



Raadsbesluit

Onderwerp: Nota Privacybeleid haarlem

BBV nr: 2016/574466

1. Inleiding

Aanleiding

Privacy is een onderwerp dat de laatste jaren veel in de belangstelling staat. Data zijn hot en worden het nieuwe goud genoemd. De mogelijkheden om gegevens en dus ook persoonsgegevens digitaal op te slaan, te bewerken en te delen hebben de afgelopen jaren een enorme vlucht genomen. Ook als gemeente maken we veel gebruik van data. Het gebruik van digitale gegevens brengt gemak en nieuwe mogelijkheden. Tegelijk brengt het ook risico's met zich mee. Voorkomen moet worden bijvoorbeeld dat – welwillend of kwaadwillend – meer mensen dan nodig en wenselijk toegang hebben of zichzelf toegang verschaffen tot de opgeslagen gegevens. Mensen van wie de gemeente gegevens verwerkt, hebben er recht op dat de gemeente daar uiterst zorgvuldig mee omgaat. In de Nota Informatievoorziening 'Transparant & Veilig' (2015/162970) is daarom een Privacynota aangekondigd. In deze nota wordt het Haarlemse beleid beschreven met betrekking tot het gebruik en de bescherming van persoonsgegevens.

Wat deed Haarlem tot nu toe aan privacy?

Privacy is natuurlijk niet een volledig nieuw thema. Van 1988 tot 2006 kende Haarlem een zogeheten Registratiecommissie, die tot taak had te adviseren over de bescherming van persoonsgegevens. In 2006 werd deze commissie opgeheven en werd ook de Privacyverordening ingetrokken, omdat de zorg voor privacy onderdeel werd van de algemene interne kwaliteitszorg. Door voortschrijdende digitalisering en ook nieuwe wetgeving volstaat dat niet meer en is extra aandacht nodig en een expliciet privacykader.

Raakvlakken met ander beleid

Privacybeleid raakt aan beleid rond informatievoorziening en informatiebeveiliging (2015/128172), integriteitsbeleid (2015/467586) en beleid over geheimhouding (2015/34307). Haarlem stelt bovendien steeds meer data beschikbaar in de vorm van open data. Een beleidsstuk daarover is in voorbereiding.

Zienswijzen anonimiseren?

De afgelopen weken is er discussie ontstaan over de vraag of bij de beantwoording van zienswijzen de naam van de indieners zouden moeten staan of dat ze worden geanonimiseerd. Het college stelt voor de namen van degenen die een zienswijze hebben ingediend wel bekend te maken bij de beantwoording van de zienswijzen en dus ook te publiceren op internet. Uit het antwoord van de minister van binnenlandse zaken op kamervragen over deze kwestie¹ blijkt dat "het aankomt op een afweging van belangen door gemeenten in het specifieke geval". Post- en mailadres worden daarbij niet vermeld.

2. Voorstel aan de raad

Het college stelt de raad voor:

¹ [Beantwoording-kamervragen-over-verwarring-omtrent-het-publiceren-van-namen-door-gemeenten](#)
Kenmerk 2014-0000288486

1. De Nota Privacybeleid Haarlem vast te stellen;
2. In te stemmen met de volgende uitgangspunten:
 - *Werk met het minimum aan persoonsgegevens*
Als het nodig is of verplicht om persoonsgegevens te verwerken, gebeurt dat met het minimum dat nodig is.
 - *Maximale transparantie*
Het principe van maximale transparantie betekent op het gebied van privacy dat gedocumenteerd wordt waar welke persoonsgegevens worden verwerkt en met welk doel.
 - *Privacy by design*
Waar nieuwe werkprocessen worden ingericht worden die direct zo ontworpen dat de privacy is gewaarborgd.
 - *Role based access*
Toegang tot persoonsgegevens krijgen medewerkers alleen als dat voor hun taak noodzakelijk is. Autorisaties worden actueel gehouden en het gebruik van gegevens wordt steekproefsgewijs gecontroleerd.
 - *Inzagerecht*
Burgers kunnen opvragen welke gegevens de gemeente over hem of haar verwerkt;
3. Met ingang van 1 februari 2017 de formatie van de afdeling Strategie en Beleidscoördinatie uit te breiden met 1fte voor de functie Privacyadviseur, in schaal 11A en de jaarlijkse lasten ad € 85.000,- te dekken uit de algemene middelen.

