Hoogheemraadschap van Delfland

Privacybeleid

Hoogheemraadschap van Delfland

Versie 2.0 – Definitief

Classificatie - Openbaar

10 december 2019

Inleiding

Bij het uitvoeren van de wettelijke taken werkt het Hoogheemraadschap van Delfland veel met persoonsgegevens. Dat gaat niet alleen om persoonsgegevens van burgers, maar ook om de gegevens van medewerkers en (keten)partners. Al deze partijen moeten erop kunnen vertrouwen dat Delfland zorgvuldig met deze gegevens omgaat. De Algemene Verordening Gegevensbescherming (AVG) van de Europese Unie bevat hiervoor de kaders waaraan Delfland moet voldoen. Maar bovenal is het zorgvuldig omgaan met persoonsgegevens ook onlosmakelijk verbonden met een integere overheid.

Nieuwe ontwikkelingen op het terrein van technologie, innovatie, globalisering en een steeds meer digitaal werkende overheid stellen stevige eisen aan de bescherming van persoonsgegevens. Delfland is zich hier van bewust en zorgt dat de persoonsgegevens worden beschermd door onder andere maatregelen te nemen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

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.

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 en sollicitanten tevens doelgroepgerichte privacyverklaringen opgesteld.

Basisprincipes

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 ze verwerkt worden.

Hoofdstuk 1 Algemeen

Wetgeving
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)
- Uitvoeringswet Algemene Verordening Gegevensbescherming

Begripsbepalingen (artikel 4 AVG)

a. *Betrokkene:* De persoon op wie de persoonsgegevens betrekking hebben. De betrokkene is degene van wie de gegevens worden verwerkt.

b. *Verwerker:* De persoon of organisatie die de persoonsgegevens verwerkt in opdracht van een andere persoon of organisatie.

c. *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.

d. *Gegevensbeschermingseffectbeoordeling:* Met een gegevensbeschermingseffectbeoordeling 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 meer gebruikelijke begrip DPIA.

e. *Verwerkingsverantwoordelijke:* Een persoon of instantie die alleen, of samen met een ander, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt.

f. *Verwerking:* Een verwerking is alles wat je met een persoonsgegeven doet, zoals: vastleggen, bewaren, verzamelen, bij elkaar voegen, verstrekken aan een ander, en vernietigen.

Reikwijdte
Het beleid is van toepassing op alle verwerkingen van persoonsgegevens die namens Delfland als verwerkingsverantwoordelijke plaatsvinden.

Verantwoordelijke
Binnen de verantwoordelijkheids- en bevoegdheidsverdeling van Delfland ligt de verwerkersverantwoordelijkheid 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.

Hoofstuk 2 Verwerkingen

Verwerkingen (Artikel 4, AVG)
De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:

- 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

Doeleinden (Artikel 5, AVG)
Volgens de wet mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. Delfland verwerkt alleen persoonsgegevens met een duidelijk en gerechtvaardigd omschreven doel. De gegevens worden niet voor andere doelen verwerkt. Deze doelen zijn gebaseerd op de (wettelijke) taken van Delfland voor burgers en organisaties en van Delfland in de rol van werkgever.

Categorieën van persoonsgegevens
Delfland verwerkt persoonsgegevens voor de uitoefening van de diverse waterschapstaken. Voorbeelden hiervan zijn contactgegevens van inwoners en contactpersonen van organisaties, zoals naam, adres, emailadres en telefoonnummer. Deze gegevens worden via verschillende manieren verkregen. Ze worden aangeleverd om gebruik te kunnen maken van de diverse diensten en producten zoals bijvoorbeeld vergunningaanvragen. Er worden hiervoor geen bijzondere persoonsgegevens verwerkt (artikel 9, AVG).

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.

Rechtmatige grondslag (Artikel 6, AVG)
De wet zegt dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag uit de wet van toepassing moet zijn. Delfland verwerkt alleen persoonsgegevens met een rechtmatige grondslag:

- 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.

Wijze van verwerking
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Delfland zorgt ervoor dat persoonsgegevens zoveel mogelijk verzamelt bij de betrokkene zelf. Delfland verwerkt alleen persoonsgegevens wanneer het doel niet op een andere manier kan worden bereikt.

In de wet wordt ook gesproken over proportionaliteit. Delfland verwerkt alleen persoonsgegevens als dat in verhouding staat tot het doel. Delfland kiest altijd voor het gebruik van zo min mogelijk persoonsgegevens in relatie tot het te bereiken doel.

Hoofdstuk 3 Plichten van Delfland

Informatieplicht (Artikel 13,14, AVG)
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.

Aanstellen van een Functionaris voor gegevensbescherming (FG) (Artikel 37 t/m 39, AVG)
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). Het is niet de bedoeling dat de functionaris de taken op het gebied van bescherming van de privacy van de afdelingen in de organisatie overneemt. 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

Register van verwerkingen (Artikel 30, AVG)
Delfland is verantwoordelijk voor het aanleggen en bijhouden van een register van alle verwerkingen waarvan Delfland de verwerkingsverantwoordelijke is. Elk 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.

Beveiliging (Artikel 32, AVG)
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.

Privacy by design en by default (Artikel 24, AVG)
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. Voor iedere nieuwe verwerking van persoonsgegevens wordt een risico-inventarisatie uitgevoerd ten aanzien van de bescherming van de persoonsgegevens.

Gegevensbeschermingseffectbeoordeling (Artikel 35, AVG)
Met een gegevensbeschermingseffectbeoordeling ofwel 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.

