worden in het privacyreglement gebruikt.

AP

De Autoriteit Persoonsgegevens, op grond van de AVG bevoegd om toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de Wet bepaalde (voorheen: College bescherming persoonsgegevens).

AVG

Algemene Verordening Gegevensbescherming, VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Betrokkene

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

Dataminimalisatie

Alleen de informatie die noodzakelijk is voor de uitvoering van wettelijke taken wordt opgeslagen.

Functionaris Gegevensbescherming (FG)

Het college van burgemeester en wethouders benoemt een functionaris voor de gegevensbescherming, zoals bedoeld in de AVG, die belast is met toezicht op het privacy- en beveiligingsbeleid van de gemeente.

Privacy impact assessments (PIA's)

Met een de uitvoering van PIA's worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. De AVG noemt dit een Gegevensbeschermingseffectbeoordeling.

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, foto). 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).

Privacy Officer (PO)

Het college van burgemeester en wethouders stelt een privacy Officer aan, die belast is met coördineren, informeren en adviseren op het gebied van AVG en bewustwording creëren binnen de organisatie.

Verwerker

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

Verwerking

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

Verwerkingsverantwoordelijke

De verantwoordelijke voor de verwerking van persoonsgegevens, zoals bedoeld in de AVG, is het college van burgemeester en wethouders, respectievelijk de burgemeester.

2. Reikwijdte

Het reglement is van toepassing op alle verwerkingen van persoonsgegevens door alle bestuursorganen van de gemeente. Oftewel: voor alle verwerkingen die namens de gemeente plaatsvinden.

3. Verantwoordelijke

De bestuursorganen van de gemeente zijn allemaal verantwoordelijken voor de verwerkingen die door of namens de gemeente worden uitgevoerd. De bestuursorganen van de gemeente zijn onder andere de burgemeester, het college van Burgemeester en Wethouders (college van B&W) en de Raad.

4. Verwerkingen

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.

4.1 Doeleinden

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.

4.2 Rechtmatige grondslag

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 waarbij de betrokkene partij is;
- 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.

4.3 Wijze van verwerking

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 treft de gemeente organisatorische en technische maatregelen om risico's met betrekking tot beveiliging van alle persoonsgegevens tot een minimum te beperken. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. Hoe de gemeente dit doet staat in het informatiebeveiligingsbeleid.

4.4 Doorgifte

Persoonsgegevens mogen in principe niet worden doorgegeven naar een organisatie in een land buiten de EU. Dit komt omdat binnen de EU een goede bescherming voor de persoonsgegevens is, en daarbuiten niet in alle gevallen. 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.

5 Transparantie en communicatie

5.1 Informatieplicht

Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken. De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Betrokkenen krijgen vooraf duidelijke informatie tijdens de dienstverlening en via de website en andere kanalen (telefonisch, schriftelijk, email) over de verwerking van hun persoonsgegevens en het doel van de verwerking.

5.2 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.

5.3 Rechten van betrokkenen

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;
- inzage recht: 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 te maken tegen de verwerking van zijn/haar persoonsgegevens. De gemeente zal hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

5.4 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.

6 Plichten van de gemeente

6.1 Register van verwerkingen

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 naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke 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 ander land of internationale organisatie;
- de termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- een algemene beschrijving van de beveiligingsmaatregelen.

6.2 Verwerkersovereenkomsten

Bij veel gemeentelijke processen worden gegevens verwerkt door derden. Denk hierbij aan informatiesystemen die in een Cloudoplossing draaien, maar ook aan uitbestede werkzaamheden of samenwerkingsverbanden. Het delegeren van werkzaamheden aan derden brengt risico's met zich mee op het gebied van gegevensverwerking en informatiebeveiliging. De gemeente blijft verantwoordelijk voor de verwerking van de gegevens. Zij moet er daarom op toezien dat gegevens juist verwerkt en beveiligd worden, en dat daarover afspraken worden gemaakt met de betreffende derde partij (verwerker) middels een "verwerkersovereenkomst". Hierbij is het belangrijkste uitgangspunt dat deze verwerkers voldoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen bieden zodat de verwerking aan de vereisten voldoen en de bescherming van de rechten van de betrokkene is gewaarborgd.

6.3 Privacy bij design en privacy by default

Privacy by design houdt in dat vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens en de maatregelen die hiervoor nodig zijn.

Privacy by default betekent dat de standaard instellingen in systemen zijn ingesteld om maximale privacy bescherming te borgen. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'.

6.4 Privacy impact assessments (PIA's)

Voor processen, diensten en producten en informatiesystemen, waar persoonsgegevens worden verwerkt, worden PIA's uitgevoerd. Hiermee worden verwerkingen van persoonsgegevens, doeleinden, risico's en (voorgenomen) maatregelen beschreven. Het doel is om de impact van de verwerkingen op de bescherming van persoonsgegevens in kaart te brengen om vervolgens waar nodig de juiste maatregelen te treffen.

6.5 Aanstellen van een Functionaris voor gegevensbescherming en Privacy officer (PO)

De gemeente heeft een FG en een PO aangesteld. De FG en de PO zijn betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de FG zijn toezicht houden op de implementatie en naleving van het privacybeleid, het rapporteren aan de directie en het bestuur over het gevoerde beleid met betrekking tot privacy en optreden als contactpersoon van het AP.

De taken van de PO zijn informeren, adviseren, coördineren en bewustwording creëren binnen de organisatie.

Om de functiescheiding te waarborgen is er een knip gelegd tussen de toezichthoudende en controlerende rol van de FG en de coördinerende, adviserende en de uitvoerende rol van de PO. Het is niet de bedoeling dat de FG en de PO de taken op het gebied van bescherming van de privacy van de ateliers overnemen. De ateliers zijn zelf verantwoordelijk voor het goed en conform regelgeving omgaan met privacygevoelige gegevens.

6.6 Meldplicht datalekken

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 de 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 eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd.

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 de regeling niets over zegt, beslist het verantwoordelijke bestuursorgaan van de gemeente.

Aldus vastgesteld door burgemeester en wethouders van gemeente Meerijstad op [datum],

[Naam. Functie]

[Naam. Functie]

[Handtekening]

[Handtekening]