PRIVACY BELEID

Vaststelling en periodieke validatie

Vastgestelde versie	**Datum vaststelling**	**Wie**	**Functie**
[4.0]	23-05-2023	Pieter Janssen	Secretaris directeur
Volgende validatie	07-2024		
Classificatie	Openbaar		

Inhoudsopgave

1. Inleiding

Het Hoogheemraadschap van Delfland (verder te noemen: Delfland) werkt bij het uitvoeren van de wettelijke taken en in zijn dienstverlening persoonsgegevens. Dit betreft verwerking van persoonsgegevens van burgers, bestuurders en (keten)partners in uitvoering van wettelijke taken, dienstverlening, belastingheffing, toezicht en handhaving en de organisatie van verkiezingen, maar ook van medewerkers van Delfland.

Naast de wettelijke verplichting en de beheersing van bestuurlijke risico's is vooral het vertrouwen in een zorgvuldige, integere (digitale) publieke dienstverlening voor Delfland van groot belang. Dat betekent dat alle partijen erop moeten kunnen vertrouwen dat Delfland zich houdt aan de wet en dat gegevens zorgvuldig, rechtmatig en op een veilige manier worden verwerkt.

De Algemene Verordening Gegevensbescherming (AVG) van de Europese Unie bevat hiervoor de kaders waaraan Delfland moet voldoen. Delfland geeft door middel van dit beleid een duidelijke richting aan de wijze waarop privacy wordt beschermd: het beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van Delfland. In dit beleid laat Delfland zien op welke manier dagelijks om gegaan wordt met persoonsgegevens en privacy, en wat er wettelijk wel en niet verantwoord is.

Bestuur en management spelen een cruciale rol bij het actief uitdragen van dit privacybeleid. Het privacybeleid van Delfland is in lijn met relevante nationale en Europese wet- en regelgeving.

Dit privacybeleid beschrijft, samengevat, op welke wijze Delfland omgaat met de verwerking van persoonsgegevens en hoe deze worden beschermd.

Delfland heeft dit privacybeleid opgesteld en dit beleid wordt verkort en vereenvoudigd weergegeven in de privacyverklaring. Het privacybeleid en de privacyverklaring zijn onlosmakelijk met elkaar verbonden. Het beleid is het meer uitgewerkte fundament van de verklaring en omgekeerd kan de burger in de verklaring eenvoudig in een oogopslag de belangrijkste elementen hiervan zien. Naast de privacyverklaring voor de burger heeft Delfland voor de medewerkers, sollicitanten en doelgroepgerichte privacy verklaringen opgesteld.

Delfland hanteert bij het verwerken van persoonsgegevens de volgende basisprincipes:

- Delfland verwerkt persoonsgegevens conform de eisen van de AVG;
- Delfland verwerkt persoonsgegevens alleen noodzakelijk voor de dienstverlening aan burgers en organisaties voor de taken die het moet uitvoeren als waterschap;
- Delfland verwerkt persoonsgegevens van zijn medewerkers alleen voor de taken die het moet uitvoeren als werkgever;
- Delfland zorgt ervoor dat de verkregen persoonsgegevens overeenkomen met de doelstellingen waarvoor deze worden verwerkt.

Het beleid is vastgesteld en beoordeeld binnen de organisatie. Het bevat de visie op en de principes waarlangs privacy in Delfland wordt georganiseerd. Het beleid wordt periodiek, of bij relevante, significante wijzigingen van wetgeving beoordeeld op toepasselijkheid op de meest recente ontwikkelingen.

2. Algemeen

2.1 Wettelijk kader

Delfland is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het Privacybeleid. Voor het Privacybeleid gelden onder andere de volgende wettelijke kaders:

- De Algemene Verordening Gegevensbescherming (AVG)
- De Uitvoeringswet Algemene Verordening Gegevensbescherming
- De Wet politiegegevens (Wpg)

In de Europese Unie is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De ruimte die de AVG laat nadere invulling op nationaal niveau te geven is geregeld in de Uitvoeringswet Algemene Verordening gegevensbescherming (UAVG).

De AVG legt een verantwoordingsplicht op aan organisaties die persoonsgegevens verwerken om aantoonbaar te maken dat zij voldoen aan de regels op het gebied van persoonsgegevensbescherming. Delfland verwerkt persoonsgegevens en zal moeten kunnen aantonen:

Welke gegevensverwerkingen plaatsvinden

Dat de verwerkingen aan de belangrijkste beginselen van gegevensverwerking voldoen o.a. rechtmatigheid, transparantie, doelbinding en juistheid

En dat de juiste technische en organisatorische maatregelen zijn genomen om persoonsgegevens te beschermen.

Als bestuursorgaan is Delfland gebonden aan de algemene regels van de Algemene wet bestuursrecht (Awb) en ook gebonden aan de regels die voortvloeien uit onder andere de Waterwet en het Waterschapsbesluit. Regels rondom het bewaren en vernietigen van persoonsgegevens volgen uit de Archiefwet en de Selectielijst Waterschappen. Verder zijn nog de volgende wettelijke kaders van belang:

- Baseline Informatiebeveiliging Overheid (BIO)
- Cyber Security Implementatie Richtlijn (CSIR)

In het kader van de verwerking van persoonsgegeven op grond van de Wet politiegegevens geeft die wet een aan de AVG vergelijkbaar normenkader mee.

