Waterschap Rivierenland

WATERSCHAPSBLAD

Officiële uitgave van het dagelijks bestuur van het Waterschap Rivierenland

Nr. 7423
30 juni
2022

Privacybeleid Waterschap Rivierenland 2022

Het College van Dijkgraaf en Heemraden van Waterschap Rivierenland

gelet op de desbetreffende bepalingen van de Waterschapswet en het algemeen reglement voor Waterschap Rivierenland;

besluit:

1. kennis te nemen van de evaluatie van het "Privacybeleid Waterschap Rivierenland 2018";
2. het "Privacybeleid Waterschap Rivierenland 2018" in te trekken;
3. het navolgende "Privacybeleid Waterschap Rivierenland 2022" vast te stellen.

PRIVACYBELEID WATERSCHAP RIVIERENLAND 2022

1. Inleiding

1.1 Aanleiding

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) rechtstreeks van toepassing in alle lidstaten van de Europese Unie. De AVG beschermt enerzijds de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Anderzijds legt de AVG-verplichtingen op aan organisaties die persoonsgegevens verwerken. Eén van die verplichtingen is het vaststellen van privacy beleid.
Het verwerken van persoonsgegevens is geen kernactiviteit van Waterschap Rivierenland, maar een afgeleide van of ondersteunend aan de primaire processen. In dat verband werkt iedere medewerker van het waterschap in meer of mindere mate met persoonsgegevens. De persoonsgegevens hebben betrekking op enerzijds gegevens van burgers en anderzijds op gegevens van collega's, waaronder ook worden verstaan persoonsgegevens van bedrijven en organisaties waarmee het waterschap samenwerkt.
Met het vaststellen van privacy beleid wil Waterschap Rivierenland in control zijn voor wat betreft het omgaan met persoonsgegevens. Naast een goede beveiliging en verantwoord gebruik van persoonsgegevens, waarbij wordt voldaan aan wet- en regelgeving, worden privacy risico's geïnventariseerd en worden passende maatregelen genomen. In het privacy beleid geeft waterschap Rivierenland op organisatorisch- en strategisch niveau duidelijkheid over de keuze van de inrichting van privacy om te waarborgen dat de verwerking op een rechtmatige wijze plaatsvindt. Daarmee voldoet het waterschap aan de in de AVG opgenomen verantwoordingsplicht.
Op 18 september 2018 (registratienummer 2018070632) heeft Waterschap Rivierenland het "Privacy beleid Waterschap Rivierenland 2018" vastgesteld. Dit beleid is op 14 november 2018 bekendgemaakt in het Waterschapsblad van Waterschap (Nr. 11239). Het is goed gebruik om beleid na verloop van tijd te evalueren en waar nodig te actualiseren.

1.2 Privacy visie

Ten aanzien van de privacy hanteert het waterschap de volgende visie:
"Als overheidsorganisatie heeft Waterschap Rivierenland wettelijk taken waarvoor het noodzakelijk is om persoonsgegevens te verwerken. Op ons rust een belangrijke verantwoordelijkheid om zorgvuldig om te gaan met deze persoonsgegevens, zowel van de inwoners van ons werkgebied als van onze collega's, zowel medewerkers als bestuurders. Daarbij houden we ons vanzelfsprekend aan de wet. Maar naast de wettelijke bepalingen laten we ook ethiek meewegen in onze keuzes. We stellen ons, vooral bij gevoelige verwerkingen, niet alleen de vraag of het mag, maar ook of het deugt. Het vertrouwen van onze ingelanden is een groot goed en mag niet geschaad worden door onrechtmatige, onjuiste of onzorgvuldige verwerking van persoonsgegevens."

1.3 Ambitieniveau

Waterschap Rivierenland verwerkt weinig bijzondere persoonsgegevens. De schaalgrootte van deze verwerkingen mag, in verhouding tot andere overheden zoals bijvoorbeeld gemeenten of belastingsamenwerkingen, als beperkt worden gezien. Weliswaar kennen we een aantal gevoelige processen, denk aan grondzaken, handhaving of de personeelsadministratie, maar er is geen noodzaak om de bescherming integraal tot het hoogste beschermingsniveau op te voeren.
Het devies hierbij is dat het voldoende is indien aan de in de privacywetgeving opgenomen vereisten wordt voldaan. Ongeacht de noodzakelijke zwaarte van de beveiliging moet compliance worden geborgd. De volwassenheid van de processen bepaalt de mate waarin we in-control zijn. Voor het bepalen van de volwassenheid van (persoons-)gegevensbescherming binnen Waterschap Rivierenland gebruiken we het Capability Maturity Model (CMM).

In november 2019 is de opdrachtgeverstafel akkoord gegaan met het Programmaplan Informatieveiligheid en Privacy 2020-2024 (versie 0.8), waarin de ambitie is vastgelegd om de BIO en de AVG in “opzet en bestaan” per 1 januari 2022 aantoonbaar te hebben geïntegreerd in de bedrijfsvoering van de waterschappen (volwassenheidsniveau 3). Tevens is in dit programmaplan de lange termijnambitie opgenomen om “de werking” van de implementatie van de BIO en de AVG in de bedrijfsvoering van de waterschappen per 1 januari 2025 aantoonbaar op volwassenheidsniveau 4 (beheersing) te hebben.

