GEMEENTE HOORN

JAARRAPPORTAGE 2023

INFORMATIEBEVEILIGING & PERSOONSGEGEVENS

Aan: de gemeenteraad

Auteurs: Michèle van der Horst en Suzanne Pannemans

Inhoudsopgave

1 Inleiding

Vanuit onze rol als functionaris informatiebeveiliging en functionaris gegevensbescherming informeren wij de gemeenteraad jaarlijks over de stand van zaken, ontwikkelingen en aandachtspunten op het gebied van informatiebeveiliging en persoonsgegevens[1].

Om de rapportage leesbaar te houden is uitleg over onderwerpen te vinden in hoofdstuk 4 Vraag en Antwoord. Woorden die in de rapportage zijn onderstreept, zijn in hoofdstuk 4 uitgelegd. Door op het onderstreepte woord te klikken, gaat u direct naar de uitleg van dat onderwerp.

1.1 Wat is privacy?

Iedereen heeft 'recht op de eerbiediging van de persoonlijke levenssfeer'. Dit is een grondrecht[2]. Hieronder valt het huis, briefwisseling, communicatie, innerlijke leven, lichamelijke integriteit, niet te worden bespied of afgeluisterd en het recht op een zorgvuldige behandeling van persoonsgegevens.

In het beleid Persoonsgegevens[3] is als uitgangspunt opgenomen:
'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.'

Een zorgvuldige behandeling van persoonsgegevens is uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG). Dit is Europese wetgeving. In Nederland staan aanvullende voorwaarden in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). De (U)AVG is van toepassing op privaat- en bestuursrechtelijke verwerkingen van persoonsgegevens.

1.2 Wat is informatiebeveiliging?

Informatiebeveiliging is het treffen en onderhouden van maatregelen om de juiste beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen.

- Beschikbaarheid: het garanderen van de beschikbaarheid van informatie wanneer dat nodig is.
- Integriteit: de mate waarin informatie actueel, juist en betrouwbaar is.
- Vertrouwelijkheid: de mate waarin gegevens beschermd moeten worden tegen kennisname en mutatie door onbevoegden.

In het Informatiebeveiligingsbeleid van de gemeente Hoorn staat:
'We digitaliseren onze dienstverlening en ons werk, organiseren data gedreven en moderniseren onze informatievoorziening. Door deze digitalisering is de bescherming van gegevens en informatievoorziening van steeds groter belang. Inwoners moeten erop kunnen vertrouwen dat we zorgvuldig met gegevens omgaan en dat we deze veilig beheren.'

Voor de gehele overheid is een normenkader voor informatiebeveiliging afgesproken waar elke organisatie aan moet voldoen. Dit is de Baseline Informatiebeveiliging Overheid (BIO)[4]. De BIO is gebaseerd op de NEN-ISO 27001 en 27002. De AVG kent de verplichting tot het treffen van passende technische en organisatorische maatregelen[5]. De BIO voorziet in een groot deel van deze maatregelen.

---

1 Artikel 38.3 AVG, 36.4 Wpg en Functieprofielen IBD-VNG
2 Artikel 10 grondwet
3 Beleid persoonsgegevens gemeente Hoorn
4 Baseline Informatiebeveiliging Overheid
5 Artikel 32 AVG

2 Risico's

2.1 Risico's voor inwoners en ondernemers

Het onzorgvuldig omgaan met gegevens kan enorme gevolgen hebben voor inwoners en ondernemers. Denk aan reputatieschade, financiële schade en emotionele schade door digitale criminaliteit[6]. Het gevoel continu gevolgd te worden, uitsluiting, discriminatie en onjuiste besluitvorming zijn risico's, bijvoorbeeld door de inzet van technologie (zie ook paragraaf 2.4).

