

Strategisch Privacybeleid Gemeente Hoeksche Waard

1. Inleiding

Gemeente Hoeksche Waard werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente om de gemeentelijke wettelijke taken goed uit te kunnen voeren. Denk hierbij aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om deze taken goed te volbrengen is het noodzakelijk dat de gemeente persoonsgegevens verwerkt. De burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. Gemeente Hoeksche Waard is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (hierna te noemen: AVG).

Het Strategisch Privacybeleid Gemeente Hoeksche Waard is de (strategische) kapstok voor het privacybeleid van gemeente Hoeksche Waard, waaraan aanvullende (tactische en operationele) regelingen zijn opgehangen, zoals regelingen voor het uitoefenen van AVG rechten en een protocol omtrent datalekken. Dit beleid vervangt het in 2021 vastgestelde "Privacybeleid Gemeente Hoeksche Waard".

Geldigheidsduur

Dit beleid is vastgesteld door het college van B&W als eindverantwoordelijke voor de gemeentelijke gegevensverwerking. Het beleid wordt in 2028 geëvalueerd en - waar nodig - aangepast. Daarnaast kan het college van B&W tussentijds besluiten tot aanpassing (bijvoorbeeld bij grote organisatorische veranderingen en wetswijzigingen). Dit beleid is geldig totdat een nieuwe dan wel aangepaste versie van het privacybeleid door het college van B&W is vastgesteld.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch privacybeleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.

In het jaarlijks uit te brengen en nog te ontwikkelen gemeentelijk jaarplan (vastgesteld door de directie) worden deze tactische en operationele aspecten van de bescherming van persoonsgegevens verder uitgewerkt en geconcretiseerd. In dit jaarplan staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het privacybeleid is opgenomen.

Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Definities

De definities van artikel 4 van de AVG hebben in dit beleidsdocument dezelfde betekenis. Deze definities zijn opgenomen in de bijlage die aan dit beleid is toegevoegd (bijlage 1).

1.3 Reikwijdte

Gemeente Hoeksche Waard verzamelt en gebruikt persoonsgegevens van inwoners, ondernemers, medewerkers, (keten)partners en andere natuurlijke personen (hierna te noemen: 'betrokkenen').

Het Strategisch Privacybeleid Gemeente Hoeksche Waard is van toepassing op alle verwerkingen van persoonsgegevens door of namens gemeente Hoeksche Waard, waaronder:

1. De verwerking van persoonsgegevens binnen de bedrijfsprocessen van de gemeente;
2. De verwerking van persoonsgegevens die is uitbesteed, of op een andere manier is georganiseerd, zoals deelname van de gemeente aan een rechtspersoon die voor de gemeente bepaalde diensten verricht;
3. De gegevensuitwisseling met derde partijen zoals bij samenwerkingsverbanden of leveranciers.

Inachtneming bijzondere wettelijke voorschriften

Op basis van het Strategisch Privacybeleid Gemeente Hoeksche Waard, geeft gemeente Hoeksche Waard uitvoering aan de AVG. Voor zover van toepassing, houdt gemeente Hoeksche Waard tevens

rekening met bijzondere wettelijke voorschriften – met name privacy-relevante bepalingen in de Wet basisregistratie personen, Telecommunicatiewet, Participatiewet, Jeugdwet en Wet maatschappelijke ondersteuning enzovoort.

1.4 Doel

Met dit privacybeleid geeft gemeente Hoeksche Waard een kader voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de persoonlijke levenssfeer van de personen waarvan de gemeente persoonsgegevens verwerkt (of laat verwerken). Daarnaast beoogt dit privacybeleid taken en verantwoordelijkheden op het gebied van de bescherming van persoonsgegevens helder af te bakenen.

De verdere uitwerking van dit beleid is - waar relevant - vastgelegd in de operationele documenten binnen de gemeente, zoals handreikingen, concrete werkprocedures of werkafspraken/protocollen voor algemene onderwerpen zoals datalekken.

