Gemeente Haarlem

GEMEENTEBLAD

Officiële uitgave van de gemeente Haarlem

Nr. 21316

19 januari

2026

Gemeentelijk privacybeleid 2025-2028

1. Inleiding

1.1 Introductie

1.1.1 Privacybeleid

Deze beleidsnota beschrijft het Privacybeleid voor de gemeente Haarlem voor de jaren 2025 tot 2028 en vervangt de nota Privacybeleid en het daarmee samenhangende *'Privacyreglement Haarlem'* uit 2018. Deze beleidsnota is richtinggevend en kaderstellend.

1.1.2 Volgende stap in privacybescherming

Met dit beleid zet de gemeente een volgende stap in de bescherming van persoonsgegevens en bouwt voort op de ervaring met naleving van privacywetgeving van de afgelopen jaren. Daarnaast is een aantal rapporten en adviezen gebruikt om dit beleid vorm te geven, waaronder:

- Nota Privacybeleid (2017)
- Privacyreglement Haarlem (2018)
- Gemeentelijk beleid voor Informatiebeveiliging en Bedrijfscontinuïteit (2023)
- Jaarrapportages Functionaris Gegevensbescherming (2020-2023)
- Rapportage 213A van Eiffel; Adviesaudit Privacybeleid (2024)
- Visie 'Haarlem in de informatiesamenleving' (2024)
- Datastrategie 'Data, de Haarlemmerolie van nu' (2023-2026)
- 'Sectorbeeld Overheid' van de Autoriteit persoonsgegevens (2024)
- Haarlemse cloudvisie (2024)
- Intern beleid generatieve AI (2024)

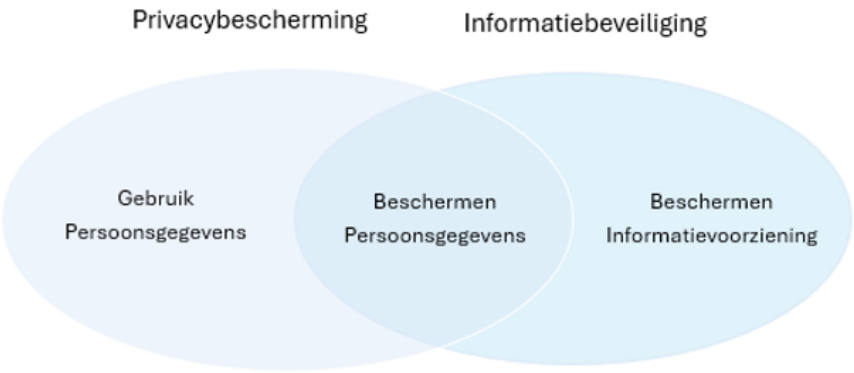
1.1.3 Reikwijdte privacybeleid

Het privacybeleid geldt voor alle processen en handelingen van de gemeente waarin persoonsgegevens worden verwerkt en gedeeld. Het is onderdeel van de dienstverlening.
Het beperkt zich echter niet alleen tot de Informatie Technologie (IT), maar heeft betrekking op het (politieke) bestuur, medewerkers, inwoners, klanten, bezoekers, externe relaties en ketenpartners zoals politie, overheden en (maatschappelijke) organisaties.
Het beleid borgt daarmee de privacy gedurende de hele levenscyclus van informatiesystemen en de hele levenscyclus van gegevens, ongeacht de toegepaste technologie, zowel op papier als digitaal.

1.2 Wat is Gegevensbescherming?

Gegevensbescherming en privacy zijn nauw met elkaar verbonden, maar niet helemaal hetzelfde. Gegevensbescherming richt zich specifiek op het beschermen en correct verwerken van persoonsgegevens volgens wettelijke regels, met als doel deze te beschermen tegen beschadiging, ongeautoriseerde toegang en verlies. Het gaat dus over meer dan alleen persoonsgegevens. Het is een belangrijk concept in de moderne digitale wereld waarin de gemeente zich bevindt, waar veel (persoonlijke) informatie wordt verzameld, opgeslagen en gedeeld.

Het is cruciaal om deze door de gemeente beheerde gegevens van burgers en bedrijven te beschermen tegen diefstal, lekken, corruptie en verlies van die gegevens. Het ondersteunt bij het naleven van wettelijke voorschriften en het beschermen en faciliteren van rechten van betrokkenen, en het beschermen van de reputatie van de organisatie.



Gegevensbescherming bestaat dus uit twee - deels overlappende - pijlers: Privacybescherming en Informatiebeveiliging. Privacy gaat om het afschermen van persoonsgegevens. Dit houdt het treffen van beveiligingsmaatregelen in om de privacy en veiligheid van persoonlijke informatie te waarborgen. Toegang tot persoonsgegevens dient te worden verstrekt op een *'need to know'* basis: enkel bevoegde medewerkers hebben toegang tot de benodigde gegevens voor zover noodzakelijk voor de uitvoering van het werk. Informatiebeveiliging draait om het beschermen van persoonsgegevens en de informatievoorziening als geheel. Naast informatiebeveiliging zijn ook aanverwante terreinen als gegevensmanagement en data governance van belang bij gegevensbescherming.

