CVDR

Officiële uitgave van Groningen.

Nr. CVDR610577_1

6 juni 2018

Privacybeleid gemeente Groningen 2018

HET COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN DE GEMEENTE GRONINGEN;

BESLUIT:

vast te stellen het

Privacybeleid gemeente Groningen 2018

1. Inleiding

De gemeente Groningen (hierna: de gemeente) verwerkt veel persoonsgegevens van burgers voor haar dienstverlening en het uitvoeren van haar gemeentelijke taken. Ook verwerkt de gemeente persoonsgegevens van personen die werkzaam zijn voor haar. gemeente gaat zorgvuldig om met persoonsgegevens. Dit privacy beleid (hierna: het beleid) geeft aan op welke manier. Dit beleid is een uitwerking van de Algemene Verordening Gegevensbescherming (AVG).

2. Definitie en begripsbepaling

a. *Anonimiseren*: persoonsgegevens die voor een taakuitvoering niet meer noodzakelijk zijn, worden verwijderd uit een dataset. De dataset bevat dan enkel geanonimiseerde gegevens, die wel worden bewaard voor bijvoorbeeld onderzoeksdoeleinden of om te gebruiken als open data. Bij anonimiseren is onomkeerbaar, waarbij na toepassing ervan herleiden van gegevens tot individuen niet meer mogelijk is.
b. *AP*: de Autoriteit Persoonsgegevens. Dit is de landelijke toezichthouder die toeziet of persoonsgegevens op een juiste manier worden verwerkt (voorheen: College bescherming persoonsgegevens).
c. *Betrokkene*: de persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
d. *CFIB*: Concern Functionaris Informatie Beveiliging, verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen de gemeente.
e. *FG*: Functionaris Gegevensbescherming, toezichthouder op de verwerking van persoonsgegevens
f. *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.
g. *Privacy impact assessment (PIA)*: in een vroeg stadium op een gestructureerde en heldere manier in beeld brengen wat de privacy risico's zijn en welke maatregelen getroffen dienen te worden aan de hand van de geconstateerde risico's.
h. *Pseudonimiseren*: is het versleutelen van gegevens op een zodanige manier dat de betrokkene niet meer rechtstreeks identificeerbaar is, maar nog wel individualiseerbaar. Er is hier sprake van (de mogelijkheid tot) omkeerbaarheid.
i. *Verwerkingsverantwoordelijke*: een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
j. *Verwerker*: de persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
k. *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.

3. Reikwijdte

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

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

4. Uitgangspunten voor de verwerking van persoonsgegevens

a. *Geen persoonsgegevens, tenzij die nodig zijn*

Privacy begint bij het niet verzamelen van gegevens. Bij het inrichten van een werkproces moet de eerste vraag zijn, of het überhaupt noodzakelijk is om persoonsgegevens te verzamelen, gelet op het doel van het proces. Alleen voor zover er een noodzaak bestaat, vindt verwerking van persoonsgegevens. En als persoonsgegevens worden verwerkt, dan worden alleen die persoonsgegevens gebruikt, die strikt noodzakelijk zijn.

b. *Het doel voor de verwerking moet duidelijk zijn*
Persoonsgegevens worden slechts 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 verzameld dan strikt nodig is voor dat doel (proportionaliteit), en er wordt niet verzameld als er een manier voorhanden is om de informatie te krijgen op een wijze die minder inbreuk maakt op de privacy (subsidiariteit).

c. *Er moet een rechtmatige grondslag zijn voor de verwerking*
De gemeente vraagt toestemming aan de betrokkene voor de verwerking van persoonsgegevens, tenzij sprake is van een verplichting om de persoonsgegevens te verwerken op grond van een wettelijke bepaling of een overeenkomst.

d. *De kwaliteit van de persoonsgegevens is in orde*
De verwerkte persoonsgegevens moeten juist zijn. Het verwerken van onjuiste gegevens kan problemen met zich meebrengen en vervelende gevolgen hebben voorbetrokkenen en voor de goede uitoefening van de overheidsfunctie. Om deze reden moeten alle redelijke maatregelen worden genomen om onjuiste persoonsgegevens onverwijld te wissen en te rectificeren. Voor zover mogelijk, vinden geautomatiseerd controles op bestanden met persoonsgegevens plaats.

e. *De beveiliging van persoonsgegevens*
De persoonsgegevens worden alleen verwerkt door bevoegde personen met een geheimhoudingsplicht. Daarnaast beveiligt de gemeente alle persoonsgegevens om te 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 van de gemeente.

f. *Verwijdering van persoonsgegevens*
De gemeente bewaart de persoonsgegevens niet langer dan nodig. De meeste termijnen hiervoor liggen vast in de Archiefwet en andere wetten waar de termijnen zijn vastgelegd. Dit houdt in dat de gegevens vernietigd worden, of ze worden zo aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Welke bewaartermijn van toepassing is op een verwerking is terug te vinden in het digitaal register persoonsgegevens.