Naast dit door het college vastgestelde privacybeleid is een strategisch informatiebeveiligingsbeleid door haar vastgesteld. Hierin zijn maatregelen opgenomen om de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens te garanderen. Informatiebeveiliging is een randvoorwaarde voor de bescherming van persoonsgegevens. Het gemeentelijke privacybeleid kan daarom niet los worden gezien van het gemeentelijke informatiebeveiligingsbeleid.

1.5 Visie en ambitie

In het Hoofdlijnenakkoord van de gemeenteraad 2022-2026 van gemeente Hoeksche Waard ("Samen doordacht doen"¹) staat:

Om effectief en efficiënt te kunnen werken, moeten medewerkers beschikken over goede voorzieningen op het gebied van informatiemanagement. Dagelijks werken medewerkers van de gemeente met (persoons)gegevens van inwoners. Aandacht voor en investeren in informatiebeveiliging en privacybescherming is nodig om de gegevens van onze inwoners te beschermen en digitale dreigingen aan te kunnen.

De komende jaren zet gemeente Hoeksche Waard in op het verhogen van de privacy bewustwording en verdere professionalisering van de privacy functie in de organisatie. Een goede privacy huishouding is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed eigenaarschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Daarbij is verantwoord en bewust gedrag van alle medewerkers essentieel voor privacy binnen de gemeente.

Het voorgaande is nader uitgewerkt in de doorontwikkeling van de organisatie van gemeente Hoeksche Waard. Versterkt zet gemeente Hoeksche Waard in op alles dat met digitale veiligheid te maken heeft.

1.6 Raakvlakken en overlap met andere beleidsthema's

Het Strategisch Privacybeleid Gemeente Hoeksche Waard heeft raakvlakken met andere beleidsthema's of vertoont hiermee overlap.

Integriteit

Privacybeleidsvoering is wettelijk gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het gemeentelijk integriteitsbeleid, zoals beschreven in de gedragscode Integriteit van Gemeente Hoeksche Waard.

Kwaliteit

Privacybeleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte en klantvriendelijke gemeentelijke taakuitoefening en goed werkgeverschap ('de mens centraal').

Continuïteit- en risicomanagement

Privacybeleid schept waarborgen op het gebied van continuïteit en risicomanagement, omdat privacybeleid afbreuk- en aansprakelijkheidsrisico's tegengaat en voorkomt dat werkprocessen spaak lopen omdat de bijbehorende gegevensverwerkingen een schending van het recht op privacy inhouden (onrechtmatige overheidsdaad).

¹) [Ontwerp-brochure-hoofdlijnenakkoord.pdf \(gemeentehw.nl\)](#)

Informatiebeveiliging

Informatiebeveiliging en privacy zijn termen die vaak hand in hand gaan. Het zijn twee verschillende begrippen, echter met een gemeenschappelijk raakvlak. Informatiebeveiliging heeft een breder bereik dan de bescherming van (alleen) persoonsgegevens. Informatiebeveiliging draait om de bescherming van alle gevoelige informatie(systemen) tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid. Een informatiebeveiligingsincident hoeft daarom niet altijd een datalek te betreffen. Dat is enkel het geval wanneer er persoonsgegevens betrokken zijn.

Een adequate informatiebeveiliging van persoonsgegevens is wettelijk verplicht voor gemeenten om te kunnen voldoen aan de AVG. Artikel 32 van de AVG schrijft voor dat: "Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen".

Informatiebeveiliging maakt daarmee een onderdeel uit van de AVG. De AVG laat de inschatting van risico's en het bepalen van de benodigde maatregelen over aan de verwerkingsverantwoordelijke (de gemeente). Normenkaders als de Baseline Informatiebeveiliging Overheid ("BIO") helpen de gemeente om de risico's goed in te schatten en de benodigde maatregelen te treffen. In de praktijk betekent dit dat de Chief Information Security Officer (CISO), de Functionaris Gegevensbescherming (FG) en de Privacy officer(s) nauw samenwerken. Hoe de gemeente omgaat met informatiebeveiliging is beschreven in het informatiebeveiligingsbeleid van gemeente Hoeksche Waard.

Privacybeleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van privacy incidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de gemeentelijke informatievoorzieningen en opgeslagen persoonsgegevens.

Personeel en organisatie

Het sturen op gekwalificeerd personeel, cultuur en een gekwalificeerde organisatie wordt uitgevoerd vanuit het HRM beleid.

Communicatie

Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het Communicatiebeleid Gemeente Hoeksche Waard.

Inkoop

Het inkoopbeleid betreft alle diensten en processen die de gemeente uitbesteedt of inkoopt, of waarbij wordt samengewerkt met derden. Hierbij worden eisen gesteld aan de waarborgen die de betreffende derde partij kan bieden. Deze dienen in lijn te zijn met de eisen aan privacywaarborgen die vanuit de gemeente gesteld worden.

2. Strategisch beleid

2.1 Principes voor de verwerking van persoonsgegevens

De AVG is gebaseerd op een aantal principes voor de verwerking van persoonsgegevens. Gemeente Hoeksche Waard onderschrijft deze principes en stelt zich ten doel persoonsgegevens slechts te verwerken in overeenstemming met deze principes.

Rechtmatige grondslag

Persoonsgegevens worden door gemeente Hoeksche Waard slechts verwerkt in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze. Dit betekent onder meer dat verwerkingen alleen plaatsvinden indien hiervoor een rechtmatige verwerkingsgrondslag bestaat. Veelal vloeit de grondslag voor een verwerking bij een gemeente voort uit een wet (wettelijke verplichting) of een publiekrechtelijke taak.

Welbepaalde doeleinden

Gemeente Hoeksche Waard verwerkt persoonsgegevens voor zeer uiteenlopende doeleinden. Zonder doel mogen persoonsgegevens niet worden verwerkt. De verwerking van persoonsgegevens vindt plaats op een wijze die noodzakelijk is om de doeleinden te bereiken waarvoor de gegevens zijn verkregen. Dit betekent dat gemeente Hoeksche Waard alleen die persoonsgegevens verwerkt die noodzakelijk zijn om het doel te bereiken (ter zake dienend).

Verdere verwerking

Persoonsgegevens kunnen in bepaalde gevallen worden verwerkt voor andere doelen dan waarvoor ze in eerste instantie zijn verzameld. Daarbij geldt onder andere dat de twee doelen aan elkaar verwant moeten zijn, er zich geen nadelige effecten voor de betrokkenen voordoen, dan wel dat hiervoor extra waarborgen zijn getroffen. Gemeente Hoeksche Waard voert, voordat de verwerking start, een toets

uit om te bepalen of de gegevens voor andere doelen mogen worden gebruikt op grond van de wet- en regelgeving.

Minimale gegevensverwerking

Gegevens mogen alleen worden verwerkt als dit in verhouding staat tot het doel. Als het doel waarvoor persoonsgegevens worden verwerkt, zonder of met minder persoonsgegevens kan worden bereikt, dan kiest gemeente Hoeksche Waard bij voorkeur voor die mogelijkheid. Ook als het doel waarvoor persoonsgegevens worden verwerkt op een wijze kan worden verwezenlijkt die minder inbreuk maakt op de privacy van de betrokkene, dan kiest gemeente Hoeksche Waard bij voorkeur voor die mogelijkheid.

Juiste en actuele gegevens

Gemeente Hoeksche Waard zorgt ervoor dat alleen persoonsgegevens worden verwerkt die juist en actueel zijn gelet op het doel waarvoor zij verzamelt zijn of vervolgens worden verwerkt. Gemeente Hoeksche Waard neemt redelijke maatregelen om persoonsgegevens juist en actueel te houden, onjuiste persoonsgegevens te actualiseren, te rectificeren en/of te wissen.