1.4 Doel van het privacy beleid

Zoals uit voorgaande privay visie volgt, heeft Waterschap Rivierenland vanuit zijn wettelijke en dienstverlenende taken te maken met het verwerken van persoonsgegevens van derden, haar eigen medewerkers en bestuurders. In dit verband kan onder andere worden gedacht aan het verlenen van vergunningen, de personeelsadministratie en het behandelen van bezwaren, klachten en aansprakelijkstellingen. Door toenemende samenwerking met (overheids-)partners neemt de ketenverwerking van persoonsgegevens toe. Het is daarom belangrijk inzicht te hebben waar persoonsgegevens (zich in de organisatie) bevinden en wie verantwoordelijk is voor de verwerking ervan.
Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik en tegen verlies dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij Waterschap Rivierenland.
Het privacybeleid is dan ook van belang voor alle medewerkers, betrokkenen en organisaties waarmee het waterschap samenwerkt. Het heeft consequenties voor het werk van alle medewerkers die met persoonsgegevens werken. Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het waterschap, waaronder alle bestuursleden, medewerkers, bezoekers en externe relaties.- Het privacybeleid wordt, bij aanvang van de werkzaamheden voor het waterschap, met hen gedeeld, waarbij ook wordt ingegaan op de vraag wat dit beleid voor deze werkzaamheden betekent.
Het privacybeleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren, waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid. Daarnaast geeft het privacybeleid medewerkers en andere betrokkenen inzicht in de wijze waarop is beschreven hoe het waterschap omgaat met privacy. Verder helpt het privacybeleid bij het creëren van bewustwording over het belang en de noodzaak van het verantwoord omgaan met en het beschermen van persoonsgegevens. As gevolg daarvan kunnen betrokkenen er op vertrouwen dat Waterschap Rivierenland op een zorgvuldige en veilige manier omgaat met persoonsgegevens.

1.5 Reikwijdte privacy beleid

Privacy is een breed begrip om het (grond)recht op de persoonlijke levenssfeer van een individu te beschrijven. Daaronder vallen niet alleen persoonsgegevens, maar ook fysieke en sociale aspecten. Dit beleid richt zich in eerste instantie op de informationele privacy, omdat de privacywetgeving zich daar op richt. Informationele privacy betekent bescherming van personen in verband met de informatie die over hen bekend is en ten aanzien van hen wordt toegepast.
Het privacy beleid is van toepassing op de hele organisatie, alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar het waterschap verantwoordelijk voor is. Bij de implementatie van dit geactualiseerde beleid zullen de proceseigenaren, systeemeigenaren, gegevenseigenaren en medewerkers van het waterschap worden betrokken.
Van het privacybeleid zijn strafrechtelijke- en belastinggegevens uitgesloten. Ten aanzien van strafrechtelijke gegevens geldt namelijk niet de AVG, maar de Europese Richtlijn gegevensbescherming politie en justitie en de Wet politiegegevens (Wpg). Hieronder vallen ook de taken ter bescherming van de openbare veiligheid.
Dit betekent dat medewerkers van het waterschap bij de uitoefening van hun taken als buitengewoon opsporingsambtenaar (BOA) gehouden zijn aan voornoemde richtlijn en wet.
Ten aanzien van belastinggegevens gelden de bepalingen van de Algemene wet inzake rijksbelastingen (AWR). Tevens dient bij belastinggegevens rekening te worden gehouden met de omstandigheid dat de heffing en de inning door het waterschap slechts is beperkt tot de leges. De overige waterschapsbelastingen worden namelijk op basis van delegatie opgelegd en geind door Belastingsamenwerking Rivierenland (BSR, een gemeenschappelijke regeling met een openbaar lichaam), waarvan Waterschap Rivierenland één van de deelnemers is. Door deze delegatie zijn alle bevoegdheden en verplichtingen aangaande de overgedragen waterschapsbelastingen overgegaan op BSR, zodat BSR zelfstandig verantwoordelijk is voor het naleven van de AVG en de fiscale wetgeving inzake privacy en geheimhouding.
Tot slot ziet dit privacybeleid niet op de informatieveiligheid, aangezien daar een apart beleidsdocument voor is opgesteld.

1.6 Leeswijzer
In dit privacy beleid wordt in hoofdstuk 2 eerst ingegaan het van toepassing zijnde juridisch kader. Vervolgens wordt in hoofdstuk 3 ingegaan op het organisatorische kader. In hoofdstuk 4 wordt ingegaan op de toepassing van het privacy beleid in de praktijk. In hoofdstuk 5 wordt vervolgens ingegaan op de uitgangspunten en de richtlijnen die van toepassing zijn bij de verwerking van persoonsgegevens. De implementatie van het privacy beleid binnen de organisatie van het waterschap komt in hoofdstuk 6 aan de orde. De rechten voor betrokkenen komen in hoofdstuk 7 aan de orde. In hoofdstuk 8 wordt ingegaan op het omgaan met incidenten inzake persoonsgegevens. Tot slot wordt in hoofdstuk 9 ingegaan op de verantwoordingplicht die het waterschap in het kader van de AVG heeft.