1.3 Wat is Privacy?
Privacy verwijst naar het recht van individuen om hun persoonlijke informatie te beschermen tegen ongeautoriseerde toegang. In de Nederlandse Grondwet is privacy omschreven als het recht op eerbiediging van de persoonlijke levenssfeer. Het concept privacy omvat dus verschillende aspecten, waaronder:

- de bescherming van persoonsgegevens als randvoorwaarde voor privacybescherming
- het recht op vertrouwelijke communicatie
- de autonomie om te bepalen wie toegang heeft tot persoonlijke informatie

Privacy is onder andere verankerd in de Grondwet, het Europees Verdrag voor de Rechten van de Mens (EVRM) en verder uitgewerkt in o.a. de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de Wet politiegegevens (Wpg). Ook binnen het brede scala aan materiewetgeving die van toepassing is op gemeentes, is aandacht voor privacy.

Het concept privacy in het kader van dit beleid draait voornamelijk om de verwerking en bescherming van persoonsgegevens door de gemeente. Met persoonsgegevens wordt de informatie bedoeld die – al dan niet met enige moeite, direct of indirect - herleid kan worden tot, en betrekking heeft op individuele personen.

Privacybescherming wordt uitgevoerd vanuit een aantal beleidsprincipes. Deze worden in hoofdstuk 2 besproken.

1.4 Wat is Informatiebeveiliging?
Onder informatiebeveiliging wordt verstaan: het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Belangrijke begrippen hierbij zijn Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van persoonsgegevens en andere gegevens.

Beschikbaarheid	De mate waarin gegevens en gegevensverwerkingen op de juiste momenten beschikbaar zijn voor gebruikers.
Integriteit	De mate waarin de juistheid en volledigheid van gegevens is gewaarborgd.
Vertrouwelijkheid	De mate waarin gegevens alleen toegankelijk zijn voor degenen die hiervoor gerechtigd zijn.

De verdere uitwerking van het Informatiebeveiligingsbeleid ligt vast in het 'Gemeentelijk beleid voor informatiebeveiliging en bedrijfscontinuïteit'. Deze beleidsstukken staan naast elkaar.

1.5 Visie gemeente op privacybescherming

1.5.1 Dienstverlening

De gemeente staat midden in de samenleving. Samen maken ze de stad en het dorp. De omvang van de dienstverlening is in de afgelopen jaren flink toegenomen. Ze heeft meer taken gekregen en de interactie tussen inwoners, de gemeente en haar (keten)partners is steeds diverser en omvangrijker geworden. Vanwege de toenemende digitalisering is de kwaliteit van de informatie nog belangrijker voor een goede bedrijfsvoering en dienstverlening. Die kwaliteit steunt op het goed borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van bedrijfs- en persoonsinformatie. Gegevensverwerking is geen doel op zich, maar staat ten dienste van de betrokkenen en is onderdeel van de dienstverlening. Zowel intern als extern bij organisaties - onder andere in het sociaal domein- bestaat een grote behoefte tot gegevensdeling om taken uit te kunnen voeren, en om diensten te verlenen aan betrokkenen. Wetgeving zoals de *Wet aanpak meervoudige problematiek sociaal domein* (WAMS) is in ontwikkeling om dit beter mogelijk te maken. Ook de *Wet gegevensverwerking door samenwerkingsverbanden* (WGS) biedt de gemeente de ruimte om samen te werken.

1.5.2 Nieuwe ontwikkelingen, risico's, wetgeving

Nieuwe ontwikkelingen zoals het gebruik van algoritmen, al dan niet in combinatie met Artificiële Intelligentie (AI), stelt ons voor nieuwe uitdagingen, maar bieden ook oplossingen. Daarnaast heeft zich een vorm van criminaliteit ontwikkeld met als bedrijfsmodel geld verdienen aan het ontwrichten van de informatievoorziening en het gijzelen, stelen en verkopen van persoonsgegevens. De omvang en de impact van deze criminaliteit zijn aanzienlijk, en stijgt ieder jaar verder[1] . Het vraagt om robuuste technische beveiliging, maar ook om getraind, geschoold en bewust personeel op dit gebied.

Ook op geopolitiek vlak zijn er ontwikkelingen gaande die zich richten op ontwrichting van bedrijven en instellingen, en de samenleving als geheel. En vanuit 'Brussel' wordt er steeds meer gevraagd aan en van ons. Een voorbeeld hiervan is de *AI Act*[2] . De AI Act stelt juridische kaders voor de ontwikkeling, uitrol en toepassing van systemen met AI. Dat vergt voor zowel leveranciers, als de gemeente en medewerkers een aanzienlijke inspanning. Zowel op het gebied van compliance, als op 'AI geletterdheid' van de organisatie en medewerkers, zeker waar het mogelijk hoog risico AI betreft.

Deze ontwikkelingen vragen om ambitie en visie van de gemeente. Om zo privacybescherming optimaal te ontwikkelen en in te bedden in alle processen die Haarlem uitvoert voor zichzelf, voor andere gemeenten, of laat uitvoeren door andere organisaties.