Bewaartermijnen

Gemeente Hoeksche Waard stelt de bewaartermijn van een verwerking vast aan de hand van wettelijke bepalingen en de selectielijsten. Gemeenten hebben op grond van de Archiefwet 1995 onder andere de plicht om zogenaamde selectielijsten op te stellen. Deze selectielijsten bepalen voor een selectie van documenten hoelang deze moeten worden bewaard.

Gemeente Hoeksche Waard stelt de bewaartermijn vast op basis van noodzakelijkheid. Persoonsgegevens mogen dan niet langer worden bewaard dan noodzakelijk. Gemeente Hoeksche Waard bewaart gegevens alleen langer als deze geanonimiseerd worden, zodat directe of indirecte identificatie van een persoon niet meer mogelijk is.

Integriteit en vertrouwelijkheid

Gemeente Hoeksche Waard neemt passende technische en organisatorische maatregelen om de persoonsgegevens, met name bijzondere persoonsgegevens, te beschermen tegen misbruik en onrechtmatige of ongeautoriseerde verwerking. Gemeente Hoeksche Waard handelt hierbij in overeenstemming met haar informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid verplicht gemeente Hoeksche Waard om informatie te beveiligen tegen ongeautoriseerd gebruik, vernietiging (per ongeluk of onrechtmatig), verlies of vervalsing, onbevoegde bekendmaking of toegang en alle andere onrechtmatige manieren van verwerking.

Privacy by Design en Privacy by Default

Gemeente Hoeksche Waard houdt bij de ontwikkeling van nieuwe diensten, systemen of processen rekening met aspecten van privacy en gegevensbescherming om zo te komen tot een zo optimaal mogelijke bescherming van Persoonsgegevens. Dit uitgangspunt wordt Privacy by Design genoemd. Gemeente Hoeksche Waard draagt er zorg voor dat concrete maatregelen zoveel mogelijk doorgevoerd worden in het ontwerp. Daarbij neemt de gemeente Privacy by Default als uitgangspunt: de standaardinstellingen zijn altijd zo privacy-vriendelijk mogelijk.

Toegang tot gegevens

Uitsluitend geautoriseerde gebruikers zijn bevoegd tot onder meer het invoeren, rechtstreeks raadplegen, wijzigen en verwijderen van persoonsgegevens voor zover aan hen hiervoor bevoegdheden zijn toegekend. Deze bevoegdheden worden verleend op grond van het binnen gemeente Hoeksche Waard geldend beleid voor toegang tot gegevens, waaronder haar informatiebeveiligingsbeleid. Het beheer van bevoegdheden wordt periodiek gecontroleerd. De gemeente hanteert daarnaast specifieke oplossingen en toepassingen, waaronder het bijhouden van loggegevens, om ongeautoriseerde toegang tot en niet toegestane verwerkingen van persoonsgegevens zo veel mogelijk te voorkomen en aan te pakken.

Inbreuk in verband met persoonsgegevens

Bij toegang tot, verlies of wijziging van persoonsgegevens bij gemeente Hoeksche Waard, zonder dat dit de bedoeling is, kan sprake zijn van een datalek. Dat moet, afhankelijk van het risico, worden gemeld bij de toezichthouder (de Autoriteit Persoonsgegevens) en soms bij de getroffen betrokkenen. Gemeente Hoeksche Waard registreert datalekken, zet de bevindingen om in verbeterpunten en ziet toe op de opvolging hiervan. Nadere regels ten aanzien van het vaststellen, melden en afhandelen van datalekken zijn opgenomen in het Protocol Datalekken gemeente Hoeksche Waard.