2.2 Begrippen

Hieronder een overzicht van gebruikte begrippen waarvan het voor dit beleid noodzakelijk is ze nader te beschrijven en verder niet in het beleid zelf uitgewerkt zijn. Bij de begripsbepalingen is zoveel mogelijk uitgegaan van de definities uit de Algemene Verordening Gegevens Bescherming (AVG). In artikel 4 AVG wordt een aantal begrippen genoemd:

a. *Persoonsgegevens:* Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen. Het gaat hierbij niet alleen om vertrouwelijke gegevens, zoals over iemands gezondheid, maar om ieder gegeven dat te herleiden is tot een bepaald persoon (bijvoorbeeld: naam, adres, geboortedatum), maar ook het zorgvuldig omgaan met het BSN. Naast gewone persoonsgegevens kent de wet ook bijzondere persoonsgegevens. Dit zijn gegevens die gaan over gevoelige onderwerpen, zoals etnische achtergrond, medische gegevens en politieke voorkeuren.

b. *Verwerking:* Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.
c. *Verwerkingsverantwoordelijke:* Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.
d. *Verwerker:* De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.
e. *Betrokkene:* De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.
f. *Gegevensbeschermingseffectbeoordeling: met* een gegevensbeschermingseffectenbeoordeling worden de effecten en risico's van de nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Dit heet ook wel een 'Data Protection Impact Assessment' (DPIA). Binnen Delfland hanteren we het begrip DPIA;

Veilige en zorgvuldige omgang met persoonsgegevens. Verder zijn van voor de invulling van een zorgvuldige omgang met persoonsgegevens de volgende functies/functionarissen van belang:

- FG: functionaris voor de gegevensbescherming, intern toezichthouder op de verwerkingen
- CISO: chief information security officer, organisatie informatiebeveiliging.
- PO privacy officer: adviseur en ondersteuner op de te toetsen producten op operationeel en tactisch niveau.

2.3 Reikwijdte

Het privacybeleid is van toepassing op alle verwerkingen van persoonsgegevens die door of namens Delfland als verwerkingsverantwoordelijke plaatsvinden. Ook is deze van toepassing op de verwerking van persoonsgegevens die door de bijzondere opsporingsambtenaren van Delfland worden verwerkt voor hun opsporingstaak. De verwerking van die persoonsgegevens valt onder het regime van de Wet politiegegevens.

2.4 Verantwoordelijke

Binnen de verantwoordelijkheids- en bevoegdheidsverdeling van Delfland ligt de verwerkers-verantwoordelijkheid bij het dagelijks bestuur. Het dagelijks bestuur stelt het privacybeleid vast en de secretaris-directeur is als hoofd van de ambtelijke organisatie eindverantwoordelijk voor het uitvoeren van het privacybeleid.

2.5 Doelgroep

Het privacybeleid is geschreven voor iedereen die in het kader van zijn werkzaamheden voor of namens Delfland persoonsgegevens verwerkt. Daarnaast is het beleid in te zien voor iedereen die meer informatie willen over de wijze waarop Delfland omgaat met de verwerking van hun persoonsgegevens.

Delfland heeft toezichthoudende en handhavende taken. De Buitengewone opsporingsambtenaren van Delfland verwerken in het kader van de handhavingstaken politiegegevens. Deze politiegegevens hebben op grond van de Wpg een weliswaar eigen, maar met de AVG vergelijkbaar, beschermings en verantwoordingsregime.

Delfland heeft dit privacybeleid opgesteld en dit beleid wordt verkort en vereenvoudigd weergegeven in de privacyverklaring. De privacyverklaring maakt onderdeel uit van het privacybeleid. Naast de privacyverklaring voor de burger heeft Delfland voor de medewerkers en sollicitanten tevens doelgroepgerichte privacy verklaringen opgesteld.

3. Uitgangspunten en normen

3.1 Verwerkingen

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen als genoemd in artikel 4.2 AVG.

- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Alhoewel dit artikel een tal van voorbeelden noemt, is deze lijst zeker niet limitatief. Alles wat gedaan kan worden met persoonsgegevens onder het begrip ‘verwerken’ valt. Het maakt daarbij niet uit of de handeling handmatig of automatisch wordt verricht.

3.2 Persoonsgegevens

Met persoonsgegevens worden bedoeld: 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 identificator (IP-adres) of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

In het kader van haar wettelijke en dienstverlenende taken verwerkt Delfland persoonsgegevens. Dit betreffen bijvoorbeeld de persoonsgegevens die nodig zijn voor het besluiten op aangevraagde (water)vergunningen, of verzoeken om handhaving, of gegevens die worden verwerkt in het kader van het informeren van burgers over lopende projecten ter verbetering of behoud van de waterveiligheid.
Voorbeelden hiervan zijn contactgegevens van inwoners en van organisaties, zoals naam, adres, emailadres en telefoonnummer. Er worden voor deze taken geen bijzondere persoonsgegevens verwerkt.
In het kader zijn handhavingstaken verwerkt Delfland politiegegevens. Deze kennen op grond van de Wpg een weliswaar eigen, maar met de AVG vergelijkbaar, beschermings- en verantwoordingsregime.
Ook gegevens van bestuurders, zodat zij hun taken kunnen uitvoeren en daarvoor ook vergoedingen ontvangen, worden verwerkt.