De gemeente is zich bewust van deze maatschappelijke ontwikkelingen en realiseert zich eveneens dat zij een belangrijke rol speelt in het beschermen van de informatie die haar is toevertrouwd door haar inwoners, ondernemers en (keten)partners. De gemeente heeft een machtspositie, en een *'verticale relatie'* met bewoners en ondernemers. De inwoner of ondernemer kan niet naar een ander loket voor diensten.

1.5.3 Uitgangspunten

In onze interne dienstverleningsuitgangspunten in het Organisatiekompas, en in de Datastrategie wordt daarom benadrukt dat de gemeente betrouwbaar en te vertrouwen wil zijn, omdat ze in optreden en uitvoering het gezicht is van de betrouwbare overheid. In 2024 heeft de Haarlemse Raad de nota *'Haarlem in de Informatiesamenleving'* vastgesteld. Hierin zijn een aantal publieke waarden geformuleerd:

- De mens staat voorop
- Rechtvaardig en democratisch gelegitimeerd
- Gegevens zijn betrouwbaar en veilig
- De gemeente is transparant en controleerbaar

De datastrategie *'Data, de Haarlemmerolie van nu'* die gaat over hoe de gemeente met data en de inzet daarvan om wil gaan, beschrijft de volgende (data-)waarden in het verlengde daarvan:

- Transparant: publiek inzicht in zoveel mogelijk data
- Data wordt zoveel als mogelijk openbaar gemaakt, enerzijds ter verantwoording van besluitvorming en anderzijds voor hergebruik. Ook kunnen inwoners van de gemeente te allen tijde te weten komen hoe en waarom (hun) data gebruikt wordt.
- Waardecreërend: publieke waarde uit data halen
- Data wordt direct én indirect ingezet ten behoeve van maatschappelijke opgaven en uitsluitend met oog voor de menselijke maat.

1) *Gemeenten flink getroffen door cyberincidenten*

2) *eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0206*

- Betrouwbaar: data is veilig en correct
- Inwoners kunnen vertrouwen dat (hun) data onder de hoede van de gemeente in veilige handen is en dat gebruikte data klopt.
- Verantwoord: data gebruik met de menselijk maat
- Inwoners kunnen rekenen op het bewust en verantwoord handelen van de gemeente. En de gemeente zoekt actief het gesprek met de samenleving over ethische dilemma's.

Deze waarden vormen samen met de beginselen van de AVG de basis waarop dit privacybeleid gestoeld is. De AVG-beginselen zijn:

- Rechtmatigheid: persoonsgegevens worden alleen verwerkt als daar een geldige wettelijke grondslag voor is;
- Behoorlijkheid: de persoonsgegevens worden op een eerlijke en zorgvuldige manier verwerkt, waarbij rekening gehouden wordt met de belangen van betrokken personen;
- Transparantie: betrokkenen moeten weten welke gegevens verzameld worden, waarom dat gedaan wordt, en wat er met hun gegevens gebeurt.
- Doelbinding: persoonsgegevens worden alleen verzameld en gebruikt voor een specifiek, vooraf bepaald en gerechtvaardigd doel, en niet voor andere doeleinden.
- Dataminimalisatie: enkel die persoonsgegevens worden verwerkt die strikt noodzakelijk zijn voor het beoogde doel.
- Juistheid: persoonsgegevens zijn correct, actueel en worden zo nodig bijgewerkt om te voorkomen dat onjuiste of verouderde gegevens worden verwerkt.
- Opslagbeperking: persoonsgegevens worden niet langer bewaard dan nodig is voor het doel waarvoor ze zijn verzameld en worden verwijderd zodra ze niet meer nodig zijn.
- Vertrouwelijkheid en integriteit: persoonsgegevens worden zodanig beveiligd dat ze beschermd zijn tegen ongeoorloofde toegang, onrechtmatige verwerking, verlies, vernietiging of wijziging.

1.5.4 Privacybescherming als integraal onderdeel van de bedrijfsvoering

Privacybescherming raakt alle aspecten van een organisatie, de systemen, processen en medewerkers. Het is geen 'sluitpost' of alleenstaand onderdeel van een project of een puur technische kwestie, maar een continu proces dat onderdeel is van onze dagelijkse werkzaamheden.

De AVG vereist daarom dat privacybescherming verankerd is in de bedrijfsprocessen. Voor de komende beleidsperiode heeft de gemeente een aantal ambities geformuleerd om hieraan recht te doen; de doelen van dit beleid.

1.6 Doelen van dit beleid

Dit privacybeleid richt zich op de middellange termijn (tot 2028). In deze periode wil de gemeente een aantal doelen bereiken:

1.6.1 Privacybescherming verder op orde

De gemeente heeft de afgelopen jaren een flink aantal *'privacy producten'* ontwikkeld. Deze worden gebruikt bij de bedrijfsvoering, dragen bij aan naleving van wet- en regelgeving, ondersteunen bij privacy risicomanagement, en bewerkstelligen bewustwording van het belang van privacybescherming. Hierdoor is de gemeente in staat haar kernprocessen op dit gebied uit te voeren.