3. Beoogd resultaat

Het doel van deze nota is driedig:

1. Het beschrijven van de Haarlemse uitgangspunten op het gebied van privacybescherming;
2. Een concreet kader te bieden voor het werken met persoonsgegevens;
3. Voorbereiding op de nieuwe Europese Algemene Verordening Gegevensbescherming.

4. Argumenten

Haarlem wil een betrouwbare overheid zijn

Mensen van wie de gemeente gegevens verwerkt, hebben er recht op dat hun persoonlijke levenssfeer wordt beschermd. Zij moeten ervan kunnen uitgaan dat die gegevens niet in handen komen van anderen die daar niets mee te maken hebben. Dat geldt ook als de gegevens niet door de gemeente zelf worden verwerkt maar door andere in opdracht van de gemeente.

Haarlem moet zich voorbereiden op nieuwe wetgeving

De huidige Wet bescherming persoonsgegevens wordt vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG), die in werking treedt op 25 mei 2018. Die stelt nieuwe regels, met name op het gebied van handhaving en transparantie. Zo wordt de maximale boete verhoogd tot tien miljoen euro, worden hogere eisen gesteld aan transparantie en wordt het verplicht vast te leggen wat het privacybeleid is, hoe gegevens worden verwerkt en beschermd. Ook zullen alle overheden een Functionaris

Gegevensbescherming moeten benoemen. In 2017 bereidt Haarlem zich voor om klaar te zijn op het moment dat de AVG in werking treedt.

Extra capaciteit is nu nodig

Om op tijd voorbereid te zijn op de nieuwe regels, is het nodig zo snel mogelijk extra capaciteit te werven. Concrete voorbereidingen die getroffen moeten worden zijn:

- Alle processen waarin persoonsgegevens worden verwerkt moeten worden benoemd en beschreven, met daarbij
- het doel van de verwerking, de grondslag daarvoor,
- hoe geborgd is dat alleen de noodzakelijke gegevens worden verwerkt,
- hoe lang ze worden bewaard,
- wie verantwoordelijk is
- wie toegang heeft
- met wie ze worden gedeeld,
- welke bewerkersovereenkomsten zijn gesloten.

Waar dat nog niet gebeurd is, zullen alsnog bewerkersovereenkomsten moeten worden gesloten (overeenkomsten met organisaties die in opdracht van de gemeente gegevens bewerken, om afspraken te maken over welke gegevens ze verwerken, wie eigenaar is, wie waarvoor verantwoordelijk is e.d.).

Er moet worden bepaald voor welke processen waar dat nog niet gebeurt moet worden bijgehouden wie de gegevens raadpleegt en steekproeven moeten worden georganiseerd om te controleren of dit volgens de regels gebeurt.

De nota moet worden vertaald in een concreet normenkader, dat handvatten geeft voor de organisatie en dat het mogelijk maakt audits te houden. Vooralsnog wordt hiervoor een bestaand kader gebruikt dat door het Centrum Informatiebeveiliging en Privacy is geschreven. Dit moet worden geactualiseerd en waar nodig toegespitst op de Haarlemse situatie.

Voor nieuwe werkprocessen zullen deze punten direct bij het inrichten goed moeten worden georganiseerd.

Burgers hebben recht op inzage in welke persoonsgegevens de gemeente van het verwerkt en met wie ze worden gedeeld. Om op zo'n vraag te kunnen antwoorden is een goed overzicht nodig en een duidelijk proces. Ook dat vraagt de nodige voorbereidingen.

Op verschillende manieren zal aandacht worden gevraagd voor het belang van privacy en wat dat betekent voor ieders werk om het bewustzijn hiervan te verhogen. Waar nodig worden opleidingen aangeboden.

Het college wil zich op tijd voorbereiden en niet pas actie ondernemen als de verordening in werking treedt. De nieuwe regels zijn immers al vastgesteld, ze treden pas in 2018 in werking juist om iedereen de gelegenheid te bieden op tijd de juiste maatregelen te treffen.