2.2 Risico's voor de gemeente

Risico's voor de gemeente kunnen groot zijn, bijvoorbeeld:

- Uitval van de dienstverlening en bedrijfsvoering.
- Incidenten (digitale criminaliteit, datalek) kunnen leiden tot hoge herstelkosten, reputatieschade en verlies van vertrouwen in de gemeente. Het kan ook impact hebben op medewerkers omdat ze hun werk niet of minder goed kunnen doen.
- Personen hebben recht op schadevergoeding[7] als er schade is omdat de gemeente verwijtbaar in strijd met de wet heeft gehandeld.
- De Autoriteit Persoonsgegevens kan sancties opleggen. De belangrijkste sancties zijn de boete[8], de last onder dwangsom, het verwerkingsverbod, de berisping en de waarschuwing.

2.3 Succesfactoren

Om de risico's te beheersen zijn er een aantal succesfactoren:

- De mens: kennis en bewustzijn bij medewerkers en een gevoel van veiligheid om incidenten te melden, zijn belangrijk. Risico's op onbedoeld onveilig of onrechtmatig omgaan met gegevens en het niet (tijdig) herkennen en melden van incidenten, worden hierdoor lager.
- Eigenaarschap bij het management: betrokken management die stuurt en voorbeeld gedrag vertoont, draagt bij aan informatiebeveiliging en privacy.
- De organisatie: specialistische kennis en vaardigheden zijn nodig om de organisatie te ondersteunen en adviseren.
- Techniek: veilige en goed werkende bedrijfsmiddelen, systemen en techniek zijn van groot belang voor continuïteit van de dienstverlening en bedrijfsvoering. Het verkleint het risico dat criminelen virussen, ransomware inzetten of kwetsbaarheden in systemen gebruiken om gegevens te beschadigen, stelen of gijzelen en losgeld eisen.
- Financiën: budget voor informatieveiligheid en privacy zorgt voor een structurele, cyclische aanpak en dat de organisatie het tempo van de digitale ontwikkelingen en risico's aan kan.
- Samenwerkingen en leveranciers: afspraken met samenwerkingspartners en leveranciers over informatieveiligheid en privacy en hierop controleren, zorgen dat gegevens ook bij deze organisaties beschermd zijn.

---

[6] 2,2 miljoen Nederlanders slachtoffer online criminaliteit in 2022 | CBS

[7] Artikel 82 AVG

[8] Boetebeleidsregels Autoriteit Persoonsgegevens 2023

3 Hoe staat de gemeenteraad ervoor?

In dit hoofdstuk leest u per onderwerp (vaak een wettelijke verplichting) de stand van zaken, verbeteringen en de aandachtspunten op het gebied van informatiebeveiliging en persoonsgegevens.

3.1 Beleid

De gemeente heeft de volgende beleidsdocumenten en regelingen vastgesteld op het gebied van informatiebeveiliging en persoonsgegevens:

- Informatiebeveiligingsbeleid (2019)
- Incidenten en responsebeleid (2019)
- Data-analysebeleid (2020)
- Dataclassificatiebeleid (2020)
- Personeelshandboek met onder andere de gedragscode, Verklaring Omtrent het Gedrag (VOG), regeling bedrijfsmiddelen en gebruik devices, internet en e-mail (2020)
- Digitaal toegangsbeleid (2021)
- Whatsapp richtlijn en bewaartips (2021)
- Beleid persoonsgegevens[9] (2022)
- Back-up en restorebeleid (2022)
- Tijdelijke richtlijn Chat GPT (2023)

De organisatie heeft het advies gekregen om een testbeleid, loggingbeleid en cookiebeleid op te stellen. Dit zorgt voor een afwegings- en handelingskader die de griffie en gemeenteraad volgen of op kunnen steunen.

3.2 Rollen en verantwoordelijkheden

De griffie heeft een medewerker Digitale veiligheid, die voldoende kennis en tijd heeft om deze rol te vervullen. De organisatie heeft verschillende functionarissen die de griffie kunnen adviseren en ondersteunen op informatiebeveiliging en persoonsgegevens.