Als werkgever verwerkt Delfland persoonsgegevens van medewerkers, maar ook van uitzendkrachten en externen die voor Delfland werken voor de personeels- en salarisadministratie. Uit de verantwoordelijkheid van Delfland als werkgever, vloeit voort dat van medewerkers van Delfland naast de normale persoonsgegevens ook bijzondere persoonsgegevens kunnen worden verwerkt. Dit is gebaseerd op een wettelijke grondslag. Medewerkers worden hierover geïnformeerd via de Privacyverklaring voor medewerkers

3.3 Grondslag

De AVG vereist dat een verwerker een rechtmatige grondslag moet hebben om persoonsgegevens te verwerken. Artikel 6 AVG noemt 6 grondslagen, waarvan er altijd één aan te wijzen moet zijn voor een rechtmatige verwerking.

- Nakoming wettelijke verplichting
- Taak van algemeen belang of openbaar gezag
- Toestemming voor verwerking
- Uitvoering van een overeenkomst
- Gerechtvaardigd belang
- Vitaal belang
- Om een verplichting na te komen die in de wet staat
- Voor de uitvoering van een overeenkomst waar de betrokkene onderdeel was;
- Om een ernstige bedreiging voor de gezondheid van de betrokkene te bestrijden;
- Voor de goede vervulling van de waterschapstaken;
- Wanneer de betrokkene toestemming heeft gegeven voor de specifieke verwerking.

3.4 Doelbinding

Delfland verwerkt alleen persoonsgegevens als er sprake is van een van de bovengenoemde grondslagen.
Daarnaast mogen persoonsgegevens alleen verwerkt worden als daarvoor een duidelijk en gerechtvaardigd doel is vastgesteld. De gegevens die voor dit vastgestelde doel worden verwerkt worden niet voor andere doeleinden gebruikt. De doelen waarvoor Delfland persoonsgegevens verwerkt komen voort uit de wettelijke en dienstverlenende taken van Delfland in de rol van overheidsorganisatie of werkgever.

3.5 Rechtmatige verwerking

Het verwerken van persoonsgegevens mag alleen met een grondslag en doelbinding. Daarnaast moet de verwerking ten aanzien van betrokkene transparant en behoorlijk zijn.
De verwerkte persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt en ook niet langer dan nodig (dataminimalisatie).
Ook geldt dat de verwerking proportioneel moet zijn, de gebruikte gegevens en de inbreuk op privacy moeten in verhouding staan. Dan is sprake van een rechtmatige verwerking.

Verder zal Delfland in het licht van bovenstaande dan zorgdragen voor passende organisatorische en technische maatregelen voor een zorgvuldige veilige verwerking. Ook zorgt Delfland voor juistheid, kwaliteit en actualisatie van de gegevens en worden persoonsgegevens niet langer verwerkt dan noodzakelijk is voor het doel van de verwerking. De van toepassing zijnde (wettelijke) bewaar- en vernietigingstermijnen in acht genomen. Persoonsgegevens worden bewaard indien dat wettelijk is toegestaan in een omgeving waarin passende technische of organisatorische maatregelen genomen zijn waardoor de beveiliging ervan gewaarborgd is.

4. Verantwoording door Delfland

Delfland verwerkt persoonsgegevens. De AVG vraagt van de organisatie, ten aanzien van die verwerkingen, zich te verantwoorden en aantoonbaar te maken dat zij voldoen aan de regels op het gebied van persoonsgegevensbescherming.

De Wpg verplicht tot het doen van een periodieke interne audit en een tweejaarlijkse externe audit.

4.1 Informatieplicht

Delfland informeert betrokkenen over welke persoonsgegevens worden verwerkt en hoe deze worden verwerkt. Op de website is het privacystatement opgenomen. Het privacystatement is een verkorte weergave van dit beleid. Daar worden betrokkenen op de hoogte gesteld van de manier waarop Delfland met persoonsgegevens omgaat en staat ook uitleg over de 'rechten van betrokkene'. Delfland informeert betrokkenen over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan Delfland geven, worden zij op de hoogte gesteld van de manier waarop Delfland met persoonsgegevens om zal gaan.

Vaak staat op de aanvraagformulieren vermeld welke gegevens zonder toestemming niet openbaar gemaakt zullen worden. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat Delfland persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt. Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze gegevens voor de eerste keer worden verwerkt.

4.2 Functionaris gegevensbescherming

Delfland heeft een FG en een plaatsvervangend FG aangesteld. De FG is betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de functionaris zijn informeren, adviseren, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de Autoriteit Persoonsgegevens (AP). De FG neemt niet de taken en verantwoordelijkheden op het gebied van bescherming van de privacy van de afdelingen in de organisatie over. De afdelingen hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. Een verwerking van persoonsgegevens wordt eerst aan de FG gemeld voordat de verwerking begint. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en richtlijnen op het gebied van privacy.