Deze kernprocessen zijn:

- Opstellen, implementeren en onderhouden van het privacybeleid
- Geven van voorlichting over privacy en verhogen van de bewustwording
- Onderhouden van een Register van verwerkingsactiviteiten (verwerkingsregister), inclusief Algoritmeregister[3]
- Uitvoeren van de Meldplicht Datalekken, inclusief registratie en rapportage
- Uitvoeren van Data Protection Impact Assessments (DPIA) voor nieuwe projecten en bestaande verwerkingen
- Ondersteunen en adviseren bij aankoopbeleid IT systemen en projectmanagement ten aanzien privacyaspecten
- Afsluiten en managen van verwerkersovereenkomsten
- Adviseren afdelingen bij vraagstukken over privacy, gegevensdeling en/of verwerking van persoonsgegevens
- Uitvoeren van de rechten van betrokkenen, inclusief registratie en rapportage
- Transparantie realiseren en borgen, door privacy verklaringen op te stellen

3) *Impactvolle algoritmes worden tevens gepubliceerd in het Algoritmeregister van de Overheid*

- Borgen van Privacy by Design en Privacy by Default bij het ontwerp van processen en informatiesystemen
- Rapportage over de uitvoering van deze processen aan de Functionaris Gegevensbescherming, het management, het bestuur en desgevraagd bij de Autoriteit Persoonsgegevens (AP)

De producten worden periodiek gecontroleerd op actualiteit en herzien indien nodig. Deze activiteiten worden gepland en uitgevoerd volgens het Privacy Jaarplan. Om de organisatie en afdelingen te helpen bij het naleven van privacy wet- en regelgeving, worden de afdelingen en domeinen ondersteund door privacy adviseurs.

1.6.2 Vergroten van de Privacy volwassenheid

Om compliance aan te kunnen tonen, is een bepaald niveau van volwassenheid nodig. De komende jaren zal er een flinke inspanning geleverd worden om de afdelingen hierbij verder te helpen.

De afdelingsmanagers zijn verantwoordelijk voor de naleving van privacy wet- en regelgeving. Zij worden hierbij ondersteund door de privacy adviseurs. In hoofdstuk 3 wordt dit verder uitgewerkt.

1.6.3 Geïnformeerde, geschoolde en bewuste afdelingen en medewerkers

Het privacy bewustzijn van de organisatie moet verder vergroot worden. Het is een cyclus van continue informeren, leren en ondersteuning bieden. Hiervoor wordt een bewustwordingsprogramma opgesteld.

Privacybescherming werkt door in bijna alle gemeentelijke processen. Het zou niet moeten worden gezien als een laatste horde, maar als een randvoorwaarde voor succesvolle dienstverlening en een betrouwbare gemeente. Daarom dienen medewerkers, afhankelijk van hun functie in meer of mindere mate, zich bewust te zijn van de spelregels qua omgang met persoonsgegevens, de systemen waar ze in zitten, en de rechten van de mensen over wie de gegevensverwerking gaat.

Ook moeten medewerkers potentiële datalekken kunnen herkennen, en weten waar ze deze moeten melden, en binnen welke termijn.

Bij projecten waarbij persoonsgegevens een rol gaan spelen, dient van te voren over de risico's voor de betrokkenen van de gegevensverwerking te worden nagedacht. Bijvoorbeeld door de uitvoering van een DPIA, en de betrokkenheid van een privacy adviseur bij projecten, om zo een project goed op te kunnen leveren. Maar ook bij het afsluiten van verwerkersovereenkomsten, en het vaststellen van privacy vereisten in plannen van aanpak en aanbestedingen.

2. Privacybeleid

2.1 Zeggen wat je doet, doen wat je zegt

Het bereiken van de privacy doelstellingen doen we aan de hand van de volgende beleidsregels voor privacybescherming. Hiermee wil de gemeente transparant zijn over wat ze doet, en vertellen hoe.

2.1.1 Voldoen aan wet- en regelgeving

Privacybescherming draagt bij aan het realiseren van onze doelstellingen, rekening houdend met geldende wet- en regelgeving. Voor privacybescherming is de AVG en UAVG leidend.

Er worden enkel persoonsgegevens verwerkt indien daar een grondslag voor is. Deze grondslagen vloeien voornamelijk voort uit taken die de gemeente uitvoert op basis van wettelijk toegekende bevoegdheden, of een wettelijke verplichting.

Vanuit de privaatrechtelijke taak als werkgever geeft de gemeente uitvoering aan de arbeidsovereenkomst met medewerkers, of beroept zich op een gerechtvaardigd belang, bijvoorbeeld om de veiligheid van werknemers te vergroten, of eigendommen te beschermen.

De gemeente is gebonden aan de grondslagen uit de Wpg voor de taken die worden uitgevoerd door buitengewoon opsporingsambtenaren (boa's) in het kader van hun politietaak:

- Opsporen van strafbare feiten
- Handhaven van de openbare orde
- Schrijven van een proces-verbaal bij het plegen van een strafbaar feit, en afhandelen van hieraan gerelateerde betalingen zoals boetes voor fout parkeren

Ieder jaar wordt een interne privacy audit op naleving van de Wpg uitgevoerd. Eens per vier jaar is het wettelijk verplicht een externe Wpg audit te laten uitvoeren. Intern houdt de FG toezicht op naleving van zowel de AVG als de Wpg. De grondslagen van alle verwerkingen liggen vast in het verwerkingsregister van de afdelingen.