2. Juridisch kader

2.1 De Algemene verordening gegevensbescherming en de Uitvoeringswet AVG
De bescherming van persoonsgegevens is verankerd in de Grondwet, het Europees Verdrag voor de rechten van de Mens (EVRM) en het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR). De regels over hoe om te gaan met dit grondrecht zijn met ingang van 25 mei 2018 opgenomen in de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG).
De AVG is van toepassing op de gehele of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
Op de volgende verwerkingen is de AVG echter niet van toepassing:
- het verwerken van persoonsgegevens door een natuurlijke persoon in het kader van een louter persoonlijke of huishoudelijke activiteit;
- verwerking van persoonsgegevens geregeld bij of krachtens de Wet Basisregistratie personen;
- verwerking van persoonsgegevens door politie en justitie als zij hun taken voor de opsporing en vervolging van strafbare feiten en tenuitvoerlegging van straffen uitvoeren. Daarvoor geldt de Europese Richtlijn gegevensbescherming politie en justitie en de Wet Politiegegevens (WPG). Hieronder vallen ook de taken ter bescherming van de openbare veiligheid. Dit betekent dat medewerkers van het waterschap bij de uitoefening van hun taken als buitengewoon opsporingsambtenaar (BOA) gehouden zijn aan voornoemde richtlijn en wet.

2.2 Overige wetgeving
In diverse bijzondere wetten, die ook voor het waterschap relevant zijn, zijn ook regels met betrekking tot privacy opgenomen. Zo bevatten bijvoorbeeld de Telecommunicatiewet, de Archiefwet, de Algemene wet inzake rijksbelastingen, het Wetboek van Strafrecht en de Wet basisregistratie personen afwijkende en/of aanvullende eisen ten aanzien van de privacy.
De betreffende bijzondere wetten dienen in onderlinge samenhang met de AVG te worden bezien. Over het algemeen geldt als uitgangspunt dat de AVG van toepassing is als algemene wet, waarvan de bepalingen echter niet van toepassing zijn indien er bijzondere wetgeving geldt.

2.3 Beleidsdocumenten Waterschap Rivierenland
Diverse interne beleidsstukken hebben een relatie met het privacy beleid of zijn hier een nadere uitwerking van. Daar waar in dit privacy beleid wordt verwezen naar een zorgvuldige omgang met persoonsgegevens of de bescherming van privacy wordt verondersteld dat het privacy beleid daaraan ten grondslag ligt. In dit verband wordt onder meer verwezen naar het Protocol personeelsvolgsystemen, de gedragscode integriteit voor medewerkers, de gedragscode gebruik online en offline middelen, de richtlijnen voor gebruik van sociale media, de uitvoeringsregeling integriteitsbeleid en de servicenormen van het waterschap. Tot slot wordt in dit verband verwezen naar het informatiebeveiligingsbeleid van Waterschap Rivierenland.

2.4 Jurisprudentie
Naast wet- en regelgeving vormt ook de jurisprudentie een belangrijke bron voor de bescherming van privacy. In jurisprudentie wordt immers nader duiding gegeven aan wet- en regelgeving, hetgeen gevolgen kan hebben voor de wijze waarop de dagelijkse werkzaamheden binnen het waterschap worden verricht.

3. Organisatorisch Kader

3.1 Inleiding
De feitelijke verwerking van persoonsgegevens vindt plaats in de hele organisatie. Het is daarom van belang om binnen de organisatie duidelijk aan te geven wie waarvoor verantwoordelijkheid draagt. Binnen Waterschap Rivierenland worden verschillende rollen met bijbehorende taken en verantwoor-

delijkheden onderkend. Uiteindelijk is het zorgvuldig omgaan met persoonsgegevens een verantwoordelijkheid voor iedereen in de organisatie van het waterschap.
Ten einde als waterschap te voldoen aan de AVG zijn ten aanzien van de privacy (informatiebeveiliging valt buiten dit beleid) verschillende rollen met bijbehorende verantwoordelijkheden onderscheiden.

3.2 Het College van dijkgraaf en heemraden
Het College van dijkgraaf en heemraden (CDH) is eindverantwoordelijk voor de rechtmatige, zorgvuldige en transparante verwerking van persoonsgegevens binnen het waterschap. Dit geldt ook voor de verwerkingen van persoonsgegevens die ter beschikking worden gesteld aan derden of worden gedeeld in samenwerkingsverbanden.
Het CDH stelt het beleid, de uitvoeringsmaatregelen en de procedures vast op het gebied van verwerkingen van persoonsgegevens met inachtneming van de aanbevelingen van de Functionaris Gegevensbescherming.
Het CDH bevordert de beschikbaarheid van voldoende middelen om uitvoering van het privacy beleid te waarborgen. Naleving van de privacywetgeving is de uitdrukkelijke verantwoordelijkheid van het College van dijkgraaf en heemraden en niet van de Functionaris Gegevensbescherming.

3.3 Portefeuillehouder privacy
Het CDH wijst uit haar midden een portefeuillehouder Privacy aan die bestuurlijk verantwoordelijk is voor de uitvoering van het privacy beleid en de controle en de naleving daarvan. De portefeuillehouder Privacy is ambassadeur voor het uitdragen van het belang van een goede organisatie van privacy en ziet erop toe dat privacy een vast onderdeel van de bedrijfsvoering wordt.