Voor vragen over privacy of over deze toelichting kan contact worden opgenomen met de Functionaris Gegevensbescherming van Delfland via: privacy@hhdelfland.nl

4.3 Inzicht in verwerkingen

De AVG legt een verantwoordingsplicht op aan organisaties die persoonsgegevens verwerken om aantoonbaar te maken dat zij voldoen aan de regels op het gebied van persoonsgegevensbescherming. Delfland verwerkt persoonsgegevens en zal moeten kunnen aantonen:

- Welke gegevensverwerkingen plaatsvinden
- Dat de verwerkingen aan de belangrijkste beginselen van gegevensverwerking voldoen o.a. rechtmatigheid, transparantie, doelbinding en juistheid
- Met wie gegevens worden gedeeld.
- En dat de juiste technische en organisatorische maatregelen zijn genomen om persoonsgegevens te beschermen.

4.4 Register van Verwerkingsactiviteiten

Delfland is verantwoordelijk voor het aanleggen en bijhouden van een overzicht van alle verwerkingen waarvan Delfland de verwerkingsverantwoordelijke is in een register. Elke verwerking in het register bevat een beschrijving van wat er tijdens een verwerking plaatsvindt en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, indien van toepassing, de gezamenlijke verwerkingsverantwoordelijke, inclusief de noodzaak voor een (verwerkers)overeenkomst voor uitwisseling persoonsgegevens;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarbinnen de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

4.5 Rechtmatige en zorgvuldige verwerkingen

Voor alle persoonsgegevensverwerkingen geldt dat deze technisch en organisatorisch beveiligd zijn. Daarvoor is een privacy organisatie ingericht volgens de principes van het three lines of defense model. Voor de sturing en monitoring is een DPCA-cyclus ingericht. Er wordt nauw samengewerkt met informatiebeveiliging.

Om privacy zo vroeg mogelijk in processen en ontwikkelingen te borgen worden de principes van privacy by design en by default toegepast. Bij verwerkers voor Delfland worden de eisen ten aanzien van de zorgvuldige verwerking van de persoonsgegevens zoals die gelden voor Delfland, met een verwerkersovereenkomst geborgd. Delfland heeft een datalekprotocol ter afhandeling van incidenten die persoonsgegevens betreffen. Ook wordt voor betrokkenen invulling gegeven aan de uitoefening van hun rechten.

4.5.1 Beveiliging van verwerkte persoonsgegevens

Delfland is verantwoordelijk voor de bescherming van persoonsgegevens. Dit betekent dat Delfland het proces en de organisatie zo moet inrichten dat alle persoonsgegevens passend beveiligd worden. Hiervoor wordt, waar mogelijk, aangesloten bij informatiebeveiligingsbeleid van Delfland en de Baseline Informatiebeveiliging Overheden (BIO) en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

Delfland zorgt ervoor dat de persoonsgegevens die worden verwerkt, geclassificeerd zijn en afdoende zijn beveiligd met technische en organisatorische maatregelen behorende bij de classificatie. Dit moet voorkomen dat persoonsgegevens onwettig kunnen worden verwerkt, dat inzage of verwerking plaatsvindt door iemand die daar geen recht toe heeft. De wijze waarop Delfland dit doet staat vermeld in het informatiebeveiligingsbeleid van Delfland en in een eventueel aanvullend beveiligingsplan specifiek opgesteld voor een proces of registratie.

De medewerkers zijn al, mede op basis van de BIO, verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen. De geheimhoudingsplicht is voor vaste werknemers van Delfland verankerd in de ambtseed of-belofte. Tijdelijke krachten die toegang hebben tot persoonsgegevens moeten een integriteits- en geheimhoudingsverklaring ondertekenen.

4.5.2 Gegevensbeschermingseffectbeoordeling / Protection Impact Assessment (DPIA)

Delfland is op grond van de AVG verplicht een Data Protection Impact Assessment (DPIA) uit te voeren wanneer de verwerking van persoonsgegevens waarschijnlijk *een hoog privacy risico* oplevert. Om te bepalen of een verwerking een *mogelijk hoog privacy risico* oplevert gebruikt Delfland de Privacy Risico Analyse (PRA). Delfland baseert zich daarbij op de negen criteria voor een verplichte DPIA van de Europese privacy toezichthouders en de lijst van de Autoriteit Persoonsgegevens met typen verwerkingen waarvoor een DPIA altijd verplicht is.
Met een DPIA worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Delfland voert deze uit wanneer er sprake is van een geautomatiseerde,

grootschalige verwerking of wanneer er een grootschalige monitoring van openbare ruimten plaatsvindt. Als er bijzondere persoonsgegevens worden verwerkt, kan dit een extra reden zijn om een DPIA uit te voeren. Een DPIA is in het bijzonder gewenst bij verwerkingen waarbij nieuwe technologieën worden gebruikt.

4.5.3 Privacy by design en by default

Om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen bij de ontwikkeling van producten en diensten past Delfland de principes toe van 'privacy by design en by default'. Deze zijn verankerd in de enterprise architectuur. Voor iedere nieuwe verwerking van persoonsgegevens wordt in een vroegtijdig stadium een risico-inventarisatie uitgevoerd ten aanzien van de bescherming van de persoonsgegevens.