Samenwerking

Gemeente Hoeksche Waard schakelt soms derden in om persoonsgegevens in opdracht van haar te verwerken. Deze derden worden verwerkers genoemd. Ook een verwerker moet zich houden aan de privacyregelgeving en aan het Strategisch Privacybeleid van Gemeente Hoeksche Waard. De AVG

verplicht gemeenten tot het maken van contractuele afspraken met verwerkers, zogenaamde verwerkersovereenkomsten.

Samenwerkingsverbanden

Verder kan het voorkomen dat gemeente Hoeksche Waard samenwerkt met andere organisaties om een taak van algemeen belang uit te voeren. In die gevallen kan sprake zijn van meerdere verwerkersverantwoordelijken (gezamenlijk of individueel). De gemeente maakt met bedoelde organisaties afspraken over de wijze waarop persoonsgegevens worden verwerkt. Deze organisaties waarborgen een beschermingsniveau dat gelijk is aan dat van de gemeente.

Doorgifte buiten de EER

Doorgifte van persoonsgegevens aan landen buiten de Europese Economische Ruimte (EER) of een internationale organisatie, vindt alleen plaats in overeenstemming met de relevante bepalingen in toepasselijke wet- en regelgeving en dit privacybeleid.

Transparantie

Gemeente Hoeksche Waard informeert de betrokkenen tijdig, op een zo eenvoudig mogelijke, begrijpelijke en toegankelijke wijze over het feit dat zij persoonsgegevens verwerkt, op welke wijze en voor welke doeleinden. De betrokkene wordt op heldere en laagdrempelige wijze geïnformeerd over zijn rechten en de wijze waarop hij deze kan uitoefenen. Alleen indien de wet anders bepaalt, wijkt gemeente Hoeksche Waard van deze informatieplicht af.

Rechten van betrokkenen

Iedereen heeft het recht om te vernemen welke persoonsgegevens gemeente Hoeksche Waard over hem/haar heeft verzameld en waarvoor deze worden gebruikt. Betrokkenen hebben de mogelijkheid om hun rechten uit hoofdstuk III van de AVG uit te oefenen, te weten het recht van inzage, recht op rectificatie, recht op verwijdering, recht op bezwaar, recht op beperking en recht op overdraagbaarheid. Nadere regels ten aanzien van de rechten van betrokkenen zijn opgenomen in het Protocol afhandelen verzoek om inzage Gemeente Hoeksche Waard.

Geschillenbeslechting

Indien de betrokkene van mening is dat gemeente Hoeksche Waard niet op een juiste wijze met zijn persoonsgegevens is omgegaan, kan hij een klacht indienen volgens de van toepassing zijnde Klachtenregeling gemeente Hoeksche Waard. Ook is hierin geregeld wat de mogelijkheden voor betrokkene zijn wanneer hij niet tevreden is over de afhandeling van zijn klacht door gemeente Hoeksche Waard. De betrokkene heeft ook het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens, met betrekking tot de naleving van wet- en regelgeving op het gebied van de bescherming van persoonsgegevens.

Verantwoording

Onder de verantwoordelijkheid van zowel het college van B&W als de gemeenteraad vindt een groot aantal verwerkingen van persoonsgegevens plaats. Daar vindt extern en intern toezicht op plaats. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de privacyregels in Nederland. Daarnaast beschikt de gemeente over een interne toezichthouder: de Functionaris Gegevensbescherming (FG). De FG ziet erop toe dat de AVG intern wordt nageleefd. Gemeente Hoeksche Waard stelt voldoende middelen ter beschikking aan de FG om het toezicht adequaat uit te kunnen voeren.

Verwerkingsregister

Gemeente Hoeksche Waard beschikt over een verwerkingsregister, waarin alle verwerkingen van persoonsgegevens gedocumenteerd zijn en inzichtelijk zijn gemaakt.