3.4 Teamleiders
De teamleiders zijn verantwoordelijk voor de verwerkingen en het beheer van persoonsgegevens die plaatsvinden binnen hun team op de betreffende afdeling. De teamleiders zijn medeverantwoordelijk voor het creëren van bewustwording en de naleving van het privacy beleid binnen de werkprocessen van de eigen afdeling.

3.5 Systeemeigenaar /functioneel beheerder
Iedere systeemeigenaar of functioneel beheerder is verantwoordelijk voor zijn applicatie en bijbehorende ICT-faciliteiten. De systeemeigenaar of functioneel beheerder moet er voor zorgen dat de applicatie blijft beantwoorden aan de eisen van de wet- en regelgeving, waaronder de privacywetgeving.

3.6 Chief Information Security Officer
De Chief Information Security Officer (CISO) is eindverantwoordelijk voor de informatieveiligheid, dat raakvlakken heeft met privacy.

3.7 Information Security Officer
De Information Security Officer (ISO) wordt geconsulteerd bij de implementatie van het privacy beleid, aangezien het zorgvuldig omgaan met persoonsgegevens onderdeel uitmaakt van wet- en regelgeving op het gebied van de informatiebeveiliging.

3.8 Communicatieadviseur
De communicatieadviseur draagt zorg voor de uitvoering van het awareness programma privacy binnen de organisatie.

3.9 Privacy ambassadeur
Een privacy ambassadeur (PA) is een medewerkers op een afdeling of binnen een team waar veelvuldig met persoonsgegevens wordt gewerkt. De privacy ambassadeur is de eerst aan te spreken persoon voor medewerkers van de betreffende afdelingen/teams. Deze functionaris heeft affiniteit met en kennis van de privacywetgeving en stimuleert de actieve toepassing van het privacy beleid van WSRL in de werkprocessen van de afdeling/het team.

3.10 Medewerker Waterschap Rivierenland
Het succes van het in achtnemen van privacyaspecten in de dagelijkse praktijk is voor het overgrote deel afhankelijk van de medewerkers van Waterschap Rivierenland. Ten einde dit succes zo groot mogelijk te maken, worden de medewerkers regelmatig geïnformeerd en getraind met betrekking tot privacyaspecten.

3.11 Verbonden partijen
Waterschap Rivierenland werkt bij de aan haar opgedragen taken veel samen met andere partijen om te komen tot een efficiëntere uitvoering van taken. Een dergelijke samenwerking kan op verschillende manieren invulling worden gegeven. Een samenwerking kan bijvoorbeeld vorm worden gegeven door

het sluiten van een samenwerkingsovereenkomst met één of meer andere partijen. Een zwaardere vorm van samenwerking is het laten uitvoeren van taken door zogenaamde 'Verbonden Partijen'. Deze partijen zijn organisaties waaraan Waterschap Rivierenland zich bestuurlijk én financieel verbindt om aan het waterschap opgedragen taken uit te voeren. Bij welke verbonden partijen het waterschap deelneemt, is opgenomen in de "Nota Governance verbonden partijen", die als bijlage onderdeel uitmaakt van de begroting en de jaarrekening. De verbonden partijen zijn ieder zelf verantwoordelijk voor het voldoen aan de privacywetgeving. In de reguliere overlegstructuren stelt Waterschap Rivierenland het belang om te voldoen aan de privacywetgeving aan de orde.

3.12 Functionaris Gegevensbescherming

Binnen waterschap Rivierenland is een Functionaris Gegevensbescherming (FG) aangesteld en als zodanig aangemeld bij de toezichthouder privacy, de Autoriteit Persoonsgegevens (AP). Als plaatsvervangend FG zijn de privacy officers aangewezen.
De wettelijke taken van de FG zijn het informeren en adviseren van het betrokken personeel, het houden van toezicht op de naleving van de AVG, de advisering m.b.t. gegevensbeschermingseffect-beoordelingen (GEB's) en samenwerking met en contactpersoon voor de AP.
De FG moet worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens en heeft toegang tot alle persoonsgegevens die in de organisatie in omloop zijn en de diverse verwerkingsactiviteiten die daarmee gepaard gaan. Het waterschap ondersteunt de FG bij de uitvoering van de taken die hem zijn toebedeeld volgens de AVG.
De FG heeft in de eerste plaats de rol van intern toezichthouder. Daarnaast heeft de FG een adviserende en coördinerende rol en fungeert als klankbord voor medewerkers en als contactpersoon en aanspreekpunt in de richting van de Autoriteit Persoonsgegevens.
De FG moet zijn taken onafhankelijk uit kunnen voeren. Dit betekent dat hij geen instructies mag krijgen over de uitvoering van de taken. De FG heeft een toezichthoudende rol en toetst hoe de bescherming van persoonsgegevens binnen het waterschap wordt opgepakt. De FG is niet betrokken bij de operationele uitvoering. De FG heeft een bijzondere rechtspositie: hij geniet ontslagbescherming voor de uitvoering van zijn taken (net zoals de leden van de OR). De FG rapporteert over zijn taken aan het College van dijkgraaf en heemraden. Vanwege zijn onafhankelijke rol is de functie van FG binnen WSRL belegd bij het Team Concerncontrol.
Concreet heeft de FG de volgende taken:

- Het informeren en adviseren van de organisatie en de verwerkers die namens WSRL persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van de AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van het beleid van WSRL (als verwerkingsverantwoordelijke) of de verwerker(s) met betrekking tot de bescherming van persoonsgegevens;
- Het toezien op toewijzing van verantwoordelijkheden, bewustwording en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Het geven van advies met betrekking tot de gegevensbeschermingseffectbeoordeling (GEB) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- Het bijhouden van het register van geconstateerde en gemelde datalekken;
- Toezien op de juistheid en de volledigheid op het register van verwerkingsactiviteiten;
- Jaarlijks rapporteren over de stand van zaken;
- Het samenwerken met de Autoriteit Persoonsgegevens;
- Het optreden als contactpunt voor de Autoriteit Persoonsgegevens.
- Het optreden als contactpersoon voor betrokkenen;

De FG heeft geen formele sanctiebevoegdheden, maar het waterschap ondersteunt de FG met de volgende maatregelen:

- De FG is bevoegd om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen om zijn wettelijke taken5 uit te voeren. Hiertoe maakt de FG eigen keuzes, zonder instructie over de uitvoering van zijn werkzaamheden;
- De FG is over de uitvoering van zijn taken tot geheimhouding en vertrouwelijkheid gehouden.

3.13 Privacy Officer

Om te voorkomen dat een FG zich te veel met uitvoerende taken bezighoudt en daarmee in feite mogelijk zijn eigen werkzaamheden controleert, worden deze taken bij Waterschap Rivierenland uitgevoerd door een Privacy Officer (PO). De Privacy Officer rapporteert aan en werkt nauw samen met de FG. De rol van Privacy Officer wordt bij Waterschap Rivierenland uitgevoerd door twee juristen uit het Team Bestuurs- en Juridische Zaken (T-BJZ). De verschillende uitvoerende taken zijn over deze twee personen verdeeld, met dien verstande dat zij elkaars werkzaamheden kunnen uitvoeren.

Naast het adviseren en het bijstaan van de FG en het in behandeling nemen van meldingen van datelekken hebben de privacy officers de volgende taken:
- het schrijven, het evalueren en het actualiseren van het privacy beleid;
- het begeleiden van de organieke inbedding van het privacy beleid binnen de organisatie van het waterschap;
- het invullen van het privacy risicomanagement (Privacy by Design en de DPIA);
- het bewaken van doelbinding bij gegevensverwerkingen;
- het periodiek actualiseren van het register van verwerkingen;
- het invullen van het privacy kwaliteitsmanagement;
- het verstrekken van informatie over het verwerken van persoonsgegevens aan betrokkene;
- het begeleiden van betrokkene bij het inroepen van een recht, zoals opgenomen in de AVG;
- het bewaken van termijnen voor het bewaren van persoonsgegevens;
- het adviseren over de doorgifte van persoonsgegevens aan derden;
- het registeren en het behandelen van meldingen van (mogelijke) datalekken.

3.14 Privacy team
Het privacyteam van Waterschap Rivierenland bestaat uit drie personen, te weten de FG en de twee PO's. Zij overleggen periodiek over privacyaangelegenheden, in het kader van de privacy te gebruiken documenten en bespreken privacyincidenten (meldingen van (mogelijke) datalekken. Waar nodig vindt bijvoorbeeld ook afstemming plaats met de collega's die betrokken zijn bij ICT indien het gaat om de beveiliging van persoonsgegevens alsmede met de afdeling OMC indien het gaat om de bewustwording van de privacyaspecten die met de dagelijkse werkzaamheden voor het waterschap zijn verbonden. Het privacyteam is bereikbaar via privacy@wsrl.nl

4. Toepassing privacybeleid in de praktijk

4.1 Inleiding
In het privacy beleid worden de kaders voor het omgaan met persoonsgegevens vastgelegd. Sommige onderwerpen zijn nader uitgewerkt in afzonderlijke regelingen, zoals het Protocol personeelsvolgsystemen en de Procedure Meldplicht Datalekken.
Daarnaast wordt in het beleid verwezen naar gedragscodes en richtlijnen die door de Autoriteit Persoonsgegevens zijn vastgesteld en waarin de uitvoering van de AVG nader wordt geconcretiseerd.
Het privacy beleid is te beschouwen als een levend document, dat regelmatig aangevuld en/of gewijzigd kan worden.

4.2 Privacy Baseline
In de Privacy Baseline van het Centrum Informatiebeveiliging en privacybescherming (CIP) zijn de eisen van de AVG vertaald naar concrete, hanteerbare normen die duidelijk maken wat er van organisaties wordt verlangd op beleids-, uitvoerings- en control (beheers)niveau om te voldoen aan de wettelijke verplichtingen en daarmee de privacy van burgers te borgen. Door het in acht nemen van de criteria van de Privacy Baseline wordt voldaan aan de specifieke doelen van privacybescherming: afscherming, corrigeerbaarheid en transparantie. Deze begrippen zijn in de Privacy Baseline als volgt omschreven:
Afscherming:
Zorgt ervoor dat persoonsgegevens niet op een onrechtmatige manier kunnen worden verwerkt, zoals het gebruiken, doorgeven of koppelen van persoonsgegevens voor andere doelen dan de oorspronkelijke of voor onbekende doeleinden.