4.5.4 Bewaartermijnen en vernietiging

Actief verwijderen van persoonsgegevens
Delfland bewaart de persoonsgegevens niet langer dan nodig is voor de uitvoering van de taken, of zoals vastgelegd in diverse wetten zoals bijvoorbeeld de Archiefwet. Wanneer er nog persoonsgegevens opgeslagen zijn die niet langer nodig zijn voor het bereiken van het doel worden deze zo snel mogelijk verwijderd. Dit houdt in dat deze gegevens vernietigd worden, of zo worden aangepast dat de informatie niet meer gebruikt kan worden om iemand te identificeren. Delfland stelt hiervoor onder andere een bewaartermijnprocedure op.

4.6 Delen van persoonsgegevens met derden

4.6.1 Verwerkersovereenkomst

Soms schakelt Delfland een externe partij in voor het verwerken van persoonsgegevens. In geval van samenwerking met externe partijen waarbij sprake is dat die partij *hoofdzakelijk* is ingeschakeld voor het verwerken van persoonsgegevens, is die partij een verwerker in de zin van de AVG. In dat geval blijft Delfland wel verantwoordelijk voor de verwerking van de persoonsgegevens. Daarom worden met partijen die namens Delfland persoonsgegevens verwerken verwerkersovereenkomsten gesloten met daarin de afspraken. Het sluiten van deze overeenkomsten is verplicht en het standaardmodel van het waterschap is daarin leidend.

In bepaalde gevallen heeft Delfland een partij ingeschakeld om bijvoorbeeld een waterschapsgerelateerd werk uit te voeren, maar is het in het kader van die uitvoering ook nodig dat die partij persoonsgegevens verwerkt. Het verwerken van de persoonsgegevens is in zo'n geval *bijkomstig* aan het hoofddoel van de overeenkomst met de externe partij. Het hoofddoel is namelijk het uitvoeren van het waterschapsgerelateerd werk en niet het verwerken van persoonsgegevens. In zo'n geval zijn er twee verwerkingsverantwoordelijken, zowel Delfland als de ingeschakelde partij. Er wordt dan in een gegevensleveringsdocument afspraken gemaakt over hoe wordt omgegaan met de persoonsgegevens.

In het verwerkingenregister wordt bij de betreffende verwerking de verwerkersovereenkomst of afspraak genoemd.

4.6.2 Samenwerkingsverbanden

Delfland werkt samen in diverse verbanden met andere overheden en organisaties. Indien er tussen deze organisaties doorgifte en/of verwerking van persoonsgegevens plaatsvindt als onderdeel van de overeengekomen samenwerking waarbij beide organisaties beide verwerkersverantwoordelijken zijn, worden er aanvullend op de samenwerkingsovereenkomst, afspraken gemaakt over de uitwisseling van persoonsgegevens. De Regionale Belasting Groep (RBG) en Aquon (beide zijn gemeenschappelijke regelingen waar Delfland in deelneemt) zijn voorbeelden van samenwerkingsverbanden. Deze zelfstandige rechtspersonen zijn eigenstandig verwerkingsverantwoordelijken in de zin van de AVG met betrekking tot het verwerken van persoonsgegevens.

4.6.3 Doorgifte van persoonsgegevens

Delfland geeft geen persoonsgegevens door aan een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

4.6.4 Melden en afhandelen Datalekken

Als er een vermoeden is van een incident met betrekking tot informatiebeveiliging en/of privacy moet dit gemeld worden via Topdesk Selfservicedesk dat openstaat voor alle interne meldingen. Voor externe meldingen is er op de website van Delfland het mailadres (privacy@hhdelfland.nl) van het privacy team beschikbaar.

Er is sprake van een datalek wanneer er een (beveiligings) incident plaatsvindt waarbij persoonsgegevens onrechtmatig worden verwerkt / er een inbreuk is op de beschikbaarheid, vertrouwelijkheid of integriteit van persoonsgegevens. Deze gegevens vallen bijvoorbeeld in handen van derden die geen toegang tot die gegevens mogen hebben of gaan verloren.
De FG bepaalt of sprake is van een datalek.

Delfland heeft een datalekprotocol. Aan de hand daarvan beziet Delfland of het, gelet op omvang, ernst en risico's noodzakelijk is om dit te melden aan de Autoriteit Persoonsgegevens (AP). Indien Delfland heeft besloten dit te moeten melden, dan wordt dit uiterlijk 72 uur nadat er kennis van de inbreuk is genomen, aan de AP gemeld. Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. In het geval dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen, dan meldt Delfland dit aan de betrokkenen in eenvoudige en duidelijke taal. Om toekomstige datalekken te voorkomen worden bestaande datalekken geëvalueerd op initiatief van de FG.

Over meldingen en datalekken wordt periodiek gerapporteerd aan DT en portefeuillehouder en het dagelijks bestuur.

4.7 Rechten van betrokkenen

De AVG bepaalt niet alleen de plichten van degenen die de persoonsgegevens verwerken, maar bepaalt ook de rechten van de personen van wie de gegevens worden verwerkt. Deze rechten worden de rechten van betrokkenen genoemd. Delfland informeert de betrokkenen actief over de verwerkingen en over hun rechten via de algemene website van Delfland.