2.1.2 Zicht en grip op de processen waarbij persoonsgegevens worden verwerkt

Iedere afdeling die persoonsgegevens verwerkt heeft een verwerkingsregister waarin dit is vastgelegd. Hiermee hebben we grip op, zicht op, en inzicht in de processen waarbij persoonsgegevens worden gebruikt. Het register wordt onder andere gebruikt bij privacy management, projecten, DPIA's, en de uitvoering van rechten van betrokkenen. Indien een afdeling een nieuwe verwerking start, wordt deze toegevoegd aan het register.

De afdelingen beheren hun eigen register, en eens per jaar doet het privacy team een gecoördineerde uitvraag aan de afdelingen om het register te controleren op actualiteit, volledigheid en correctheid. In de komende jaren werken we toe naar het online publiceren van het register op de gemeentewebsite.

2.1.3 In een vroeg stadium nadenken over passende privacybescherming

Bij (IT) projecten met een privacy component, wordt per project geadviseerd over de voorgenomen gegevensverwerking en beveiligingsmaatregelen. Indien persoonsgegevens worden verwerkt, wordt gecontroleerd of dat volgens de beginselen van de AVG gebeurt, wat het risico van de verwerking is voor de betrokkenen, welke beveiligingsmaatregelen moeten worden toegepast, en of een risicoanalyse nodig is. In die gevallen wordt een DPIA uitgevoerd. De Functionaris Gegevensbescherming adviseert altijd over de voorgenomen gegevensverwerking. Bij twijfel of een DPIA verplicht is, wordt een DPIA Quickscan uitgevoerd die uitsluitsel geeft.

Er worden passende technische en organisatorische maatregelen genomen voor de bescherming van onze systemen en gegevens. We passen daarbij dataminimalisatie en privacy by design en by default toe.

2.1.4 Het scholen van medewerkers over privacybescherming, en de gevaren van cybercriminaliteit

Een groot deel van privacybescherming is mensenwerk. Medewerkers zijn allemaal in meer of mindere mate bezig met het beschermen van de persoonsgegevens van burgers en bedrijven, onze systemen waarin dat gebeurt, en de processen die dat mogelijk maken. Menselijk handelen kan echter ook een risico zijn. (on)Bewust kunnen er fouten worden gemaakt met mogelijk grote gevolgen.

Daarom maken we medewerkers voortdurend en op verschillende manieren bewust over dit onderwerp. Alle medewerkers die in dienst komen volgen op dit moment een e-learning AVG Basiskennis. Er is in 2025 een nieuw gemeente breed bewustwordingsprogramma opgezet waarbij medewerkers, functieafhankelijk, geschoold worden in:

- Datagedreven werken
- Gegevensmanagement
- Generatieve AI
- Informatiebeheer
- Informatiebeveiliging
- Privacy & Ethiek

Op deze wijze wordt passend invulling gegeven aan het bevorderen van het bewustzijn op het gebied van datagebruik, -beheer en -bescherming.

Daarnaast zijn er andere kanalen zoals het gemeentelijk Intranet, posters, blogs etc. beschikbaar om voorlichting te geven over de diverse onderwerpen. De privacy adviseurs gaan langs bij afdelingen om voorlichting en presentaties te geven. Jaarlijks wordt op de Dag van de Privacy (28 januari) op diverse manieren aandacht aan privacybescherming gegeven. Ook is er ruimte en budget voor ad hoc acties of campagnes zoals phishing. Om alle activiteiten te coördineren wordt vanaf 2025 een jaarlijks Bewustwordingsplan opgezet.

2.1.5 Herkennen en leren van incidenten

Waar gewerkt wordt, worden soms fouten gemaakt. Vervelend, maar het kan iedereen overkomen. Er wordt continue aandacht gegeven aan beveiligingsincidenten en mogelijke datalekken. Via voorlichting en instructies wordt ervoor gezorgd dat medewerkers beveiligingsincidenten en datalekken kunnen herkennen, en weten waar ze deze kunnen melden.

Het melden van een mogelijk datalek is nadrukkelijk géén schandpaal. Alle medewerkers worden gestimuleerd om incidenten te melden. De privacy en security adviseurs coördineren alle meldingen. Dat gebeurt volgens de interne datalekprocedure. Indien nodig worden datalekken gemeld bij de Autoriteit Persoonsgegevens en de betrokkene(n).

In het datalekregister worden alle incidenten vastgelegd, inclusief beoordeling en afhandeling. De Functionaris Gegevensbescherming maakt periodiek een rapportage van de incidenten, en waar mogelijk en nodig worden maatregelen genomen om de kans op herhaling te verkleinen.

2.1.6 Het transparant informeren van burgers en bedrijven over gegevensverwerking

Transparantie is een kernbegrip binnen de gemeente. Daar waar het gaat om openbaarheid van overheidsinformatie, het programma Wet Open Overheid (WOO), Open data Haarlem, of om gegevensverwerking, de gemeente wil zo transparant als mogelijk zijn.