Corrigeerbaarheid:
Tijdens en na elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens en de uitkomsten van de verwerking aan te passen, indien deze niet voldoen aan de doelverbinding of de kwaliteitsvereisten en daardoor de betrokkenen (kunnen) benadelen.

Transparantie:
Voor, tijdens en na elke verwerking van persoonsgegevens is er duidelijkheid over de doelverbinding, de wettelijke grondslag en de organisatorische en technische inrichting van de verwerking van persoonsgegevens.

Bij het implementeren van het privacy beleid zijn deze criteria uit de Privacy Baseline van het CIP als uitgangpunt genomen.

4.3 Privacy risico's
Bij de beschreven privacy visie past alleen maar een terughoudende risicobereidheid waar het gaat om de omgang met persoonsgegevens. Betrokkenen hebben geen keuze in hun relatie met het waterschap. Het waterschap handelt op grond van wettelijk toebedeelde taken en bevoegdheden en treedt

soms diep binnen in de persoonlijke levenssfeer. Denk aan het verwerven van grond of onroerende zaken bij ingrepen in het landschap. Zorgvuldigheid is hierbij geboden. De risicobereidheid van WSRL als het gaat om de verwerking van persoonsgegevens moet gesteld worden op "terughoudend".
Naast terughoudendheid dient te worden voorkomen dat de volgende situaties zich (gaan) voordoen:

- illegale gegevensverwerking: gebruik, opslag of uitwisseling van informatie is bij wet verboden.
- disproportionele gegevensverwerking: gebruik, opslag of uitwisseling van informatie is
  (a) ontoereikend of juist overmatig of
  (b) het organisatiebelang bij de gegevensverwerking is onevenredig klein terwijl de impact op personen onevenredig nadelig kan zijn.

- irrelevante gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie dient geen bedrijfsdoel, doet niet ter zake of is verouderd.
- onnauwkeurige gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie is
- geen juiste weergave van de werkelijkheid.
- onveilige gegevensverwerking: de gebruikte, opslagen of uitgewisselde informatie dreigt te
- gemakkelijk toegankelijk te zijn voor onbevoegden, gemanipuleerd te worden of onbeschikbaar te zijn.
- niet-inachtneming van bijzondere wettelijke voorschriften: bij gebruik, opslag of uitwisseling
- van informatie worden formele verplichtingen veronachtzaamd.
- onbewaakte gegevensverwerking: de proceseigenaar verzuimt om te controleren of de privacy-waarborgende maatregelen daadwerkelijk zijn geëffectueerd of te evalueren in hoeverre zijn proces bijstelling behoeft.

4.4 Gedragsnormen

Ten einde voornoemde situaties te voorkomen verwacht het college van dijkgraaf en heemraden van de proceseigenaren een rechtmatige en een zorgvuldige verwerking van persoonsgegevens. Proceseigenaren kunnen hiervoor rekenen op support van het privacyteam.
Het college voert een voorwaardenscheppend beleid teneinde binnen Waterschap Rivierenland een privacybestendige cultuur te realiseren. Proceseigenaren voorzien in passende organisatorische en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen ('privacywaarborgen') en documenteren die maatregelen in de werkinstructies. Proceseigenaren zijn verantwoordelijk voor de volledigheid en actualiteit van het 'register van verwerkingen'.
Het college is transparant over de bedrijfsvoering, de gegevensverwerking en de privacybeleidsvoering en faciliteert de uitoefening van rechten door personen over wie het waterschap gegevens verwerkt. Proceseigenaren verlenen hieraan hun medewerking. Het college en proceseigenaren dragen het belang uit van privacybeleidsvoering en geven zelf het goede voorbeeld. Zo maken zij privacy bespreekbaar. En bij dilemma's gaan zij de dialoog aan met doelgroepen over wie persoonsgegevens worden verwerkt.

4.5 Risicomanagement

Het niet voldoen aan de privacywetgeving kan verregaande gevolgen hebben voor zowel betrokkenen als ook het waterschap.
Verkeerd gebruik, misbruik of verlies van persoonsgegevens kan een behoorlijke impact hebben op iemands zakelijke- en/of privéleven en kan leiden tot aanzienlijke (materiele en/of immateriële) schade. Het kan van invloed zijn op iemands reputatie, leiden tot discriminatie, identiteitsfraude, financiële verliezen, verlies van vertrouwelijkheid van gegevens, verlies van bedrijfsgeheimen en verhindering om rechten en/of vrijheden uit te oefenen.
Voor Waterschap Rivierenland kan het niet voldoen aan de privacywetgeving (of zelfs de schijn daarvan) leiden tot negatieve publiciteit en imagoschade. Daarnaast kan het leiden tot juridische consequenties, zoals:

- een door de rechter opgelegd verbod op het handelen van de organisatie en de verplichting tot het treffen van herstelmaatregelen bij (dreiging van) schade;
- vergoeding van de schade die de betrokkene heeft geleden;
- een bindende aanwijzing, opgelegd door de Autoriteit Persoonsgegevens om binnen een termijn de aanwijzing op te volgen;
- een bestuurlijke boete, opgelegd door de Autoriteit Persoonsgegevens tot maximaal 20 miljoen euro;
- een last onder bestuursdwang of dwangsom opgelegd door de Autoriteit Persoonsgegevens.

