GEMEENTE HOORN

GEMEENTEBLAD

Officiële uitgave van de gemeente Hoorn

Nr. 39136

13 februari 2020

Vaststellen privacybeleid

Zaaknummer: 1720875

gelezen het voorstel van het college van Burgemeester en Wethouders d.d.

betreft: Vaststellen privacybeleid

De Raad van de gemeente Hoorn besluit:
het privacybeleid vast te stellen, waarvan de belangrijkste elementen zijn:

a. een duidelijke visie die aansluit bij de ICT-visie;
b. de randvoorwaarden en uitgangspunten bij een rechtmatige, behoorlijke en transparante omgang met persoonsgegevens;
c. een beschrijving van rollen met taken en verantwoordelijkheden binnen de privacy-organisatie;
d. de privacy-instrumenten (maatregelen) die de gemeente minimaal toepast en bijdragen aan een zorgvuldige en veilige omgang met persoonsgegevens.

Hoorn, 12 november 2019

de griffier, de voorzitter,

PRIVACYBELEID Gemeente Hoorn

1 Inleiding

Dit privacybeleid is richtinggevend en kaderstellend. Het vormt, samen met de documenten op tactisch en operationeel niveau, het fundament onder een betrouwbare verwerking van persoonsgegevens.

1.1 Wat is privacy?

Privacy is een grondrecht. Het grondrecht houdt in dat iedere persoon het recht heeft op 'de eerbiediging van de persoonlijke levenssfeer'. Daaronder vallen het eigen lichaam, huis, gezin, communicatie en persoonsgegevens. Het wordt ook wel het recht 'om met rust te worden gelaten' genoemd.

1.2 Visie

De gemeente hecht veel waarde aan een zorgvuldige verwerking van informatie, zeker als het persoonsgegevens betreft. De komende jaren maken we een volgende stap in het volwassenheidsniveau op het gebied van een zorgvuldige en veilige omgang met persoonsgegevens. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Onze visie

We digitaliseren onze dienstverlening en ons werk, organiseren data gedreven en moderniseren onze informatievoorziening. Door deze digitalisering is de bescherming van persoonsgegevens van steeds groter belang.

We mengen ons niet onnodig in het persoonlijk leven van personen. Waar persoonsgegevens nodig zijn, zorgen we voor een zorgvuldige en veilige omgang met persoonsgegevens. Personen informeren we hier actief over. Ze hebben zeggenschap over hun persoonsgegevens en zo gemakkelijk mogelijk toegang tot hun persoonsgegevens.

Vaststellen privacybeleid

Het privacybeleid wordt jaarlijks geëvalueerd en indien nodig geactualiseerd. Over de evaluatie wordt gerapporteerd in het jaarverslag van de functionaris gegevensbescherming (zie partagraaf 4.8).

1.4 (Juridisch) kader

Het 'recht op de eerbiediging van de persoonlijke levenssfeer', waaronder de bescherming van persoonsgegevens is geregeld in:

- Europees Verdrag voor de Rechten van de Mensen (artikel 8)
- Internationaal Verdrag burgerrechten en politieke rechten (artikel 17)
- Handvest van de grondrechten van de Europese Unie (artikel 8)
- Verdrag tot bescherming van personen met betrekking tot geautomatiseerde verwerking van persoonsgegevens
- Verdrag betreffende de werking van de Europese Unie (artikel 16)
- Internationaal Kinderrechtenverdrag (IVRK) (artikel 16)
- Grondwet (artikel 10)

In de grondwet en verdragen is ook bepaald dat er wetgeving nodig is, die regels stelt voor het verwerken van persoonsgegevens. Binnen de Europese Unie zijn deze regels gesteld in de Algemene Verordening Gegevensbescherming (AVG). Waar de AVG ruimte laat voor nationale keuzes, zijn deze ingevuld in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

In specifieke regelgeving is ook invulling gegeven aan de bescherming van persoonsgegevens, zoals:

- Wet maatschappelijke ondersteuning
- Jeugdwet
- Wet basisregistratie personen
- Archiefwet

Informatiebeveiliging is een randvoorwaarde voor een zorgvuldige en veilige verwerking van persoonsgegevens. In het Informatiebeveiligingsbeleid van gemeente Hoorn zijn maatregelen opgenomen om gegevens te beschermen.