Voor burgers en bedrijven hebben we een privacyverklaring opgesteld. Ook voor medewerkers is er een privacyverklaring. Hierin wordt uitgelegd wat de gemeente doet met de gegevens die ze verwerkt. Indien medewerkers, inwoners of bedrijven hier vragen over hebben, of aanvullende informatie willen, kunnen ze contact opnemen met de Functionaris Gegevensbescherming.

Het is de ambitie van de gemeente om de privacy verklaringen komende jaren verder te verbeteren. Bijvoorbeeld door deze op te stellen per domein en/of per proces. De specifieke privacyverklaring voor bodycams is hier een voorbeeld van.

2.1.7 Het uitvoeren van de rechten van betrokkenen

Er zijn procedures ingericht om uitvoering te geven aan de rechten van betrokkenen. Deze rechten zijn beschreven in de privacyverklaring. Niet alle AVG rechten zijn 'absoluut'. Het kan voorkomen dat een verzoek niet ingewilligd wordt, bijvoorbeeld omdat een andere wettelijke verplichting in tegenstrijd is met het AVG verzoek. Betrokkenen krijgen naar aanleiding van het verzoek een besluit in de zin van de Algemene wet bestuursrecht (Awb). Tegen dit besluit kan bezwaar worden gemaakt.

De afdeling Privacy ontvangt, verwerkt en coördineert AVG verzoeken, en houdt de afhandelingstermijn in de gaten. De afdeling(en) die het verzoek betreft worden door hen benaderd. De afdeling handelt het verzoek in principe zelf af, tenzij het over meerdere afdelingen gaat. Dan verzamelt de afdeling Privacy alle informatie en stuurt het besluit naar de betrokkene.

2.1.8 Adviezen van de Functionaris Gegevensbescherming

De gemeente waardeert het toezicht op, en de gevraagde en ongevraagde adviezen over naleving van de AVG en Wpg. Een onafhankelijke blik is nuttig en van toegevoegde waarde voor het voldoen aan nalevingseisen. De Functionaris Gegevensbescherming speelt daarin een belangrijke rol. Door proactief mee te denken over nieuwe projecten en bestaande processen, of advies te geven over uitgevoerde DPIA's. Het draagt bij aan het verbeteren van naleving, en het vertrouwen van burgers te behouden. Het periodiek overleg en de jaarlijkse rapportage draagt bij aan het beleid, en aan het jaarplan Privacy.

2.1.9 Verantwoord inzetten van AI als dat van toegevoegde waarde is

De gemeente erkent de snelle ontwikkelingen op het gebied van AI en de potentiële impact hiervan op de dienstverlening en werkprocessen. We hoeven geen trendsetter zijn, maar er is nieuwsgierigheid naar de mogelijkheden.

AI is geen doel op zich. Het kan een nuttig hulpmiddel zijn, maar brengt ook uitdagingen met zich mee op het gebied van privacy, veiligheid, datagebruik en ethiek. We zien de kansen, maar ook risico's. Het toepassen van AI kan niet ongebreideld. Daarom is er naast toepasselijke wetgeving zoals de AI Act, ook intern beleid ontwikkeld, en zijn er richtlijnen voor het gebruik van generatieve AI. Het DPIA sjabloon is hierop aangepast. In de komende jaren wordt dit verder ontwikkeld tot een Impact Assessment Mensenrechten en Algoritmes (IAMA). Medewerkers worden via het bewustwordingsprogramma voorgelicht over het onderwerp, om zo AI geletterdheid te vergroten. Tevens is een AI-coördinator aangesteld om deze doelen te bereiken. AI gebruik is van toegevoegde waarde indien het de persoonlijke productiviteit bevordert, of als het de effectiviteit van onze (primaire) processen vergroot.

Transparantie, eerlijkheid en het beschermen van de privacy van onze inwoners staan daarbij centraal. Door een weloverwogen aanpak te hanteren, voegt AI niet alleen waarde toe, maar draagt het ook bij aan het vertrouwen van burgers in de gemeente.

Daar waar de gemeente gebruik maakt van AI en/of algoritmes, wordt dat vastgelegd in het verwerkingsregister van de afdeling. Indien het gebruik ervan (mogelijk) een verhoogd risico voor betrokkenen kan inhouden, of impactvol kan zijn, wordt het tevens geregistreerd in het landelijk Algoritmeregister.

2.1.10 Werken met leveranciers die voldoen aan de standaarden

Voor de uitvoering van onze processen zijn we in meer en mindere mate afhankelijk van onze leveranciers. In de meeste gevallen zijn we ten aanzien van gegevensverwerking aan te merken als verwerkingsverantwoordelijke. De gemeente bepaalt het doel en middelen van de verwerking. Leveranciers

verwerken persoonsgegevens in opdracht. Dat betekent dat wij verantwoordelijk zijn voor de gegevensverwerking door de leverancier. Leveranciers worden geselecteerd op basis van wettelijke en marktconforme standaarden op het gebied van privacybescherming en informatiebeveiliging.

Waar nodig worden verwerkersovereenkomsten conform VNG model afgesloten, inclusief (GIBIT) Inkoopvoorwaarden, en worden leveranciers in een vroeg stadium beoordeeld op compliance, beveiliging en relevante certificeringen zoals ISO 27001, NEN 7510 of andere relevante certificeringen of kwaliteitskeurmerken.