5. Het digitaal register persoonsgegevens

De gemeente heeft een openbaar register van alle verwerkingen van persoonsgegevens waarvoor de gemeente verantwoordelijk is. In het register zijn een aantal gegevens opgenomen, waaronder:

1. De naam en contactgegevens van de verwerkingsverantwoordelijke, en – indien dat het geval is – de gezamenlijke verwerkingsverantwoordelijken;
2. Het doel of de doelen van de verwerking;
3. Een beschrijving van de soort persoonsgegevens en de categorieën van betrokkenen;
4. Een beschrijving van de ontvangers van de persoonsgegevens;
5. Een beschrijving van – indien dat het geval is - het delen van persoonsgegevens aan een derde land of internationale organisatie;
6. De bewaartermijn van de gegevens;
7. Een algemene beschrijving van de beveiligingsmaatregelen.

6. Risico beperkende maatregelen

De Privacy Impact Assessment
Op het moment dat er sprake is van een verhoogd risico bij het gebruik van de persoonsgegevens, brengt de gemeente de privacy risico's in kaart door de Privacy Impact Assessment (PIA). Op basis van de PIA neemt de gemeente maatregelen om de risico's zo veel mogelijk weg te nemen. Pas nadat de PIA is uitgevoerd en de maatregelen zijn getroffen die nodig zijn om de risico's te beperken, verwerkt de gemeente de persoonsgegevens. In geval van het verwerken van bijzondere persoonsgegevens en profilering wordt altijd een PIA uitgevoerd.

Privacy by design
Bij de inrichting van een werkproces - inclusief de ICT infrastructuur - is het van groot belang om direct te bedenken welke vragen en problemen vanuit privacy-oogpunt in en rondom dat werkproces een rol (kunnen) gaan spelen. Gebeurt dat, en worden daarbij goede oplossingen bedacht en ingeregeld, dan wordt er aan de voorkant voor gezorgd dat bepaalde privacy problemen zich niet kunnen voordoen. Denk bijvoorbeeld aan een logische en strakke toegangsbeveiliging, encryptie van gegevens, het scheiden van databestanden of het automatisch verwijderen van gegevens na een bepaalde periode of gebeurtenis. Dit noemen we 'privacy by design'. Privacy by design is van grote betekenis om in control te komen en te blijven op privacy gebied.

Privacy by default
Aanvullend op privacy by design wordt als uitgangspunt gehanteerd dat de instellingen van een programma, app, website of dienst zodanig zijn dat maximale privacy wordt betracht. Let wel: dat is de maximale stand van dat programma of die dienst. Het gaat niet alleen om opties die kunnen worden ingesteld, ook zaken als algemene voorwaarden moeten privacy vriendelijk zijn. Dus geen verstopte privacy-onderwerpen op een plek waar ze niet thuishoren. Geen opt-out regime, maar opt-in: pas als iemand zich ergens voor heeft aangemeld ontvangt hij informatie (opt-in), niet het automatisch versturen totdat door de betrokkene wordt verzocht dit stop te zetten (opt-out).

7. Datalekken
De gemeente gaat zorgvuldig om met persoonsgegevens. Toch kan het voor komen dat onbevoegde personen toegang krijgen tot persoonsgegevens, of persoonsgegevens kwijt zijn geraakt. In dat geval spreken we van een datalek. Wanneer er een datalek heeft plaatsgevonden, wordt direct actie ondernomen aan de hand van het protocol datalekken.

8. Transparantie en communicatie

Informatieverstrekking
De gemeente informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente verstrekken, worden zij op de hoogte gesteld op welke manier de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.

9. Rechten van betrokkenen
Als persoonsgegevens door de gemeente worden verwerkt, heeft de betrokkene een aantal rechten. 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 wijze zijn of haar gegevens worden verwerkt.
- Correctierecht: als duidelijk wordt dat de gegevens niet juist zijn, 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 op het wissen van persoonsgegevens: in gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene in een aantal in de AVG aangegeven gevallen, het recht om de persoonsgegevens te laten wissen.
- 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.
- Recht op het doorgeven van informatie (dataportabiliteit): betrokkene heeft recht om gegevens beschikbaar gesteld te krijgen op een dergelijk manier dat betrokkene deze zelf gemakkelijk door kan geven aan een andere verwerkingsverantwoordelijke.