Wat bepaalt het risico?

- Grootschaligheid van de verwerking, zowel in aantal betrokkenen als hoeveelheid informatie
- De aard of gevoeligheid van de te verwerken persoonsgegevens
- De impact op de persoonlijke levenssfeer van betrokkenen

Hoog risicoverwerkingen:
- Handhaving (WPG)
- Personeelsadministratie
- Volgsystemen in auto's en
- Volgsysteem mobiele apparatuur

Verhoogd risico:
- Grondzaken
- Vergunningen en toezicht (AVG)
- Juridische zaken
- (Grote) projecten in de publieke ruimte
- Calamiteitenzorg

Laag risico verwerkingen:
- Contacten met burgers over routinewerkzaamheden, meldingen, incidenten zonder schade,
- Contacten met andere belanghebbende overheden en georganiseerde partijen

4.6 Privacy by Design

Met privacy by Design en privacy by Default wordt zo goed mogelijk invulling gegeven aan de bescherming van de privacy van betrokkenen. Bij Privacy by design wordt reeds bij de start van het ontwerpen van een product of dienst rekening gehouden met de privacy van betrokkenen. Het doel is om de bescherming van persoonsgegevens te optimaliseren.
De zeven basisprincipes voor privacy by design zijn:

1. Preventief in plaats van reactief. Zorg dat privacy risico's zo klein mogelijk blijven, door vooraf over deze risico's na te denken en maatregelen te treffen. Het voorkomen van privacy inbreuken staat centraal.
2. Privacy is de standaard (default). Producten en diensten worden standaard ingesteld om de hoogste mate van privacy te bieden. Privacy is als het ware ingebouwd in de systemen.
3. Gegevensbescherming en beveiliging (privacy) integreren in het ontwerp. Zorg ervoor dat privacy een kerncomponent wordt van de producten of diensten, zonder afbreuk te doen aan het product of dienst.
4. Volledige functionaliteit. Door privacy in de ontwikkelingsfase in te bouwen in de systemen is er geen afweging nodig tussen de beveiliging en privacy of tussen privacy en andere functionaliteiten.
5. Bescherming gedurende de hele levenscyclus van de persoonsgegevens. Alle persoonsgegevens worden veilig opgeslagen en op een juiste manier vernietigd na afloop van de bewaartermijn.
6. Zichtbaarheid (openheid) en transparantie. Dit geeft vertrouwen bij alle betrokken partijen.
7. Respect voor privacy van de betrokkene. De belangen van de betrokkenen staan op de eerste plek door het aanbieden van sterke standaard instellingen, transparantie, duidelijke communicatie en gebruiksvriendelijke mogelijkheden.

Privacy by design betekent niet alleen het inbouwen van privacy in systemen, maar ook in werkprocessen, de managementstructuur en in het netwerk. Voorbeelden zijn:

- Persoonsgegevens zijn standaard niet openbaar zichtbaar en worden waar nodig en kan versleuteld. Als dit niet kan, dan worden eventueel (extra) beveiligingsmaatregelen genomen.
- Keuzevakjes op websites zijn niet standaard aangevinkt indien deze de verwerking van persoonsgegevens mogelijk maken.
- De algemene inkoopvoorwaarden bevatten geen clausules die nadelige gevolgen kunnen hebben voor de privacy van betrokkenen.
- Bij de ontwikkeling van software worden betrokkenen over de verwerking van persoonsgegevens geïnformeerd en op hun rechten geattendeerd.
- Bij het ontwerpen/de aanschaf wordt stilgestaan bij welke persoonsgegevens daadwerkelijk nodig zijn voor het doel waarvoor de gegevens nodig zijn.
- Door logische toegangsbeveiliging zijn persoonsgegevens alleen zichtbaar voor die medewerkers die deze vanuit hun functie nodig hebben.
- Persoonsgegevens worden niet onnodig lang bewaard. Bij privacy by design wordt rekening gehouden met bewaartermijnen tijdens het ontwerpen van het te gebruiken systeem.
- Bij testen worden geen persoonsgegevens gebruikt; alleen geanonimiseerde gegevens.
- Er wordt altijd gedacht vanuit het belang van de betrokkene (zowel voor de Beschikbaarheid, Integriteit als Vertrouwelijkheid). Daarbij hoort ook de controle die een betrokkene zelf kan uitvoeren (uitvoering van de rechten).
- Persoonsgegevens worden altijd via een vertrouwd netwerk verzonden en bij voorkeur versleuteld.
- Bij opslag van gegevens buiten het waterschap (SAAS-oplossing) worden maatregelen genomen om de beveiliging van persoonsgegevens op orde te hebben.