In principe laat de gemeente enkel persoonsgegevens verwerken binnen de Europese Economische Ruimte (EER), of in landen waar de Europese commissie een adequaatheidsbeluit voor heeft afgegeven, of een ander passend raamwerk. Indien dit principe om wat voor reden geen stand kan houden, dan zorgen we voor passende waarborgen zoals Binding Corporate Rules of Standard Contractual Clauses. Tevens wordt er een DPIA uitgevoerd om de risico's voor betrokkenen in kaart te brengen en deze, waar mogelijk, te mitigeren tot een acceptabel niveau. Ook moet worden voldaan aan het afwegingskader zoals vastgesteld in de 'Haarlemse cloudvisie'.

2.1.11 Gegevens niet langer dan nodig of wettelijk toegestaan bewaren

Opslagbeperking is een van de beginselen van de AVG. Persoonsgegevens dienen niet langer bewaard te worden dan noodzakelijk of wettelijk verplicht. Als de bewaartermijn afloopt, dienen de gegevens vernietigd te worden. Voor het bewaren en vernietigen van gegevens dient de gemeente rekening te houden met de Archiefwet. Daarom wordt voor de meeste verwerkingen de selectielijst van de VNG gevolgd.

Indien er geen wettelijke bewaartermijn is, worden de adviezen van de Autoriteit Persoonsgegevens gevolgd om een bewaartermijn te bepalen. Dat kan het geval zijn bij verwerkingen die niet voortkomen uit de publieke taak als overheid, maar vanuit de privaatrechtelijke taak als werkgever, die bijvoorbeeld de veiligheid van haar werknemers wil vergroten. De bewaartermijn wordt opgenomen in het verwerkingsregister van de betreffende afdeling.

2.1.12 Het delen en verstrekken van gegevens: als het mag of moet

De gemeente verstrekt of koppelt gegevens in beginsel enkel als het mag of moet, en als het ten dienste staat van de betrokkene. In gevallen waarbij de rechtmatigheid niet expliciet is verankerd in wetgeving, zal per geval gekeken worden wat mogelijk of niet mogelijk is. Hierbij worden de belangen afgewogen, de beginselen van de AVG zoveel mogelijk gerespecteerd, en wordt gekeken naar proportionaliteit en subsidiariteit.

De wens en behoefte om gegevens te verstrekken of te koppelen, zowel intern als extern, neemt toe. Onder andere binnen het sociaal domein, en binnen (gemeentelijke) samenwerkingsverbanden. De behoefte komt voort vanuit de uitvoering van wettelijke taken, ten behoeve van de betrokkene wiens data het betreft. In bepaalde gevallen staat dit op gespannen voet met bijvoorbeeld sectorale of landelijke wetgeving. Dit kan dilemma's creëren op het gebied van gegevensbescherming, dienstverlening, uitvoering van wettelijk opgedragen taken en privacy. De Autoriteit Persoonsgegevens signaleert deze dilemma's ook, en roept de wetgever op ervoor te zorgen dat wetten en regels organisaties in staat stellen om zowel aan de AVG te voldoen als burgers adequaat te helpen. Zij geeft echter ook aan dat dit niet wegneemt dat een grondslag nodig is voor de verwerking.

Soms loopt landelijke wetgeving achter op de uitvoering, of wordt achteraf door de landelijk wetgever een grondslag voor de verwerking gecreëerd om dit op te lossen. Wetgeving zoals de *Wet aanpak meervoudige problematiek sociaal domein* (WAMS) is in ontwikkeling om dit mogelijk te maken[4]. Ook de *Wet gegevensverwerking door samenwerkingsverbanden* (WGS) voor de aanpak van fraude biedt de gemeente deze ruimte.

2.1.13 Gebruik van cookies en tracking technologieën

Bij het aanbieden van onze websites gaan we zorgvuldig en vertrouwelijk om met gegevens van bezoekers. Gemeentelijke websites gebruiken enkel functionele en analytische cookies die geen inbreuk maken op de privacy van bezoekers. Zogenoemde 'tracking' en (re)marketing cookies zijn niet toegestaan. Ook worden er geen persoonsgegevens gedeeld met advertentieplatformen of commerciële partijen voor marketing doeleinden.

4) *Op 18 juni 2025 is de WAMS niet langer controversieel verklaard:https://www.tweedekamer.nl/downloads/document?id=2025D28999*

Waar analytische en functionele cookies worden toegepast, hebben deze tot doel de gebruikerservaring te verbeteren. Dit gebeurt waar mogelijk op basis van anonieme gegevens. De bezoeker wordt bij een eerste bezoek hiervan op de hoogte gesteld, en hierover geïnformeerd in de privacyverklaring.

3. Taken en verantwoordelijkheden

Dit hoofdstuk beschrijft de '*governance*', en heeft betrekking op verschillende aspecten binnen een organisatie en gaat over besturen en beheersen van een organisatie en verantwoordelijkheid en zeggenschap binnen die organisatie: hoe de taken, bevoegdheden en verantwoordelijkheden (TBV) zijn belegd.