3.3 Kennis en bewustzijn

Kennis en bewustzijn binnen de griffie is op orde. De griffie informeert raadsleden periodiek over dit onderwerp. Organisatie brede activiteiten en faciliteiten dragen bij aan het bewustzijn binnen de griffie:

- Er is een inwerkprogramma voor nieuwe medewerkers waar veilig werken en de behandeling van persoonsgegevens onderdeel van zijn. Zo is de digitale module ‘iBewustzijn Overheid’ van de VNG en het spelen van een escaperoom een verplicht onderdeel van het inwerkprogramma.
- Er is een wegwijzer (kennisbank) met uitleg voor medewerkers. Deze wordt regelmatig herzien en aangevuld. De onderwerpen in de wegwijzer sluiten grotendeels aan bij de onderwerpen in dit hoofdstuk.
- Oktober was de maand van Samen digitaal veilig, met interessante lezingen, berichten op intranet en informatie voor teams.
- Op verzoek wordt uitleg gegeven aan teams over veilig werken en persoonsgegevens.
- Inkoopadviseurs en informatiemanagers hebben een interne training gevolgd over verwerkingsverantwoordelijkheid en (verwerkers)overeenkomsten.
- Er is een Bewustwordingsplan Veilig werken 2023 en 2024 opgesteld door de functionarissen informatiebeveiliging, adviseur persoonsgegevens en functionaris gegevensbescherming.
- In 2023 werd ChatGPT snel geïntroduceerd en door veel mensen in gebruik genomen. Generatieve Artificial Intelligence zoals ChatGPT biedt veel voordelen, maar zorgt ook voor risico’s, uitdagingen én vragen. Daarom was er in 2023 een informatiebijeenkomst en is er een eerste Richtlijn ChatGPT gemaakt voor medewerkers.

[9] Artikel 24.2 AVG

3.4 Register van verwerkingsactiviteiten

Het register van verwerkingsactiviteiten van de gemeenteraad is juist en volledig.

3.5 Data Protection Impact Assessment (DPIA)

Er is geen DPIA op de camera's in de raadszaal uitgevoerd. Er is gekozen om deze DPIA's uit te stellen en uit te voeren op de nieuwe camera's in het nieuwe pand. Verder zijn er geen risicovolle verwerkingen van persoonsgegevens waar een DPIA voor nodig is.

3.6 Gegevensbescherming door ontwerp en standaardinstellingen

Er zijn geen veranderingen en vernieuwingen gestart in 2023 waar 'privacy by design' voor nodig was.

3.7 Afspraken met externe partijen

De griffie heeft afspraken gemaakt met externe partijen waar persoonsgegevens mee worden uitgewisseld (zie ook paragraaf 3.11). Er is voldoende aandacht vanuit de griffie voor het maken van de juiste afspraken. Waar nodig kan de griffie gebruik maken van de kennis van inkoopadviseurs en informatieadviseurs in de organisatie.

3.8 Rechten van betrokkenen

Op de website van de gemeente Hoorn staat een privacyverklaring met uitleg over de omgang met persoonsgegevens en rechten van betrokkenen. Er is een privacyverklaring Gemeenteraad opgesteld. Deze is nog niet geplaatst op de website van de gemeenteraad.

De griffie overlegt met personen over de openbaarheid van brieven en inspreeksessies (spreekrecht). Als raadsleden gegevens opvragen, bewaakt de griffie dat dit zorgvuldig volgens de AVG gebeurt.

In 2023 heeft de gemeenteraad geen verzoeken van personen ontvangen om gebruik te maken van hun rechten. Binnen de griffie is kennis en bewustzijn om verzoeken te herkennen en af te handelen. De griffie wordt ondersteund door organisatie brede kennisitems, procedures en handreikingen.

3.9 Datalekken

Kennis en bewustzijn is hoog binnen de griffie. Onder de verwerkingsverantwoordelijkheid van de gemeenteraad zijn er geen datalekken in 2023 gemeld. De griffie wordt ondersteund door organisatie brede De griffie wordt ondersteund door organisatie brede kennisitems, procedures en handreikingen.