Verwerkersovereenkomsten (artikel 28 AVG)
Met partijen die namens Delfland persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten. Het sluiten van deze overeenkomsten is verplicht. In deze overeenkomsten is onder meer geregeld met welk doel en op welke wijze de persoonsgegevens mogen worden verwerkt, welke veiligheidsmaatregelen er getroffen moeten worden, waar de persoonsgegevens worden opgeslagen, de mogelijkheden om een audit uit te voeren en of de verwerker subverwerkers (andere partijen die namens hen weer persoonsgegevens verwerken) mag inschakelen. Verder is in de overeenkomst geregeld hoe partijen omgaan met datalekken en wie de schade die door een datalek ontstaat, zal vergoeden en hoe de overeenkomst eindigt en wat er dan met de verwerkte persoonsgegevens gebeurt.

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 verwerkersverantwoordelijke zijn, worden er aanvullend op de samenwerkingsovereenkomst, afspraken gemaakt over de uitwisseling van persoonsgegevens.

Melden en afhandelen datalekken (Artikel 33, 34, AVG)
We spreken van een datalek wanneer persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben. Wanneer er een datalek heeft plaatsgevonden of er is een vermoeden daarvan, beziet Delfland of het, gelet op omvang, ernst en risico's noodzakelijk is dit te melden aan de Autoriteit Persoonsgegevens (AP). Indien er sprake is van een dergelijk datalek en Delfland heeft besloten dit te moeten melden bij de AP, wordt dit uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, aan de AP gemeld. Als dit later dan 72 uur is, wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval 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.

Doorgifte (Artikel 44 t/m 50, AVG)
Delfland geeft geen persoonsgegevens door met een land buiten de Europese Economische Ruimte (EER) of een internationale organisatie.

Wet openbaarheid van bestuur (Wob)
Via de Wob (en straks wellicht de Wet Open Overheid) bestaat de mogelijkheid om een verzoek om informatie in te dienen bij Delfland. Bij het reageren op het verzoek zorgt Delfland ervoor dat de over te leggen documenten waar nodig geanonimiseerd zijn.

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.

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.

Informatie over de inzet van camera's
Er worden bij de locaties van Delfland camera's ingezet ter beveiliging van personen en goederen. Deze beelden worden alleen voor dit doel gebruikt. Hiertoe worden alleen de openbaar toegankelijke ruimtes en de uitgangen gefilmd. Bij de ingang van het gebouw wordt er gewezen op het cameratoezicht. De beelden worden na vier weken automatisch gewist.

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.

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. Hierbij wordt onderscheid gemaakt in de specifieke aard van de activiteiten waar de persoonsgegevens worden verwerkt. Delfland evalueert de effectiviteit van de trainingen.

Hoofdstuk 4 Rechten van betrokkenen

De wet 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 ook wel de rechten van betrokkenen genoemd.

Delfland informeert de betrokkenen actief over de verwerkingen en over hun rechten. Hiervoor is een privacyverklaring opgenomen op de website van Delfland. Delfland biedt via de privacypagina op zijn website de mogelijkheid voor het uitoefenen van hun rechten van betrokkenen via: privacy@hhdelfland.nl.

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.

De rechten van betrokkenen bestaan uit de volgende rechten:

Recht op informatie (artikel 13 en 14 AVG) -Een 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 gegevenswissing/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/dataportabiliteit (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.

Hoofdstuk 5 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 de bestaande risicomanagement- en de planning & control cyclus van Delfland.

Plan - en beleidsvorming en risicoanalyse
In het privacybeleid worden de doelstellingen en uitgangspunten voor de bescherming van persoonsgegevens van Delfland vastgelegd. Hiermee vormt het beleid de leidraad voor de overige stappen van het managementsysteem.

De volgende stap is de risicoanalyse. De risicoanalyse is bij Delfland belegd bij de afdeling concerncontrol. 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.
- 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.

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 privacyjaarplan dat door de FG en privacy officer(s) wordt opgesteld en door de Secretaris-Directeur wordt vastgesteld. Dit plan is onderdeel van de planning & controlcyclus van Delfland.

Aan de hand van het privacyjaarplan wordt de implementatie van de aanvullende privacymaatregelen 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 privacyjaarplan kan bestaan uit de reguliere validatie van het register van verwerkingen, uitvoeren van DPIA's, bewustwordingactivteiten voor medewerkers. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het voorlichten en opleiden van management en medewerkers. Diverse activiteiten hebben een nauw raakvlak met de informatiebeveiliging. Hiervoor heeft Delfland een Informatiebeveiligingsbeleid opgesteld.

Monitoring, evaluatie en controle
Monitoring betreft het bewaken, evalueren en controleren van de privacyprocessen voor persoonsgegevens. Daarnaast moet ook 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 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.

Act
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 op kwartaalbasis gerapporteerd.

Hoofdstuk 6 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 privacyjaarplan 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).

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 privacyprocessen heeft Delfland een Privacy Handboek opgesteld.

Hoofdstuk 7 Slotbepalingen

Dit beleid treedt in werking met ingang van de eerste dag na bekendmaking in het Waterschapsblad.

Dit beleid wordt aangehaald als Privacybeleid Hoogheemraadschap van Delfland.

Ieder jaar wordt het privacybeleid beoordeeld om de noodzaak van eventuele aanpassingen vast te stellen.

Vastgesteld in de vergadering van het dagelijks bestuur van het Hoogheemraadschap van Delfland d.d. 10 december 2019.

ir. P.C. Janssen
Secretaris-directeur

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