2 Privacybeleid

2.1 Doel
Persoonsgegevens zijn nodig voor onze dienstverlening en het uitvoeren van onze wettelijke taken. Doel van dit privacybeleid is het beschrijven van kaders voor een zorgvuldige en veilige omgang met persoonsgegevens. Dit beleid geeft richting voor verdere invulling op tactisch en operationeel niveau.

2.2 Scope
Het privacybeleid is van toepassing op alle:
- taken en processen waarbinnen persoonsgegevens worden verwerkt,
- informatiesystemen waarin persoonsgegevens worden verwerkt,
- locaties, ruimten en apparatuur die worden gebruikt waar(op) persoonsgegevens worden verwerkt,
- opdrachten, contracten of samenwerkingen met (keten)partners.

Het heeft betrekking op de burgemeester, gemeenteraad, het college van burgemeester en wethouders (hierna college), alle medewerkers (intern, extern, vast en tijdelijk), inwoners, gasten, bezoekers en externe relaties.

2.3 Reikwijdte en afbakening
De (Uitvoeringswet) Algemene Verordening Gegevensbescherming geven regels voor de verwerking van persoonsgegevens. Dit privacybeleid heeft daarom alleen betrekking op de verwerking van persoonsgegevens en niet op het ruimere begrip ‘privacy’.

2.4 Randvoorwaarden en uitgangspunten
Iedereen werkzaam binnen en voor de gemeente is verantwoordelijk voor een zorgvuldige en veilige omgang met persoonsgegevens. De AVG noemt dit ‘rechtmatig, behoorlijk en transparant[1].
De uitgangspunten hierbij zijn:
- Persoonsgegevens worden alleen verwerkt als er een grondslag is.
- Persoonsgegevens worden alleen voor een gerechtvaardigd, duidelijk en concreet omschreven doel verwerkt.
- Er worden niet meer persoonsgegevens verwerkt dan voor dit doel noodzakelijk is.
- Persoonsgegevens die voor een bepaald doel zijn verkregen, worden niet voor een ander (niet verenigbaar) doel gebruikt.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor dit doel.
- Bijzondere persoonsgegevens worden niet verwerkt, tenzij hier een wettelijke uitzondering en een grondslag voor is.
- Persoonsgegevens zijn juist en actueel.
- Persoonsgegevens zijn goed beveiligd.
- Personen (‘betrokkenen’ in de AVG) worden geïnformeerd over de verwerking van hun gegevens en de mogelijkheid om hun rechten uit te oefenen.
- Datalekken worden intern en indien nodig bij de Autoriteit Persoonsgegevens (landelijk toezichthouder) gemeld.
- Personen hebben de mogelijkheid om hun rechten uit te oefenen (recht op inzage, correctie, verwijdering, bezwaar en verzet, beperking en overdraagbaarheid).
- Het is aantoonbaar dat aan deze uitgangspunten is voldaan.

[1] Artikel 5 AVG

3 De privacy-organisatie
In dit hoofdstuk zijn de rollen met taken en verantwoordelijkheden binnen de privacy-organisatie beschreven.

3.1 Bestuursorganen
Betrokkenheid van bestuurders is essentieel. Het laat zien dat de gemeente een zorgvuldige en veilige omgang met persoonsgegevens serieus neemt.

Het verantwoordelijke bestuursorgaan (burgemeester, college of gemeenteraad) is 'verwerkingsverantwoordelijke'[2] en daarmee eindverantwoordelijk voor de borging van een zorgvuldige en veilige omgang met persoonsgegevens.

Welk bestuursorgaan verantwoordelijk is, hangt af van de taak of het proces. Bijvoorbeeld openbare orde en veiligheid taken vallen onder de burgemeester, de WMO-taken onder het college en het besluitvormingsproces van de gemeenteraad onder de gemeenteraad. Waar we het in dit beleid hebben over 'de gemeente' wordt het verantwoordelijke bestuursorgaan bedoeld.

De bestuursorganen stellen de kaders op basis van wet- en regelgeving en geldende normen. De gemeenteraad heeft een controlerende taak ten opzichte van het college en de burgemeester als verantwoordelijk bestuursorgaan.

---

[2] Artikel 4.7 AVG

3.2 De directie

De directie is verantwoordelijk voor een zorgvuldige en veilige omgang met persoonsgegevens in de organisatie. De directie:

- stuurt op een zorgvuldige en veilige omgang met persoonsgegevens.
- zorgt dat teammanagers en proceseigenaren zich hierover verantwoorden.
- zorgt dat de functionaris gegevensbescherming naar behoren en tijdig wordt betrokken bij risicovolle aangelegenheden die verband houden met persoonsgegevens.
- zorgt dat de verantwoordelijke portefeuillehouders binnen het college waar nodig worden geïnformeerd over de omgang met persoonsgegevens.
- zorgt dat het college om kennisname of besluitvorming wordt gevraagd waar nodig en zich kan verantwoorden aan de gemeenteraad.
- zorgt voor kaderstelling op tactisch niveau.

3.3 Functionaris gegevensbescherming

De gemeente is verplicht een functionaris gegevensbescherming[3] aan te wijzen. De functionaris gegevensbescherming:

- ondersteunt de organisatie door intern toezicht te houden op een zorgvuldige en veilige omgang met persoonsgegevens.
- geeft gevraagd en ongevraagd advies.
- wordt betrokken bij alle aangelegenheden die verband houden met een zorgvuldige en veilige omgang met persoonsgegevens.
- is direct benaderbaar voor personen (betrokkenen) voor alles wat verband houdt met hun persoonsgegevens.
- rapporteert rechtstreeks aan het verantwoordelijke bestuursorgaan.

___

[3] Artikel 37 t/m 39 AVG

3.4 Teammanager

Een zorgvuldige en veilige omgang met persoonsgegevens binnen een bedrijfsonderdeel valt onder de verantwoordelijkheid van een teammanager. Een teammanager kan deze verantwoordelijkheid niet delegeren, uitvoerende werkzaamheden wel. Hiervoor kan hij een privacymedewerker aanwijzen (zie paragraaf 3.6).

De teammanager:

- draagt het belang van een zorgvuldige en veilige omgang met persoonsgegevens uit.
- ziet toe op een een zorgvuldige en veilige omgang met persoonsgegevens.
- zorgt dat er als aanvulling op dit privacybeleid, indien nodig, een specifiek privacybeleid en uitwerkingen op tactisch en operationeel niveau worden vastgesteld.
- zorgt dat de functionaris gegevensbescherming naar behoren en tijdig wordt betrokken bij alles wat verband houdt met de omgang met persoonsgegevens.
- zorgt dat datalekken worden gemeld volgens de interne procedure.
- zorgt voor voldoende bewustzijn en kennis bij medewerkers om zorgvuldig en veilig met persoonsgegevens om te kunnen gaan.

- rapporteert aan de directie over compliance aan wet- en regelgeving op het gebied van persoonsgegevens.

3.5 Proceseigenaar

De proceseigenaar is verantwoordelijk voor een zorgvuldige en veilige omgang met persoonsgegevens binnen een proces of informatiesysteem. Alle processen en informatiesystemen hebben een proceseigenaar. Een teammanager kan ook de rol van proceseigenaar hebben.

De proceseigenaar:
- zorgt voor een zorgvuldige en veilige omgang met persoonsgegevens. Dat betekent dat de proceseigenaar in ieder geval zorgt voor het toepassen van de privacy-instrumenten die zijn uitgewerkt in hoofdstuk 4.
- zorgt dat er regelmatig controles worden uitgevoerd om vast te stellen dat er volgens wet- en regelgeving wordt omgegaan met persoonsgegevens.
- rapporteert aan de teammanager over compliance aan wet- en regelgeving op het gebied van persoonsgegevens.

3.6 Privacymedewerker

Elk team kan een privacymedewerker aanwijzen. Een privacymedewerker:
- adviseert en ondersteunt de teammanager, proceseigenaar en teamleden bij een zorgvuldige en veilige omgang met persoonsgegevens.
- ondersteunt de teamleden bij het toepassen van de privacy-instrumenten die zijn uitgewerkt in hoofdstuk 4.

3.7 Ondersteuning en advies

Naast de privacymedewerkers zijn er diverse functies in de organisatie die bijdragen aan een zorgvuldige en veilige omgang met persoonsgegevens. Denk hierbij aan de functionaris informatiebeveiliging, inkoop-, juridische-, informatieadviseurs, programmamanagers, projectleiders, applicatiebeheerders en archiefmedewerkers.

3.8 De medewerker

Elke medewerker heeft een eigen verantwoordelijkheid voor een zorgvuldige en veilige omgang met persoonsgegevens.

Medewerkers:
- zijn voldoende op de hoogte van en houden zich aan wet- en regelgeving.
- houden zich aan de uitgangspunten genoemd in paragraaf 2.4.
- houden zich aan de afgesproken beveiligingsmaatregelen.

4 Privacy-instrumenten

De AVG vereist dat persoonsgegevens rechtmatig, behoorlijk en transparant worden verwerkt en dat dit aantoonbaar is. Daarom past de gemeente in ieder geval de in dit hoofdstuk uitgewerkte wettelijk verplichte privacy-instrumenten toe.

4.1 Register van verwerkingsactiviteiten

De gemeente houdt een register bij met alle verwerkingen van persoonsgegevens. Het register voldoet aan de wettelijke verplichtingen[4]. Onder andere de doeleinden van de verwerkingen, categorieën van betrokkenen en persoonsgegevens, derden ontvangers, bewaartermijn en beveiligingsmaatregelen zijn hierin opgenomen.

4.2 Gegegevensbeschermingseffectbeoordeling

De gemeente voert gegevensbeschermingseffectbeoordelingen[5] uit als de omgang met persoonsgegevens een hoog risico kan opleveren voor de personen van wie de gegevens zijn. Deze beoordeling geeft inzicht in de risico's en maatregelen die nodig zijn om deze risico's af te dekken. Het

wordt ook wel een Data Protection Impact Assesment (DPIA) genoemd. Elke DPIA wordt voor advies voorgelegd aan de functionaris gegevensbescherming.

4.3 Gegevensbescherming door ontwerp

Gegevensbescherming door ontwerp[6] wordt ook wel privacy by design genoemd. De gemeente past privacy by (re)design toe op nieuwe en bestaande verwerkingen van persoonsgegevens en bijbehorende systemen. Dat betekent dat vooraf rekening wordt gehouden met de bescherming van persoonsgegevens en de vereisten uit de AVG. Er wordt gezorgd voor verstandig en minimaal gebruik van gegevens en een passende bescherming.

---

[4] Artikel 30 AVG

[5] Artikel 35 AVG

[6] Artikel 25 AVG

4.4 Afspraken externe partijen

De gemeente maakt schriftelijk privacy-afspraken met externe partijen waarmee persoonsgegevens worden uitgewisseld. Externe partijen zijn onder te verdelen in 3 categorieen:

- De externe partij heeft een eigen verwerkingsverantwoordelijkheid[7] wat betreft de omgang met persoonsgegevens. Deze verantwoordelijkheid wordt vastgelegd in de hoofdovereenkomst. Ook worden maatregelen vastgelegd en getroffen die zorgen voor een veilige uitwisseling van de gegevens.
- Gemeente en de externe partij hebben een gezamenlijke verantwoordelijkheid[8]. Partijen bepalen samen 'het doel en de middelen' van de verwerking van de persoonsgegevens. Afspraken over deze gezamenlijke verantwoordelijkheid worden vastgelegd in een overeenkomst.
- De externe partij is een 'verwerker'[9] . De gemeente bepaalt het 'het doel en de middelen' van de verwerking van de persoonsgegevens. De externe partij voert de opdracht uit volgens de voorwaarden van de gemeente. Privacyafspraken worden vastgelegd in een verwerkersovereenkomst, volgens het verplichtte model van de VNG.

4.5 Inbreuk in verband met persoonsgegevens

De gemeente heeft een procedure voor het melden van inbreuken in verband met persoonsgegevens[10] , ook wel datalekken genoemd. Bij een datalek zijn persoonsgegevens mogelijk gezien of gebruikt door personen die dit niet nodig hebben of deze zijn onterecht (niet) vernietigd of verloren gegaan. Elke medewerker is verantwoordelijk om datalekken direct te melden volgens de procedure.

De functionaris gegevensbescherming, functionaris informatiebeveiliging of privacymedewerker registreert de datalekken in een register en zorgt voor melding bij de landelijk toezichthouder, indien nodig. In de cyclusdocumenten wordt inzicht gegeven in het aantal datalekken.

---

[7] Artikel 4.7 en 24 AVG

[8] Artikel 26 AVG

[9] Artikel 28 AVG

[10] Artikel 33 en 34 AVG

4.6 Informatieplicht

Voor personen moet inzichtelijk zijn in hoeverre en op welke manier hun persoonsgegevens worden verwerkt. Dit is het 'transparantiebeginsel'[11]. De gemeente informeert personen daarom in duidelijke en eenvoudige taal over de omgang met hun persoonsgegevens. Ze worden geïnformeerd over:

- de reden en de grondslag van de verwerking van persoonsgegevens.
- welke persoonsgegevens worden verwerkt.
- hoe lang persoonsgegevens worden bewaard.
- aan welke externe partijen ze mogelijk worden/zijn verstrekt.
- de rechten die de persoon heeft en hoe hier gebruik van te maken.
- wie de verwerkingsverantwoordelijke is en hoe deze te bereiken is.
- wie de functionaris gegevensbescherming is en hoe deze te bereiken is.

Deze informatie is op de website van de gemeente te vinden en waar nodig in aanvullende informatie.

4.7 Rechten van betrokkenen

Personen hebben recht op inzage, rectificatie, verwijdering, beperking, overdraagbaarheid van gegevens, bezwaar en om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming[12].

Om gebruik te maken van deze rechten kunnen personen een verzoek indienen via de website van de gemeente. Binnen vier weken laat de gemeente weten wat er met het verzoek gaat gebeuren.

Als een persoon niet tevreden is over hoe de gemeente met persoonsgegevens omgaat of hoe het verzoek is afgehandeld, kan de persoon bezwaar maken of een klacht in te dienen bij de gemeente. Ook kan de persoon een klacht indienen bij de Autoriteit Persoonsgegevens.

[11] Artikelen 5, 12 t/m 14 AVG

[12] Artikelen 15 t/m 22 AVG

4.8 Verantwoording

In de cylcusdocumenten legt het college verantwoording af aan de gemeenteraad over de naleving van de AVG en het privacybeleid.

De functionaris gegevensbescherming brengt jaarlijks verslag uit aan de bestuursorganen over de ontwikkelingen en aandachtspunten bij de omgang met persoonsgegevens. Dit jaarverslag van de functionaris gegevensbescherming is onderdeel van de jaarstukken.