3.10 Bewaren en vernietigen

Besluitvormingsdocumenten van de gemeenteraad worden vastgelegd in twee systemen. Hier is sprake van dubbele opslag. Er wordt onderzocht of het mogelijk is om een enkel systeem voor de besluitvormingsdocumenten te gebruiken en het andere systeem uit te faseren.

De griffie houdt elk jaar een opschoningsactie om meervoudige opslag en te lange bewaartermijnen in email en mappen te voorkomen.

3.11 Informatiebeveiliging

De griffie werkt binnen de werkomgeving van de gemeente Hoorn. De gemeenteraads- en commissieleden werken in een andere digitale werkomgeving. Dit is uitbesteed aan een andere externe ICT-dienstverlener dan de ambtelijke organisatie. Deze werkomgeving voldoet aan een algemeen geaccepteerde beveiligingsnorm, vergelijkbaar met de BIO. Hierover zijn schriftelijke afspraken gemaakt.

ICT-dienstverlening

2023 was het eerste jaar dat de ICT-dienstverlening werd verzorgd door de externe ICT-dienstverlener. Het goed neerzetten van de onderlinge samenwerking en het regievoeren op de contractuele afspraken, heeft veel tijd en inzet gevraagd van de organisatie. In 2023 voldeed de ICT-dienstverlener niet volledig aan de afgesproken plichten en kwaliteit. Hierdoor was er nog onvoldoende ruimte voor verbeteringen op het gebied van informatiebeveiliging.

Onveilige apps

Aan het begin van 2023 heeft de overheid besloten dat ambtenaren in dienst van de Rijksoverheid geen apps mogen installeren of gebruiken die afkomstig zijn van bedrijven uit landen met een offensief cyberprogramma gericht tegen Nederland en/of Nederlandse belangen. Dit besluit is genomen op advies van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Die heeft gewaarschuwd voor de verhoogde risico's van spionage die dergelijke software met zich meebrengt. De VNG heeft dit advies overgenomen. Dit betekent dat dit advies ook voor ons geldt. Het advies is ook om deze apps niet in te zetten als communicatiekanaal met inwoners. Voordat keuzes gemaakt kunnen worden over hoe we omgaan met het advies, is onderzoek nodig. Tot die tijd worden medewerkers geadviseerd om geen gebruik te maken van apps die afkomstig zijn van bedrijven uit landen met een offensief cyberprogramma gericht tegen Nederland en/of Nederlandse belangen.

4 Vraag en antwoord

Wat is een functionaris informatiebeveiliging?

Een functionaris informatiebeveiliging[10] treedt op als onafhankelijk strategisch adviseur voor het bestuur en het management. Deze functionaris houdt zich bezig met strategische beleids- en planvormig en strategische en tactische advisering op het gebied van informatiebeveiliging. Een functionaris informatiebeveiliging wordt ook wel Chief Information Security Officer (CISO) genoemd.

Wat is een functionaris gegevensbescherming?

Een functionaris gegevensbescherming[11] is onafhankelijk privacyadviseur en -toezichthouder binnen de organisatie. Het doel van deze functie is het bevorderen van de naleving van de kaders door middel van informeren, inspectie, waarheidsvinding, beoordeling en advisering. De aanwijzing, positie en taken zijn opgenomen in de wet[12].

Waarom is beleid belangrijk?

Beleid zorgt voor transparantie richting inwoners en intern geeft het richting voor verdere invulling op tactisch en operationeel niveau.

Welke rollen en verantwoordelijkheden zijn er?

Een verwerkingsverantwoordelijke[13] is eindverantwoordelijk voor een zorgvuldige behandeling van persoonsgegevens. Elk bestuursorgaan (gemeenteraad, college of burgemeester) is verwerkingsverantwoordelijke, elk voor de eigen taken en diensten. Voor informatiebeveiliging is dit het college of de gemeenteraad.