Indienen van een verzoek
Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk, als via de website van de gemeente ingediend worden.

De gemeente verstrekt de betrokkene onverwijld en in ieder geval binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van een dergelijke verlenging. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

Als het verzoek niet wordt opgevolgd, is er de mogelijkheid om bezwaar te maken bij de gemeente. Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

Als de gemeente een wettelijke verplichting niet nakomt, kan de betrokkene een klacht indienen. Op de website van de gemeente Groningen staat op welke manier dat mogelijk is.

10. Geautomatiseerde verwerkingen

a. *Profilering/profiling*
Computers genereren veel gegevens en zijn in staat veel bestanden met persoonsgegevens met elkaar te verbinden. De techniek geeft vele mogelijkheden tot 'profiling' (profilering); aan de hand van een geautomatiseerd verwerking van meerdere persoonsgegevens de personen selecteren die aan bepaalde van te voren vast gestelde criteria (risicofactoren) voldoen. De gemeente Groningen doet - in principe - niét aan profiling. Daarmee handelen we in overeenstemming met de Algemene Verordening Gegevensbescherming, die profilering in beginsel verbiedt en slechts in bepaalde situaties onder strikte voorwaarden toelaat.

b. *Big data en tracking*
- Gegevens in big data en tracking mogen alleen worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon en worden alleen verzameld voor onderzoek dat door of namens gemeente wordt uitgevoerd.
- Voor big data en tracking wordt uitsluitend gebruik gemaakt van brongegevens die door daartoe geautoriseerde personen zijn verzameld.
- Brongegevens die gebruikt worden voor big data toepassingen worden omgezet tot een dataset die geen persoonsgegevens bevat en dus geanonimiseerd is.
- Indien anonimiseren niet mogelijk is, wordt vooraf toestemming aangevraagd aan de FG die de aanvraag zal beoordelen in het kader van de wet en doelmatigheid. Alleen bij een goedgekeurde aanvraag mogen de gegevens gepseudonimiseerd in plaats van geanonimiseerd worden.
- Onderzoek aan de hand van de dataset mag niet door dezelfde medewerkers worden uitgevoerd die de gegevens hebben verzameld;

c. *Inzet van camera's*
Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van degenen die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen, worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's. De gemeente heeft een aparte verordening waarin de voorwaarden voor het gebruik van cameratoezicht is geregeld.

Het gebruik van camera's door particulieren op de openbare weg is alleen mogelijk met toestemming van het college van burgermeester en wethouders(hierna: college van B&W). Daarvoor wordt er een convenant afgesloten tussen de particulieren en het bestuursorgaan. Daarin staat onder meer de juridische grondslag, het doel, de maatregelen tegen verlies, de beveiligingsmaatregelen en de bewaartermijnen.

11. De organisatie van de bescherming van persoonsgegevens

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

b. *Wie is ambtelijk verantwoordelijk?*
De directies zijn integraal verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens binnen de eigen directie.

c. *Contactpersoon voor de gegevensbescherming*
Elk organisatieonderdeel heeft een contactpersoon die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel.

12. Functionaris Gegevensbescherming

De gemeente heeft een Functionaris voor Gegevensbescherming aangesteld (hierna: de FG). De FG is de gemeentelijke toezichthouder met betrekking tot de bescherming van persoonsgegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en de gemeentelijke regels op het gebied van privacy.

De FG is betrokken bij alle aangelegenheden die verband houden met de verwerking van persoonsgegevens. De FG adviseert, informeert en rapporteert de organisatie over het gebruik van persoonsgegevens, periodiek aan de gemeentesecretaris en stelt een jaarverslag op. Een verwerking van persoonsgegevens met een hoog risico wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is ook de contactpersoon voor de organisatie met de Autoriteit Persoonsgegevens – de landelijke toezichthouder op het terrein van privacy.

De FG dient voor zijn taak goed bereikbaar te zijn, in de organisatie maar ook voor de betrokkenen in verband met het uitoefenen van hun rechten. Daarom zijn de contactgegevens van de FG vermeld op de website van de gemeente en in het register van de Autoriteit Persoonsgegevens

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

Gedaan te Groningen in de collegevergadering van 29 mei 2018,

De burgemeester,
Peter denOudsten

De secretaris,
PeterTeesink