De beheersing van privacybescherming sluit aan bij het in de bedrijfsvoering bekende Drie-Lijnen-Model. In dit model zijn de Afdelingsmanagers verantwoordelijk voor de eigen processen in de eerste lijn. De privacy adviseur is de tweede lijn. Die ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn (intern toezicht) wordt het geheel door de Functionaris Gegevensbescherming van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Het borgen van privacybescherming is een continu proces. De gemeente moet periodiek de effectiviteit van de maatregelen beoordelen en waar nodig aanpassen. Daarbij wordt rekening gehouden met veranderende processen, doelgroepen, technische mogelijkheden, privacyregels, wetgeving en maatschappelijke opvattingen en ontwikkelingen.

Bij processen of verwerkingen waar meerdere afdelingen betrokken zijn, is het van belang dat intern duidelijk wordt vastgelegd welke afdeling en manager eigenaar is van het proces als geheel. Dat is doorgaans ook de afdeling die de verwerking opneemt in het verwerkingsregister. Dit voorkomt onduidelijkheden in taken en verantwoordelijkheden op het gebied van privacy en gegevensverwerking.

Afdeling/Functie	Rol/Verantwoordelijkheid	Toelichting
Gemeenteraad	Controlerend	De gemeenteraad heeft een controlerende functie en moet (kunnen) nagaan of het college *'in control'* is bij de uitvoering van de AVG. De raad kan hiervoor specifieke vragen stellen aan het college. Ook informeert de FG de gemeenteraad jaarlijks over de naleving van privacywetgeving door het college.
College van B&W	Verwerkings-verantwoordelijkheid en verantwoording afleggen	Het college van burgemeester en wethouders (B&W) is eindverantwoordelijk voor de bescherming van veruit de meeste gemeentelijke verwerkingen van persoonsgegevens. Het college moet *'in control'* zijn van privacybescherming, zelfs als de gemeente nog niet volledig aan alle AVG-vereisten voldoet. Met het vaststellen van dit beleid, stelt het college haar ambities op het gebied van privacybescherming vast voor de komende jaren. Hiermee geeft zij de richting aan in de gemeente. Dit beleidsplan wordt voorgelegd aan de gemeenteraad. Hiermee wordt transparantie naar inwoners en de gemeenteraad gewaarborgd over de gemeentelijke koers inzake gegevensverwerking. Het college legt verantwoording af aan de gemeenteraad.
Functionaris Gegevensbescherming	Intern Toezicht	Deze voor gemeenten verplichte functionaris houdt intern toezicht op de naleving van de privacywetgeving, zoals de AVG en Wpg. De Functionaris Gegevensbescherming is een wettelijk vastgelegde rol met als taken: • Het verzamelen van informatie over gegevensverwerkingen binnen de organisatie

		• Het analyseren en beoordelen of deze verwerkingen aan de wet voldoen • Het geven van informatie, adviezen en aanbevelingen aan de organisatie De Functionaris Gegevensbescherming opereert onafhankelijk, en mag geen instructies of opdrachten krijgen van het college over de uitvoering van het werk, en is niet persoonlijk aansprakelijk is voor overtredingen van de privacywetgeving binnen de organisatie. Die verantwoordelijkheid voor naleving ligt bij de verwerkingsverantwoordelijke. Naast deze interne toezichthouder, houdt de Autoriteit Persoonsgegevens (AP) op nationaal niveau toezicht op naleving. De Functionaris gegevensbescherming is eerste aanspreekpunt voor de AP. Tevens wordt periodiek gerapporteerd aan de directie, het college en de gemeenteraad.
Directie	Aansturing	De directie zorgt dat alle processen en systemen en de daarbij behorende middelen onder de verantwoordelijkheid vallen van een afdelingsmanager, en zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de staat van de privacybescherming binnen de organisatie. Op die manier kan het college zich verantwoorden aan de raad en andere toezichthouders.
Chief Information Officer (CIO)	Verantwoordelijk	De CIO is eindverantwoordelijk voor de gehele informatievoorziening, het informatiebeheer en ICT en geeft inhoudelijk leiding aan, en wordt ondersteund door een aantal strategisch adviseurs, waaronder de Functionaris gegevensbescherming en de Chief Information Security Officer (CISO). De CIO zorgt voor een visie op de informatievoorziening van de gemeente, en draagt deze uit naar de directie, interne organisatie en de externe omgeving.
Afdelingsmanagers	Uitvoering	De afdelingsmanagers zijn verantwoordelijk voor uitvoering van de gemeentelijke bedrijfsprocessen. Daarmee zijn ze verantwoordelijk voor privacybescherming binnen die processen, de verwerkingen van persoonsgegevens binnen hun domein, en de naleving van wet- en regelgeving. De afdeling is verantwoordelijk deze taken te beleggen binnen de diverse functies van de betreffende afdeling.
Privacy adviseurs	Advies	De privacy adviseurs ondersteunen en adviseren de afdelingen van de domeinen bij de naleving van wet- en regelgeving, en de implementatie van privacybeschermingsmaatregelen. Ook ondersteunen ze bij de dagelijkse borging van privacybescherming binnen de gemeentelijke bedrijfsprocessen. Dit doen ze ook bij

		domein overstijgende en intergemeentelijke vraagstukken. De privacy adviseurs beheren de producten en documenten waarmee de afdelingen worden ondersteund.