In de organisatie zijn functionarissen nodig die ondersteunen, adviseren en toezicht houden op het gebied van informatieveiligheid en persoonsgegevens. Binnen de gemeente Hoorn zijn dat:

[10] Functieprofielen Informatiebeveiliging IBD-VNG en 6.1.1.4 BIO
[11] Functieprofiel functionaris gegevensbescherming IBD-VNG
[12] Artikel 37, 38, 39 AVG
[13] Artikel 4.7 AVG

Waarom is kennis en bewustzijn zo belangrijk?

Medewerkers zijn een belangrijke schakel bij een zorgvuldige behandeling van (persoons)gegevens. Het is van belang dat ze bewust zijn en kennis hebben om risico's op een onveilige en onrechtmatige behandeling van (persoons)gegevens en het niet (tijdig) herkennen van incidenten, te verkleinen.

Wat is het register van verwerkingsactiviteiten?

De organisatie is verplicht om een register van verwerkingsactiviteiten[14] bij te houden. Per verwerking van persoonsgegevens (proces) staat hierin: het doel, de categorieën van betrokkenen, de categorieën persoonsgegevens, derden ontvangers, bewaartermijn en beveiligingsmaatregelen.

Wat is een DPIA?

Een DPIA[15] is een onderzoek naar de rechtmatigheid van de verwerking van persoonsgegevens, de risico's en maatregelen die nodig zijn. Een DPIA:

- is verplicht als er een hoog risico is voor de personen van wie de gegevens zijn en/of op de lijst van de Autoriteit Persoonsgegevens[16] staat met verplichte DPIA's.
- moet worden uitgevoerd voordat de verwerking start. Voor verwerkingen die al bestonden heeft de Autoriteit Persoonsgegevens aangegeven dat er binnen drie jaar na inwerkingtreding van de wet moeten worden uitgevoerd.
- moet worden herzien als er veranderingen zijn. De Autoriteit Persoonsgegevens adviseert ook om DPIA's periodiek opnieuw uit te voeren ook als er niks is veranderd (één keer per drie jaar).
- moet voor advies worden voorgelegd aan de functionaris gegevensbescherming.

Wat is gegevensbescherming door ontwerp en standaard instellingen?

Gegevensbescherming door ontwerp en standaard instellingen[17] worden ook wel privacy by design en privacy by default genoemd. Bij veranderingen en vernieuwingen is het verplicht om vanaf de inrichting rekening te houden met een zorgvuldige behandeling van persoonsgegevens. Denk hierbij aan minimaal gebruik van persoonsgegevens en een passende bescherming. Standaardinstellingen zijn zo gekozen dat dit maximaal wordt geborgd. Door vooraf de verplichtte instrumenten in de AVG toe te passen, wordt privacy by design grotendeel geborgd. Denk aan het register van verwerkingsactiviteiten, DPIA en rechten van betrokkenen.

Wat voor afspraken over persoonsgegevens maken we met andere organisaties?

Als de gemeente persoonsgegevens uitwisselt met andere organisaties, is het verplicht om schriftelijke afspraken te maken over de voorwaarden en beveiliging. Externe partijen zijn te verdelen in 3 categorieën:

- De externe partij heeft een eigen verwerkingsverantwoordelijkheid[18] wat betreft de persoonsgegevens.
- Gemeente en de externe partij hebben een gezamenlijke verantwoordelijkheid[19]. Partijen bepalen samen 'het doel en de middelen' van de behandeling van de persoonsgegevens.
- De externe partij is een 'verwerker'[20]. De gemeente bepaalt 'het doel en de middelen' (voorwaarden) voor de behandeling van de persoonsgegevens door de externe partij.

Wat is een datalek?

Bij een datalek[21] zijn persoonsgegevens onterecht vernietigd of verloren gegaan, veranderd, gedeeld of toegankelijk geweest voor anderen. Het is verplicht om datalekken intern te melden en te registreren.