De rechten van betrokkenen:

Recht op informatie (artikel 13 en 14 AVG)
Betrokkene moet op de hoogte worden gesteld van het feit dat verwerking van zijn persoonsgegevens plaatsvindt of zal plaatsvinden en wat de doeleinden hiervan zijn;

Recht van inzage (artikel 15 AVG)
Betrokkenen hebben het recht te weten of hun betreffende persoonsgegevens worden verwerkt door de verantwoordelijke;

Recht op rectificatie (artikel 16 AVG)
Betrokkene heeft recht op rectificatie van hem betreffende onjuiste persoonsgegevens dan wel het recht een aanvullende verklaring te verstrekken wanneer de verwerking plaatsvindt op basis van onvolledige gegevens;

Recht op gegevensverwijdering/vergetelheid (artikel 17 AVG)
De verwerkingsverantwoordelijke is verplicht persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen;

Recht op beperking van de verwerking (artikel 18 AVG)
Het recht op beperking houdt in dat de persoonsgegevens (tijdelijk) niet verwerkt mogen worden en niet gewijzigd mogen worden;

Recht op overdraagbaarheid/dataportibiliteit (artikel 20 AVG)
Dit recht houdt in dat een betrokkene de gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machineleesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen;

Recht van bezwaar (artikel 21 AVG)
Een betrokkene kan vanwege redenen die verband houden met zijn specifieke situatie gebruik maken van dit recht van bezwaar tegen de verwerking van hem betreffende persoonsgegevens, als voldaan wordt aan de in de verordening genoemde eisen;

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming/profiling (artikel 22 AVG)
Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen.

Verzoek om inzage

Een betrokkene kan bij Delfland een verzoek om inzage van de over hem verwerkte persoonsgegevens door Delfland doen of een beroep doen op een van bovengenoemde rechten. Dit kan door middel van een brief, gericht aan het adres van Delfland, maar ook via privacy@hhdelfland.nl.

Delfland heeft een inzageprotocol om aan het recht van inzage te kunnen voldoen.
Delfland geeft zo snel mogelijk en in ieder geval binnen één maand gevolg aan een verzoek van betrokkenen. Als het een complex verzoek betreft kan deze periode worden verlengd met twee maanden. De betrokkene wordt hierover zo snel mogelijk geïnformeerd en in elk geval binnen één maand na ontvangst van het verzoek.

Voordat Delfland een verzoek in behandeling neemt, vraagt Delfland om identificatie. Delfland wil zeker weten dat de juiste informatie aan de juiste persoon wordt gegeven. Om er zeker van te zijn dat de aanvraag t.a.v. bovenstaande rechten wordt gedaan door de juiste persoon vragen wij om een afspraak te maken op ons hoofdkantoor, Phoenixstraat 32 in Delft, voor identificatie van de betrokkene. Mocht deze niet in de gelegenheid zijn om naar ons hoofdkantoor te komen, dan kunnen wij in overleg ook een afspraak op een andere locatie afstemmen.

4.8 Privacy bewuste organisatie

Medewerkers van Delfland zijn zich bewust van de noodzaak om persoonsgegevens van medewerkers en burgers veilig en discreet te behandelen. Medewerkers zijn en worden getraind in het beschermen van persoonsgegevens en aspecten van informatiebeveiliging. Voor nieuwe medewerkers wordt viermaal per jaar informatiesessie gehouden over privacy en informatiebeveiliging. Delfland evalueert de effectiviteit van de trainingen.

Er is ook een onlinetraining informatiebeveiliging en privacy voor alle medewerkers. Deelname is niet verplicht maar het beleid is dat het management deelname stimuleert. Op teamniveau wordt de ontwikkeling van het deelnamepercentage gemonitord. Er is generiek trainingsmateriaal dat voor iedereen beschikbaar is. In 2023 komt er daarnaast maatwerk; er wordt lesmateriaal ontwikkeld voor specifieke doelgroepen binnen het waterschap. Met als doel de participatie en kennis te verhogen.

5. Gerelateerde zaken

5.1 Wet open overheid (WOO)

Op grond van de Wet open overheid bestaat de mogelijkheid om een verzoek om informatie in te dienen bij Delfland. Per verzoek wordt deze op de privacyaspecten bekeken. Bij beantwoording van het worden informatie en documenten waar nodig geanonimiseerd.

5.2 Wet hergebruik van overheidsinformatie

De Wet hergebruik van overheidsinformatie regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij het verzoek bekijkt Delfland of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen.

5.3 Informatie over de inzet van camera's

Bij de locaties van Delfland worden camera's ingezet ter beveiliging van personen, gebouwen en goederen. Deze beelden mogen alleen voor dit doel worden gebruikt. Hiertoe worden alleen de openbaar toegankelijke ruimtes en de uitgangen gefilmd. Bij de ingang van een gebouw met cameratoezicht wordt gewezen op het cameratoezicht. De beelden worden na vier weken gewist.

5.4 Cookies

Binnen het waterschap wordt ook gebruikgemaakt cookies (Google Analytics). Het Cookiebeleid van Delfland staat vermeld op de website.

5.5 Big data en tracking

Door middel van Big dataonderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, Delfland wordt uitgevoerd. De verzamelde gegevens door Big dataonderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig zijn voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd en/of geanonimiseerd worden zodat zij niet (direct) herleidbaar zijn tot een persoon.