Gegevenseffectbeoordeling (DPIA)

Als een verwerking mogelijk een hoog risico inhoudt voor de betrokkene, moet gemeente Hoeksche Waard een beoordeling uitvoeren van het effect van een verwerking van persoonsgegevens. Gemeente Hoeksche Waard voert in dat geval een gegevenseffectbeoordeling (ook wel 'Data Protection Impact Assessment' of 'DPIA' genoemd). Als uit de gegevenseffectbeoordeling blijkt dat er inderdaad hoge risico's zijn verbonden aan de verwerking, moet de gemeente voldoende maatregelen nemen om de risico's te verminderen. Als het niet lukt om (voldoende) maatregelen te nemen om dit risico te beperken, dan moet de gemeente met de AP overleggen, voordat zij met de verwerking start. Dit wordt een voorafgaande raadpleging² genoemd.

Functionaris gegevensbescherming (FG)

2) <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorafgaande-raadpleging>

Gemeente Hoeksche Waard is een overheidsinstantie die structureel en op grote schaal persoonsgegevens verwerkt, waaronder bijzondere persoonsgegevens. Gemeente Hoeksche Waard is daarom verplicht een FG aan te stellen. De FG is de onafhankelijke interne toezichthouder en heeft een adviserende, informerende en toezichthoudende taak. Dit betekent dat de FG toeziet op alle verwerkingen van persoonsgegevens. De FG brengt jaarlijks een verslag uit aan de gemeenteraad en het College van B&W van zijn werkzaamheden, bevindingen en aanbevelingen.

PDCA Cyclus

Gemeente Hoeksche Waard streeft ernaar om rondom de verwerking van persoonsgegevens in control te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat gemeente Hoeksche Waard weet welke maatregelen genomen zijn ten aanzien van de verwerking van persoonsgegevens, dat er een planning is van de maatregelen die nog niet genomen zijn en dat dit geheel verankerd is in een Plan-Do-Check-Act-cyclus.

Daarnaast gebruikt gemeente Hoeksche Waard de Privacy Baseline van het Centrum Informatiebeveiliging en Privacybescherming (CIP)³ als het beoordelingskader voor het waarborgen van privacy compliance binnen de gemeente. De Privacy Baseline is een normenkader dat door de gemeente gebruikt wordt voor het duiden van privacy risico's en de daarbij behorende beheersmaatregelen binnen de gemeente.

Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn in de gemeentelijke organisatie voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag om persoonsgegevens zorgvuldig te verwerken wordt aangemoedigd. Iedere medewerker wordt aantoonbaar geïnformeerd over het zorgvuldig omgaan met persoonsgegevens, bijvoorbeeld via instructies. Dit gebeurt passend binnen de context van en bij het domein waarbinnen die worden verwerkt.

3. Organisatie, rollen en verantwoordelijkheden

3.1 Three Lines

In dit hoofdstuk wordt uiteengezet welke rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines model' (ook wel bekend als 'Three Lines').



Three Lines biedt een overkoepelende visie en strategie hoe de bescherming van persoonsgegevens effectief belegd wordt binnen de organisatie. Daartoe bevat het een beschrijving van de taken en ver-

3) [Producten/diensten - cip-overheid](#)

antwoordelijkheden van het college van B&W, het managementteam (directie en teammanagers) en medewerkers, de Functionaris voor de Gegevensbescherming (FG), de Privacy Officer en de CISO (zie afbeelding hieronder).

	Verantwoordelijk	
R	Responsible/feitelijk verantwoordelijk	- Directie en teammanagers - De medewerkers (inclusief inhuur/externen) die persoonsgegevens verwerken
A	Accountable/eindverantwoordelijk	Het College van B&W
C	Consulted/adviserend	- Privacy officer - CISO - Functionaris Gegevensbescherming (FG)
I	Informed/geïnformeerd	- Gemeenteraad - FG - Belanghebbenden(n)/Betrokkene(n)

3.2 Rollen en verantwoordelijkheden

College van B&W

Het College van B&W van gemeente Hoeksche Waard is eindverantwoordelijk voor de naleving van privacywetgeving.