De huidige capaciteit volstaat niet en het lukt niet op tijd aan al deze eisen te voldoen als een extra kracht pas na vaststelling van de Kadernota 2017 kan worden geworven. Het college stelt daarom voor een nieuwe voltijds functie Privacyadviseur in te stellen. Deze adviseur zal in samenwerking met de huidige strategisch adviseur privacy (functie in deeltijd) het bestuur en de organisatie adviseren. Het gaat om onontkoombare extra capaciteit die op dit moment niet is begroot. Het college stelt daarom voor de structurele kosten van € 85.000,- te dekken uit de algemene middelen.

5. Kanttekeningen

Om privacy goed te beschermen is een goede informatiebeveiliging nodig. Haarlem heeft op dit gebied al de nodige stappen gezet. Er is een Chief Information Security Officer, een algemeen Information Security Officer en een Security Officer voor het sociaal domein. Er is de afgelopen tijd veel aandacht besteed aan versterking van het bewustzijn van de ambtelijke organisatie. Voluit invoeren van het principe van Role Based Access zal dit versterken.

6. Uitvoering

Om het beleid verder in te vullen en praktisch te vertalen wordt vooruitlopend op de verplichting onder de Europese verordening een privacyadviseur aangesteld. Deze zal samen met de strategisch privacyadviseur het interne privacynetwerk dat nu bestaat verder uitbouwen en verstevigen, om de kennis en het bewustzijn in de ambtelijke organisatie te versterken. Het gaat om een tactische vertaling en uitvoering van het privacybeleid. Het jaar 2017 is dan een jaar van transitie; voor 2018 wordt gezien waar en hoe precies de formele functie van Functionaris Gegevensbescherming in de zin van de Europese verordening wordt belegd.

Onderdeel van de Privacynota is een praktisch normenkader (bijlage 2), ontwikkeld door een samenwerkingsverband van overheden. Dit geeft duidelijke handvatten voor de ambtelijke organisatie en maakt het ook mogelijk audits te houden op het gebied van privacy, zoals ook genoemd in de motie Big data en privacy een ongelukkig huwelijk (motie 15, 30 juni 2016). Het kader is nu nog gebaseerd op de huidige Wet bescherming persoonsgegevens maar wordt aangepast aan de nieuwe regels en waar nodig aangepast aan de Haarlemse situatie.

7. Bijlagen

1. Nota Privacybeleid Haarlem
2. CIP-Privacybaseline

Het college van burgemeester en wethouders,

de secretaris

de burgemeester

8. Raadsbesluit

De raad der gemeente Haarlem,

Gelezen het voorstel van het college van burgemeester en wethouders

Besluit:

1. De Nota Privacybeleid Haarlem vast te stellen;
2. In te stemmen met de volgende uitgangspunten:
 - *Werk met het minimum aan persoonsgegevens*
Als het nodig is of verplicht om persoonsgegevens te verwerken, gebeurt dat met het minimum dat nodig is.
 - *Maximale transparantie*
Het principe van maximale transparantie betekent op het gebied van privacy dat gedocumenteerd wordt waar welke persoonsgegevens worden verwerkt en met welk doel.
 - *Privacy by design*
Waar nieuwe werkprocessen worden ingericht worden die direct zo ontworpen dat de privacy is gewaarborgd.
 - *Role based access*
Toegang tot persoonsgegevens krijgen medewerkers alleen als dat voor hun taak noodzakelijk is. Autorisaties worden actueel gehouden en het gebruik van gegevens wordt steekproefsgewijs gecontroleerd.
 - *Inzagerecht*
Burgers kunnen opvragen welke gegevens de gemeente over hem of haar verwerkt;
 - Met ingang van 1 februari 2017 de formatie van de afdeling Strategie en Beleidscoördinatie uit te breiden met 1 fte voor de functie Privacyadviseur, in schaal 11A en de jaarlijkse lasten ad € 85.000,- te dekken uit de algemene middelen.

Gedaan in de vergadering van (wordt ingevuld door de griffie)

De griffier

De voorzitter