6. Privacy governance

Om te borgen dat privacybeleid niet een dode letter wordt en de uitvoering ervan stelselmatig wordt geëvalueerd voor verbeteringen hanteert Delfland de zogenaamde Plan Do Check Act cyclus (PDCA-cyclus):

- Plan: planvorming, beleidsvorming, risicoanalyse
- Do: implementatie
- Check: monitoring, evaluatie en controle
- Act: nemen van maatregelen ter verbetering

Bij de uitvoering van de PDCA wordt aangesloten op het bestaande risicomanagement, en de planning & control cyclus van Delfland.

Plan - en beleidsvorming en risicoanalyse

De cyclus start met Privacybeleid, gebaseerd op wet- en regelgeving (AVG), landelijke normen zoals de BIO en best practices. Dit beleid wordt uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving (privacyplan). Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. Vaktechnische- dan wel afdelingsspecifieke activiteiten worden bij voorkeur opgenomen in jaarplannen van vak afdelingen of afdelingsspecifieke plannen. Prioritering geschiedt op basis van een risicoanalyse.

De coördinatie van het organisatiebrede risicomanagement is bij Delfland belegd bij de afdeling concern control & auditing. Privacy is daar onderdeel van.

Het analyseren van de risico's heeft tot doel:

- Inzicht te krijgen in de kwaliteit en de effectiviteit van de bestaande beveiligingsmaatregelen voor bescherming persoonsgegevens.
- Inzicht te krijgen in de risico's die de realisatie van het gewenste beveiligingsniveau voor persoonsgegevens in gevaar kunnen brengen.
- Inzicht krijgen in de risicobereidheid.
- Het gewenste niveau van informatiebeveiliging vast te stellen in de vorm van een classificatie van bedrijfsprocessen, informatiesystemen en gegevensverzamelingen.
- Keuzes te kunnen maken voor het beheersen van risico's t.a.v. persoonsgegevens.
- Prioriteiten te bepalen voor de verbetering van de bestaande situatie.

Do- Implementatie:

Op basis van de uitkomsten van de risicoanalyse wordt een maatregelenplan opgesteld. In dit plan worden de verbeteractiviteiten op projectmatige wijze vastgelegd. Dit resulteert in een privacy jaarplan dat door de FG en privacy officer(s) wordt opgesteld en door de Secretaris-Directeur wordt vastgesteld. Dit plan is onderdeel van de planning & control cyclus van Delfland.

Aan de hand van het privacyjaarplan wordt de implementatie van de aanvullende privacy maatregelen uitgevoerd. Dit plan bestaat uit maatregelen t.a.v. de algemene AVG vereisten. Daarnaast bestaat dit plan uit de maatregelen die zijn voortgekomen uit de risicoanalyse. Het privacy jaarplan kan bestaan uit de reguliere validatie van het register van verwerkingen, uitvoeren van DPIA's, bewustwordingsactiviteiten voor medewerkers. Dit betekent onder andere het opstellen van richtlijnen en procedures voor privacy, het voorlichten en opleiden van management en medewerkers. Bij de uitvoering van de PDCA-cyclus wordt aangesloten bij de bestaande decentrale risicomanagementsystematiek en audit.

Check -Monitoring, evaluatie en controle:

Monitoring betreft het bewaken, evalueren en controleren van de privacy processen voor persoonsgegevens. Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van privacy processen, informatie en ICT en compliance aan wet- en regelgeving. Externe controle betreft de controle (buiten het primaire proces) door een auditor. Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van

dergelijke onderzoeken uitgevoerd. Bevindingen worden opgenomen in de rapportage door de FG. Indien nodig wordt het privacybeleid hierop tussentijds bijgesteld.
Daarnaast wordt de wetgeving worden gemonitord op ontwikkelingen. Dit is een taak van de FG en moet minimaal jaarlijks te worden uitgevoerd. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen of de evaluatie van een eventueel datalek, aanleiding geven om het privacybeleid te heroverwegen. Een dergelijke beoordeling vindt minimaal eenmaal per jaar plaats en wordt geïnitieerd door de FG.

Delfland richt een Privacy Control Framework (PCF) in voor de evaluatie en controle van de privacy processen. Daarnaast voert Delfland regelmatig audits uit op de privacy processen. Dit betreft zowel interne audits en externe audits. Naar aanleiding van de audits wordt een verbeterplan opgesteld en uitgevoerd.

Act - nemen van maatregelen ter verbetering:

De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en (eventueel) externe controle. De cyclus is een continu proces, waarbij de bevindingen van controles input vormen voor het privacybeleid, de jaarplanning en privacy plannen.

De bevindingen worden in beginsel gerapporteerd aan de directie; voor ingrijpende verbeteracties wordt een verbetervoorstel gedaan. Maatregelen die voortkomen uit de diverse audits en risico-analyses worden geprioriteerd en vastgelegd in het Information Security Management Systeem (ISMS). De uitvoering van de maatregelen is de verantwoordelijkheid van de afdelingsmanagers. Hierover wordt twee keer per jaar gerapporteerd door de FG.

7. Organisatie van privacy

In dit privacybeleid worden de rollen en verantwoordelijkheden op hoofdlijnen beschreven. Onderstaand overzicht geeft een overzicht van de privacy activiteiten op hoofdlijnen weer.