Het College heeft de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen gemeente Hoeksche Waard;
- Stelt het privacybeleid vast;
- Geeft sturing aan privacy beleidsvoering en legt rekenschap af over privacy beleidsvoering aan de FG;
- Evalueert de toepassing en werking van het privacybeleid op basis van de rapportage van de FG;
- Bevordert duurzame privacycultuur.

Directeuren en teammanagers

De directeuren en teammanagers zijn eindverantwoordelijk voor de naleving van de privacywetgeving binnen het team, alsmede voor de uitvoering van het privacybeleid.

De directeuren en teammanagers hebben de volgende rollen en verantwoordelijkheden:

- Eindverantwoordelijk voor de naleving van de privacywetgeving binnen het (de) eigen team(s);
- Verantwoordelijk voor implementatie en uitvoering van het privacybeleid binnen het (de) eigen team(s);
- Informeert de FG op welke manier het (de) eigen team(s) compliant is aan de privacywetgeving;
- Verantwoordelijk voor (laten) volgen van trainingen door medewerkers binnen het (de) eigen team(s);
- Verantwoordelijk voor registreren van de gegevensverwerkingen in het verwerkingsregister voor zover dit betrekking heeft op het (de) eigen team(s);
- Verantwoordelijk voor autorisatie en intrekken van de autorisatie van medewerkers die persoonsgegevens verwerken;
- Bevordert duurzame privacycultuur;
- Betrekt een Privacy officer en/of de FG in een vroeg stadium bij nieuwe of gewijzigde verwerkingen van persoonsgegevens.

Functionaris Gegevensbescherming (FG)

Op basis van de AVG is het aanstellen van een Functionaris voor Gegevensbescherming (FG) verplicht voor gemeente Hoeksche Waard. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG conform artikel 37-39 AVG. De FG heeft een onafhankelijke adviserende en toezichthoudende positie in de organisatie.

De FG heeft de volgende rollen en verantwoordelijkheden:

- Interne toezichthouder op de naleving van de AVG namens de Autoriteit Persoonsgegevens;
- Monitort veranderingen in wetgeving en stelt de impact van deze wijzigingen vast en adviseert de organisatie bij de implementatie hiervan;

- Neemt de leiding bij het interpreteren van (nieuwe) wetgeving op het gebied van privacy en gegevensbescherming;
- Draagt privacybeleid actief uit binnen de gehele gemeente en bevordert een cultuur van duurzame gegevensbescherming;
- Adviseert verwerkingsverantwoordelijken bij privacyklachten en verzoeken van betrokkenen (ombudsfunctie);
- Adviseert verwerkingsverantwoordelijken ten aanzien van het mitigeren van privacy risico's, bijvoorbeeld bij het uitvoeren van DPIA's en hoog-risico dossiers;
- Adviseert de verwerkingsverantwoordelijke bij datalekken (volgens de meldprocedure);
- Beheert het centrale verwerkingsregister;
- Beschikt over controle- en monitoringbevoegdheden (het recht om interne onderzoeken te laten uitvoeren met toegang tot informatie);
- Rapporteert aan het College van B&W.

Privacy Officer

De Privacy Officer is het eerste aanspreekpunt voor gemeente Hoeksche Waard rondom privacygerelateerde vraagstukken, en heeft een monitorende en ondersteunende functie rondom het naleven en uitvoeren van het privacybeleid.