---

[14] Artikel 30 AVG
[15] Artikel 35 AVG
[16] Lijst verplichte DPIA's Autoriteit Persoonsgegevens
[17] Artikel 25 AVG
[18] Artikel 4.7 en 24 AVG
[19] Artikel 26 AVG
[20] Artikel 28 AVG
[21] Artikel 33 en 34 AV

Datalekken die ernstige nadelige gevolgen hebben voor personen, moeten we binnen 72 uur melden bij de Autoriteit Persoonsgegevens (AP). Er is een procedure voor het melden van datalekken.

Wat voor rechten hebben betrokkenen?

Personen hebben rechten om controle te houden over hun persoonsgegevens[22]:

- Personen hebben recht op informatie. De gemeente heeft een actieve plicht om personen vooraf in duidelijke en eenvoudige taal te informeren over persoonsgegevens (transparantiebeginsel). Dit doen we op websites en soms in andere (digitale) documenten.
- Personen hebben recht op inzage, aanpassing, verwijdering en bezwaar maken. Een inwoner kan een verzoek hiervoor doen via de website van de gemeente of via andere kanalen.
- Personen hebben het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- Personen kunnen rechtstreeks contact opnemen met de functionaris gegevensbescherming met vragen en opmerkingen over de behandeling van hun persoonsgegevens.

Hoe zit het met bewaren en vernietigen?

De gemeente maakt, ontvangt en beheert veel informatie. De informatie is belangrijk voor de bedrijfsvoering, publieke verantwoording, rechtsvinding en vanuit cultuur-historisch oogpunt. De Archiefwet geeft regels die ervoor zorgen dat de informatie goed wordt bewaard. De BIO zorgt ervoor dat de informatie goed wordt beveiligd. Onder de AVG mogen persoonsgegevens niet langer worden bewaard dan noodzakelijk[23]. Wat ‘noodzakelijk’ is moet per verwerking van persoonsgegevens worden bepaald. De Archiefwet geeft hiervoor gedeeltelijk de onderbouwing wat officiële documenten betreft.

Wat is een offensief cyberprogramma?

Een offensief cyberprogramma is erop gericht om met digitale middelen andere staten te bespioneren, beïnvloeden of - in het ergste geval - vitale infrastructuur te saboteren om zo eigen politieke, economische financiële doelen te behalen.

Wat is generatieve AI?

Generatieve AI is een technologie die op basis van een menselijke vraag of opdracht automatisch een tekst, afbeelding of video maakt. Er zijn steeds meer programma’s en online tools die deze vorm van AI inzetten. Voorbeelden van generatieve AI tools zijn ChatGPT, Bard en Copilot.

Wat is de BIO?

De Baseline Informatiebeveiliging Overheid (BIO)[24] is een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. Het is gebaseerd op NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. De BIO concretiseert een aantal normen tot verplichte overheidsmaatregelen:

- op grond van wet- en regelgeving;
- vanwege de gemeenschappelijke veiligheid van informatieketens;
- omdat deze fundamenteel zijn voor een betrouwbare c.q. professionele informatievoorziening.

De BIO helpt het lijnmanagement bij het nemen van zijn verantwoordelijkheid ten aanzien van informatiebeveiliging. In de BIO zijn namelijk op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN’s) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per bedrijfsproces bepaalt het lijnmanagement het BBN. De BIO biedt per BBN een zogenaamde BBN-toets.

---

[22] Artikel 12 tm 22 en 38.4 AVG

[23] Artikel 5.1e AVG

[24] Baseline Informatiebeveiliging Overheid

Wat is het digitale toegangsbeveiliging?

Digitale toegangsbeveiliging is een belangrijk onderdeel van de gemeentelijke informatiebeveiliging. Dit zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatie. In de BIO staan maatregelen over toegangsbeveiliging. De gemeente Hoorn heeft dit verder uitgewerkt in het Digitaal toegangsbeleid. Hierin staan bijvoorbeeld afspraken over wachtwoorden en het toekennen, beëindigen en uitvoeren van controles op toegang en rechten in systemen.