Niveau	Activiteit	Verantwoordelijke	Documentatie	Monitor / Naleving
Strategisch	Beleidsvorming	Dagelijks Bestuur/dijkgraaf	Privacybeleid	FG Interne Audit
Tactisch	Planning	Directieteam / SD	Privacyjaarplan	FG Interne Audit
Operationeel	Uitvoering	Lijnmanagement	Richtlijnen en maatregelen	FG Interne Audit

Op strategisch niveau vindt de beleidsvorming met betrekking tot informatiebeveiliging en privacy plaats. Het dagelijks bestuur is verantwoordelijk voor de vaststelling van het privacybeleid en wordt hierin ondersteund door de FG. Voor de verdere uitwerking van het beleid en de uitvoering is de secretaris-directeur verantwoordelijk.

De planning van de activiteiten met betrekking tot privacy vormt het tactische niveau. Deze activiteit valt onder de verantwoordelijkheid van de directeur van het desbetreffende organisatieonderdeel. De directeur wordt hierin geadviseerd door de FG. Het privacy jaarplan is het meet- en stuurinstrument dat bij deze planning wordt ingezet.

De uitvoering van activiteiten met betrekking tot privacy vindt plaats op operationeel niveau. Eerstverantwoordelijke voor deze activiteit is het lijnmanagement. Het lijnmanagement wordt daarbij ondersteund door de privacy officer(s).

In de verdeling van taken rollen en verantwoordelijkheden in de privacy processen wordt bij het Hoogheemraadschap van Delfland het principe van het ‘three lines of defense’ model gevolgd. De FG, CISO en PO vallen onder de afdeling Concern Control en Auditing (CCA).

De eerste lijn of defense

Het dagelijks bestuur (DB) van Delfland stelt het privacybeleid van Delfland vast. Het verwerken van persoonsgegevens behoort tot de dagelijkse aangelegenheden van Delfland. Het nemen van besluiten en het uitoefenen van bevoegdheden op grond van de AVG behoren daarmee tot de verantwoordelijkheid van het dagelijks bestuur. De feitelijke uitvoering van de werkzaamheden gebeurt binnen de (ambtelijke) lijnorganisatie. De ambtelijke lijnorganisatie bestaat uit een SD, directeuren, afdelings-, asset- en programmamanagers en medewerkers.

De ambtelijke lijnorganisatie van Delfland is verantwoordelijk voor de uitvoering van het verwerken van persoonsgegevens en dat dit compliant aan de AVG gebeurt binnen de processen en conform het privacybeleid van Delfland.

Als onderdeel van de 1ste lijn wordt de proceseigenaar ondersteund door een privacy officer voor de processen met verwerking van persoonsgegevens die onder zijn of haar verantwoordelijkheid vallen.

De tweede lijn of defense

Er is een 2de lijn die de 1ste lijn adviseert en controleert of het management daadwerkelijk zijn verantwoordelijkheden vervult t.a.v. privacy. Deze rol is belegd bij de FG. Hierbij heeft de FG onafhankelijke positie en rapporteert rechtstreeks aan de voorzitter van het DB, de dijkgraaf, de leden van het directieteam (DT) en de Autoriteit Persoonsgegevens (AP) indien dit naar eigen oordeel van de FG nodig is.

De derde lijn of defense

De derde verdedigingslinie is de functie die controleert of de interactie en coördinatie tussen de 1ste lijn en 2de lijn naar behoren werkt en geeft een objectieve, onafhankelijke mening hierover met mogelijkheden voor verbetering. Dit kan via 'self-assessments', interne audits en externe audits. Deze functie wordt intern uitgevoerd door Concern Control en Audit van Delfland en opereert vanuit een onafhankelijke positie ten opzichte van de andere organisatieonderdelen van Delfland.

Informatiebeveiliging

Voor de bescherming van de persoonsgegevens is het Informatiebeveiligingsbeleid mede van toepassing. Daarom is er op alle drie de niveaus een nauwe samenwerking en afstemming tussen de FG en de CISO om een goede taakverdeling met betrekking tot privacybescherming en informatiebeveiliging binnen Delfland te waarborgen.

Privacy Handboek

Voor de verdere onderliggende details over de verdeling van de taken, rollen en verantwoordelijkheden in de uitvoering van de privacy processen heeft Delfland een Privacy Handboek opgesteld. Daarin is de beschrijving opgenomen hoe Delfland het naleven van het privacybeleid van Delfland, het beoordelen en monitoren van zijn activiteiten en processen vormgeeft.

8. Slotbepalingen

Dit beleid treedt in werking met ingang van de eerste dag na bekendmaking in het Waterschapsblad en wordt aangehaald als Privacybeleid 2023 Hoogheemraadschap van Delfland.

Het privacybeleid van Delfland wordt, indien de ontwikkelingen daartoe nopen aangepast en vastgesteld, maar tenminste iedere drie jaar beoordeeld op actualiteit en opnieuw vastgesteld.

Het privacybeleid Hoogheemraadschap van Delfland 2022 is vastgesteld in de vergadering van het dagelijks bestuur van het Hoogheemraadschap van Delfland 23-05-2023. Daarmee is het Privacybeleid Hoogheemraadschap van Delfland, zoals vastgesteld op 10 december 2019, vervallen.

ir. P.C. Janssen
Secretaris-directeur

dr. P.H.W.M. Daverveldt
Dijkgraaf