De Privacy Officer heeft de volgende rollen en verantwoordelijkheden:

- Adviseert en faciliteert de verwerkingsverantwoordelijken ten aanzien van het naleven en de uitvoering van het privacybeleid;
- Opstellen privacybeleid en modellen, formats en standaard-overeenkomsten, waaronder o.a. de verwerkersovereenkomst en de overeenkomst voor uitwisseling van persoonsgegevens;
- Monitort en ondersteunt verwerkingsverantwoordelijken bij toepassing, opvolging en uitvoering van het privacybeleid;
- Monitort en ondersteunt het (laten) registreren van verwerkingen in het verwerkingsregister door de verwerkingsverantwoordelijke en het (laten) registreren van relevante wijzigingen;
- Adviseert de verwerkingsverantwoordelijke bij het uitvoeren van gegevenseffectbeoordeling (GEB) en de daaruit voortvloeiende risico's alsmede de organisatorische en technische maatregelen om deze te mitigeren;
- Adviseert over de bepalingen in verwerkersovereenkomsten en faciliteert bij het opstellen, aanpassen en uitonderhandelen daarvan;
- Adviseert over mechanismen voor internationale uitwisseling van persoonsgegevens naar landen buiten de EU/EER;
- Adviseert over privacy-gerelateerde bepalingen in overeenkomsten met derden waarbij persoonsgegevens worden uitgewisseld;
- Adviseert over de verwerkingsgrondslag (en adviseert, indien van toepassing, over de informed consent);
- Ontwikkelt de bewustmakingsprogramma's- en privacytrainingen voor medewerkers, organiseert deze en voert deze trainingen uit;
- Adviseert de verwerkingsverantwoordelijke over Privacy by Design & Default bij ontwikkeling van nieuwe systemen in samenwerking met de CISO en ondersteunt en faciliteert bij het opstellen en uitwerken daarvan;
- Ondersteunt en faciliteert verwerkingsverantwoordelijke bij het afhandelen van datalekken (volgens de meldprocedure).

3.3 Andere rollen en verantwoordelijkheden

Team	Betrokkenheid
Juridische Zaken	• Ondersteunen van Privacy officer ten aanzien van privacyvraagstukken en adviseren over privacy-gerelateerde bepalingen in overeenkomsten; • Coördinerende rol bij het behandelen van AVG verzoeken.
CISO	• Toepassing en implementatie van technische en organisatorische maatregelen in het kader van de bescherming van persoonsgegevens; • Adviseren van de organisatie bij datalekken (volgens de meldprocedure); • Tijdig melden van Informatiebeveiligingsincidenten bij PO/FG als er mogelijk sprake is van betrokkenheid van persoonsgegevens bij het incident.

Communicatie	• In alle gevallen waarbij communicatie (intern en extern) een rol speelt worden medewerkers van communicatie betrokken; • Adviseren van de organisatie over de communicatie bij datalekken (volgens de meldprocedure).
Concern control	• Toetst het goed en betrouwbaar functioneren van de gehele interne organisatie.
Informatiemanagement	• Inrichten van de informatievoorziening (de beoordeling van welke functionaliteit en welke data in op welke wijze / in welk systeem verwerkt kan / moet worden).

Bijlage 1: Definities uit artikel 4 AVG

persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

beperken van de verwerking: het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;

profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

bestand: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;

verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;

verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;

derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;

toestemming van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

genetische gegevens: persoonsgegevens die verband houden met de overgeërfd of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of

de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;

biometrische gegevens: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;

gegevens over gezondheid: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;

hoofdvestiging: a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd; b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;

vertegenwoordiger: een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;

onderneming: een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;

concern: een onderneming die zeggenschap uitoefent en de ondernemingen waarover die zeggenschap wordt uitgeoefend;

bindende bedrijfsvoorschriften: beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van ondernemingen die gezamenlijk een economische activiteit uitoefenen;

toezichthoudende autoriteit: een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;

betrokken toezichthoudende autoriteit: een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat: a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd; b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of c) bij die toezichthoudende autoriteit een klacht is ingediend;

grensoverschrijdende verwerking: a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;

relevant en gemotiveerd bezwaar: een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;

dienst van de informatiemaatschappij: een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (19);

internationale organisatie: een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen.