BELEID PERSOONSGEGEVENS
Gemeente Hoorn

Januari 2022
Versie 3

GEMEENTE HOORN

Inhoudsopgave

1 Inleiding 3
1.1 Waar gaat dit beleid over? 3
1.2 Doel 3
1.3 Kaders 3
1.4 Evaluatie 4

2 Uitgangspunten 5
2.1 Ons uitgangspunt 5

3 Rollen, verantwoordelijkheden 6
3.1 Gemeenteraad, college, burgemeester 6
3.2 Directie (algemeen directeur en concernmanagers) 6
3.3 Ondernemingsraad 6
3.4 Functionaris gegevensbescherming 6
3.5 Teammanager 7
3.6 Adviseur persoonsgegevens 7
3.7 Medewerker digitale veiligheid 7
3.8 Ondersteuning en advies 7
3.9 De medewerker 7

4 Instrumenten 8
4.1 Register van verwerkingsactiviteiten 8
4.2 Gegegevensbeschermingseffectbeoordeling 8
4.3 Gegevensbescherming door ontwerp en standaardinstellingen 8
4.4 Afspraken externe partijen 8
4.5 Datalekken 8
4.6 Rechten van betrokkenen 9
4.7 Audit en controles 9
4.8 Verantwoording 9

1 Inleiding

1.1 Waar gaat dit beleid over?

Iedereen heeft 'recht op de eerbiediging van de persoonlijke levenssfeer'[1]. Dit is een grondrecht. Hieronder valt het huis, briefwisseling, communicatie, innerlijke leven, lichamelijke integriteit, niet te worden bespied of afgeluisterd en het recht op zorgvuldige behandeling van persoonsgegevens. Dit beleid heeft alleen betrekking op een zorgvuldige behandeling van persoonsgegevens.

Persoonsgegevens die nodig zijn voor voorkoming en opsporing van strafbare feiten door buitengewoon opsporingsambtenaren, worden politiegegevens genoemd. Waar in dit beleid 'persoonsgegevens' staat, worden ook politiegegevens bedoeld.

Waar in dit beleid 'de gemeente' staat wordt de verwerkingsverantwoordelijke bedoeld (zie paragraaf 3.1).

Het beleid is van toepassing op:

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

[1] Art. 10 grondwet

1.2 Doel

Persoonsgegevens zijn nodig voor onze dienstverlening en het uitvoeren van onze wettelijke taken. 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 behandeling van persoonsgegevens.

Doel van dit beleid is het beschrijven van kaders voor een zorgvuldige behandeling van persoonsgegevens. Het geeft inwoners inzicht in hoe de gemeente omgaat met hun persoonsgegevens. Intern geeft het richting voor verdere invulling op tactisch en operationeel niveau.

1.3 Kaders

Het 'recht op de eerbiediging van de persoonlijke levenssfeer', waaronder een zorgvuldige behandeling 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).

De verwerking van persoonsgegevens voor het voorkomen en opsporen van strafbare feiten, valt onder de Wet politiegegevens (Wpg). Aanvullend op de Wpg zijn voor politiegegevens van toepassing:

- Besluit politiegegevens (Bpg)
- Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpgboa)
- Regeling periodieke audit politiegegevens

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

- Wet maatschappelijke ondersteuning
- Jeugdwet
- Wet basisregistratie personen
- Archiefwet
- Wet op de Ondernemingsraden

Informatiebeveiliging is een randvoorwaarde voor een zorgvuldige behandeling van persoonsgegevens. Voor de gehele overheid is een normenkader voor informatiebeveiliging afgesproken waar elke organisatie aan moet voldoen. Dit is de Baseline Informatiebeveiliging Overheid (BIO). Er is een Informatiebeveiligingsbeleid van gemeente Hoorn waarin de rollen, verantwoordelijkheden en maatregelen zijn opgenomen om gegevens te beschermen.

Waar in dit beleid ‘kaders’ staat, worden deze wet- en regelgeving, normen en dit beleid bedoeld.

1.4 Evaluatie

Dit beleid wordt jaarlijks geëvalueerd en indien nodig geactualiseerd.

2 Uitgangspunten

Iedereen werkzaam binnen en voor de gemeente is verantwoordelijk voor een zorgvuldige behandeling van persoonsgegevens, conform alle kaders.

2.1 Ons uitgangspunt

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

Dit betekent dat de gemeente:

- persoonsgegevens alleen verwerkt als er een grondslag is.
- persoonsgegevens alleen voor een gerechtvaardigd, duidelijk en concreet omschreven doel verwerkt.
- niet meer persoonsgegevens verwerkt dan voor dit doel noodzakelijk is.
- persoonsgegevens die voor een bepaald doel zijn verkregen, niet voor een ander (niet verenigbaar) doel gebruikt.
- persoonsgegevens niet langer bewaart, dan noodzakelijk is voor dit doel.
- bijzondere persoonsgegevens niet verwerkt, tenzij hier een wettelijke uitzondering en een grondslag voor is.
- zorgt dat persoonsgegevens juist en actueel zijn.
- zorgt dat persoonsgegevens goed beveiligd zijn.
- personen (‘betrokkenen’) informeert over de verwerking van hun gegevens en de mogelijkheid om hun rechten uit te oefenen.
- zorgt voor het toepassen van de instrumenten in hoofdstuk 4.
- zorgt dat aantoonbaar aan deze uitgangspunten is voldaan.

3 Rollen, verantwoordelijkheden

In dit hoofdstuk zijn de rollen met taken en verantwoordelijkheden voor een zorgvuldige behandeling van persoonsgegevens beschreven.

3.1 Gemeenteraad, college, burgemeester

De gemeenteraad, college en burgemeester:

- zijn als verantwoordelijk bestuursorgaan 'verwerkingsverantwoordelijke'[2] en daarmee eindverantwoordelijk voor een zorgvuldige behandeling van persoonsgegevens op grond van de AVG. Voor politiegegevens (Wpg) is de werkgever (het college) van de buitengewoon opsporingsambtenaren verwerkingsverantwoordelijke.
- dragen het belang uit van van een zorgvuldige behandeling van persoonsgegevens.
- stellen kaders, zoals dit beleid, vast op strategisch niveau.
- zorgen dat ze voldoende zijn geinformeerd over het naleven van de kaders en sturen hierop, waar nodig.

De gemeenteraad heeft een controlerende taak ten opzichte van het college en de burgemeester als verwerkingsverantwoordelijke. Het college en de burgemeester leggen verantwoording af aan de gemeenteraad in de cyclusdocyumenten.

3.2 Directie (algemeen directeur en concernmanagers)

De directie is verantwoordelijk voor een zorgvuldige behandeling van persoonsgegevens in de ambtelijke organisatie. De directie:

- draagt het belang van een zorgvuldige behandeling van persoonsgegevens uit en stuurt hierop.
- zorgt dat teammanagers zich hierover verantwoorden.
- zorgt dat het college, burgemeester en/of de verantwoordelijke portefeuillehouders binnen het college, worden geïnformeerd over het naleven van de kaders, waar nodig om besluitvorming worden gevraagd en zich kunnen verantwoorden aan de gemeenteraad.
- zorgt dat de functionaris gegevensbescherming naar behoren en tijdig wordt betrokken bij risicovolle verwerkingen van persoonsgegevens.
- zorgt voor kaderstelling op tactisch niveau.

3.3 Ondernemingsraad

De ondernemingsraad (OR) heeft instemmingsrecht op ontwikkelingen met risico's voor werknemers waar het gaat om hun persoonsgegevens[3]. Bijvoorbeeld controles op prestatie of gedrag. De OR heeft adviesrecht over voorgenomen besluiten tot invoering of wijziging van een belangrijke technologische voorziening[4].

3.4 Functionaris gegevensbescherming

De verwerkingsverantwoordelijken zijn verplicht een functionaris gegevensbescherming[5] aan te wijzen. Deze functionaris[6]:

- voert autonoom en onafhankelijk werkzaamheden uit.
- beschikt over voldoende ondersteuning en middelen.
- ziet toe opnaleving van de kaders.
- informeert en adviseert over de verplichtingen op het gebied van een zorgvuldige behandeling van persoonsgegevens.
- zorgt voor bewustwording en ontwikkeling van medewerkers binnen de gemeente met betrekking tot een zorgvuldige behandeling van persoonsgegevens.
- wordt betrokken bij (risicovolle) verwerkingen van persoonsgegevens.
- is direct benaderbaar voor personen over alles wat verband houdt met hun persoonsgegevens.
- werkt samen met en is contactpunt van de Autoriteit Persoonsgegevens.

[2] Artikel 4.7 AVG, 1f Wpg, 1c Bpgboa
[3] Artikel 27 lid 1k WOR
[4] Artikel 25 lid 1k WOR
[5] Artikel 37 tm 39 AVG, 36 Wpg
[6] De FG volgt de Handreiking positionering en taken van de FG (IBD)

- brengt jaarlijks verslag uit aan de verwerkingsverantwoordelijke over de ontwikkelingen en aandachtspunten op het gebied van persoonsgegevens.

3.5 Teammanager

Een zorgvuldige behandeling van persoonsgegevens binnen een bedrijfsonderdeel valt onder de verantwoordelijkheid van een teammanager.

De teammanager:

- draagt het belang van een zorgvuldige behandeling van persoonsgegevens uit en stuurt hierop.
- zorgt voor naleving van de uitgangspunten (hoofdstuk 2) en het toepassen van de instrumenten (hoofdstuk 4).
- zorgt dat er, als aanvulling op dit beleid en indien nodig, een specifiek beleid en uitwerkingen op tactisch en operationeel niveau worden vastgesteld.
- zorgt dat de functionaris gegevensbescherming naar behoren en tijdig wordt betrokken bij risicovolle verwerkingen van persoonsgegevens.
- zorgt voor bewustwording en kennis bij medewerkers om persoonsgegevens zorgvuldig te kunnen behandelen.
- verantwoord zich aan de directie over naleving van de kaders.

3.6 Adviseur persoonsgegevens

Een adviseur persoonsgegevens wordt ook wel een privacy-officer genoemd. Deze functionaris heeft een operationeel uitvoerende rol:

- evalueert dit beleid en actualiseert indien nodig.
- vertaalt dit beleid naar tactisch en operationeel niveau.
- adviseert en ondersteunt bij ingewikkelde en risicovolle vraagstukken en het toepassen van de instrumenten (hoofdstuk 4).
- bespreekt riscovolle ontwikkelingen en aandachtspunten met de functionaris gegevensbescherming en functionaris informatiebeveiliging.

[7] Artikel 9 Wpg

3.7 Medewerker digitale veiligheid

Elk team heeft een medewerker digitale veiligheid. Deze medewerker:

- adviseert en ondersteunt de teammanager en teamleden op het gebied van digitale veiligheid, waaronder een zorgvuldige behandeling van persoonsgegevens.
- ondersteunt het team met bij het toepassen van de instrumenten (hoofdstuk 4).
- stemt af met de functionaris gegevensbescherming, adviseur persoonsgegevens en functionaris informatiebeveiliging over ontwikkelingen binnen het team.

3.8 Ondersteuning en advies

Er zijn diverse functies die bijdragen aan een zorgvuldige behandeling van persoonsgegevens. Denk hierbij aan de functionaris informatiebeveiliging, coördinator informatiebeveiliging, bevoegd functionaris Wpg[7], inkoopadviseurs, juridische adviseurs, informatiemanagers, adviseurs interne beheersing, projectleiders, applicatiebeheerders en archiefmedewerkers.

3.9 De medewerker

Elke medewerker heeft een eigen verantwoordelijkheid voor een zorgvuldige behandeling van persoonsgegevens. Ze zorgen dat ze op de hoogte zijn van en houden zich aan de kaders en de afspraken over veilig werken.

4 Instrumenten

De gemeente past in ieder geval de in dit hoofdstuk uitgewerkte wettelijk verplichte instrumenten toe. Hierbij wordt een risico gebaseerde aanpak en prioritering gehanteerd.

4.1 Register van verwerkingsactiviteiten

De gemeente houdt een register bij met alle verwerkingen van persoonsgegevens. In dit register kunnen AVG en Wpg-verwerkingen worden uitgesplitst. Het register voldoet aan de wettelijke verplichtingen[8]. 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[9] uit als de behandeling van 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 en standaardinstellingen

Gegevensbescherming door ontwerp en standaard instellingen[10] worden ook wel privacy by design en privacy by default genoemd. Bij veranderingen en vernieuwingen wordt vanaf de inrichting rekening gehouden met een zorgvuldige behandeling persoonsgegevens volgens de kaders. Denk hierbij aan minimaal gebruik van persoonsgegevens en een passende bescherming. Standaardinstellingen zijn zo gekozen dat de dit maximaal wordt geborgd.

4.4 Afspraken externe partijen

De gemeente maakt schriftelijke afspraken over de voorwaarden en beveiliging, met externe partijen waarmee persoonsgegevens worden uitgewisseld.

Externe partijen zijn onder te verdelen in 3 categorieen:

- De externe partij heeft een eigen verwerkingsverantwoordelijkheid[11] wat betreft de behandeling van persoonsgegevens.
- Gemeente en de externe partij hebben een gezamenlijke verantwoordelijkheid[12]. Partijen bepalen samen 'het doel en de middelen' van de behandeling van de persoonsgegevens.
- De externe partij is een 'verwerker'[13]. De gemeente bepaalt 'het doel en de middelen' (voorwaarden) voor de behandeling van de persoonsgegevens door de externe partij.

4.5 Datalekken

De gemeente heeft een procedure voor het melden van een 'inbreuk in verband met persoonsgegevens'[14], ook wel datalek genoemd. Bij een datalek zijn persoonsgegevens mogelijk gezien of gebruikt door personen die dit niet nodig hebben of ze 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 adviseur persoonsgegevens registreert de datalekken in een register en zorgt voor melding bij de landelijk toezichthouder, indien nodig.

[8] Artikel 30 AVG en 31d Wpg
[9] Artikel 35 AVG en 4c Wpg
[10] Artikel 25 AVG en 4a en b Wpg
[11] Artikel 4.7 en 24 AVG
[12] Artikel 26 AVG en 20 Wpg
[13] Artikel 28 AVG en 6c Wpg
[14] Artikel 33 en 34 AVG en 33a Wpg

4.6 Rechten van betrokkenen[15]

Personen hebben rechten gekregen om controle te houden over hun persoonsgegevens. Denk aan het recht op informatie, inzage, aanpassing en verwijdering.

Om gebruik te maken van deze rechten kunnen personen een verzoek indienen. Binnen een maand reageert de gemeente op het verzoek.

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

Personen hebben recht op informatie. Daar kunnen ze een verzoek voor indienen. De gemeente heeft ook een actieve plicht om personen vooraf in duidelijke en eenvoudige taal te informeren. Dit doen we op websites van de gemeente en waar nodig in aanvullende informatie.

4.7 Audit en controles

De gemeente voert periodiek audits en controles uit om vast te stellen dat persoonsgegevens volgens de kaders zijn behandeld en beveiligd.

De Wet politiegegevens stelt verplicht dat er jaarlijks een interne audit en één keer in de vier jaar een externe audit wordt uitgevoerd[16].

4.8 Verantwoording

In de cylcusdocumenten legt het college verantwoording af aan de gemeenteraad over het naleven van de kaders op het gebied van persoonsgegevens.

De functionaris gegevensbescherming brengt jaarlijks verslag uit aan de verwerkingsverantwoordelijken over de ontwikkelingen en aandachtspunten op het gebied van persoonsgegevens.

[15] Artikel 12 tm 22 AVG en 24a tm 28 Wpg
[16] Artikel 33 Wpg en Regeling periodieke audit politiegegevens

Gemeente Hoorn
Nieuwe Steen 1
Postbus 603
1620 AR Hoorn
T 0229 25 22 00
www.hoorn.nl

GEMEENTE
HOORN