- Bij risicovolle informatieprocessen wordt vooraf een data protection impact analyse (DPIA) uitgevoerd.
- Er worden passende technische en organisatorische privacy verhogende maatregelen getroffen. Hierbij wordt gekeken naar de stand van de techniek voor de te nemen maatregel en de uitvoeringskosten.
- De aanschaf (of ontwikkeling) van nieuwe informatiesystemen wordt vooraf getoetst door de changeboard. Naast de technische eisen en de informatiebeveiligingseisen uit de BIO wordt hierbij tevens rekening gehouden met de privacyaspecten. Bovenstaande richtlijnen zijn hiervoor de hoofdlijnen.

4.7 Privacy bij default

Privacy by default is een onderdeel van privacy by design, waarbij als uitgangspunt geldt dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn. Daardoor worden alleen die persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel.

5. Uitgangspunten en richtlijnen bij de verwerking van persoonsgegevens

5.1 Inleiding

Als algemeen uitgangspunt bij de verwerking van persoonsgegevens door Waterschap Rivierenland geldt dat persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Daarbij dient een goede balans te worden gevonden tussen het belang van het waterschap om persoonsgegevens te verwerken en het belang van betrokkene om eigen keuzes te maken met betrekking tot zijn persoonsgegevens.

5.2 Uitgangspunten

Om aan het hiervoor beschreven algemene uitgangspunt invulling te geven, gelden de volgende uitgangspunten:

- een verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals die zijn opgenomen in artikel 6 van de Algemene Verordening Gegevensbescherming (‘rechtmatigheid’);
- persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de betrokkene behoorlijk en transparant is, hetgeen inhoudt dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Informatie en communicatie daarover dient eenvoudig toegankelijk en begrijpelijk te zijn (‘behoorlijkheid en transparantie’);
- persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, waarbij het gaat om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven alvorens een aanvang wordt gemaakt met de verwerking van persoonsgegevens. Daarbij geldt dat persoonssgegevens niet worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (‘doelbinding’);
- de verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze als gevolg waarvan de hoeveelheid en het soort gegevens beperkt blijkft tot de gegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (‘minimale gegevensverwerking’);
- er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn (‘juistheid’);
- persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (‘integriteit en vertrouwelijkheid’);
- persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, waarbij de van toepassing zijnde bewaar- en vernietigtermijnen in acht worden genomen (‘opslagbeperking’).

5.3 Richtlijnen

Bij de verwerking van persoonsgegevens worden naast voornoemde uitgangspunten de volgende richtlijnen toegepast:

1. Er is bewustzijn dat de verwerking van persoonsgegevens aan wettelijke voorschriften is gebonden.
2. Persoonsgegevens worden alleen verwerkt voor het in het register vastgelegde doel, te weten het doel waarvoor ze verkregen zijn en voor doelen die daarmee verenigbaar zijn.
3. Indien je afdeling/team persoonsgegevens verwerkt of gaat verwerken zorg er dan voor dat daarover vooraf wordt gecommuniceerd door middel van een privacyverklaring. Het privacy team kan daarin, samen met team communicatie, adviseren en begeleiden.
4. Iedere verwerking van persoonsgegevens kent een verwerkingsverantwoordelijke, veelal de proceseigenaar. De verwerkingsverantwoordelijke wijst een gegevensbeheerder aan.

5. Er worden alleen persoonsgegevens verwerkt voor zover die noodzakelijk zijn voor het doel van de verwerking en niet meer gegevens dan deze. Bijzondere persoonsgegevens, bijvoorbeeld over gezondheid, worden niet door het waterschap verwerkt, tenzij daartoe een verplichting bestaat.
6. Alleen medewerkers die de gegevens voor hun werk nodig hebben, hebben toegang tot de gegevens.
7. Indien een externe partij wordt ingeschakeld voor de verwerking van persoonsgegevens, stel dan vast welke rol deze partij heeft (verwerkingsverantwoordelijke of verwerker), zorg indien van toepassing voor een verwerkersovereenkomst of passende contractuele afspraken over de verwerking. Het privacy team kan daarin adviseren en begeleiden;
8. Persoonsgegevens worden alleen gebruikt en bewaard op de daarvoor aangewezen locaties en systemen, in een voldoende beveiligde omgeving.
9. Indien de persoonsgegevens niet meer nodig zijn en er geen noodzaak is om ze te bewaren, dan worden deze gegevens verwijderd. Ook van de apparaten en uit de systemen.
10. Bij de (wijziging van de) verwerking van persoonsgegevens dan wel het aanvangen van een nieuwe verwerking van persoonsgegevens is er het bewustzijn dat er mogelijk risico's zijn voor betrokkenen. Ten einde deze risico's weg te nemen dan wel zo veel mogelijk te beperken, worden risico's door middel van een quickscan en waar nodig via Dpia's in kaart gebracht. Het privacy team kan daarin adviseren en begeleiden Op basis van deze risico-analyse worden afspraken gemaakt over de te nemen maatregelen om de risico's weg te nemen dan wel zo veel mogelijk te beperken. Er wordt zorgvuldig omgegaan met de persoonsgegevens en indien er onverhoopt iets misgaat, dan wordt dat gemeld overeenkomstig de daarvoor vastgestelde procedure voor datalekken.
11. Persoonsgegevens worden uitsluitend aan derden doorgegeven indien daarover afspraken zijn gemaakt dan wel daartoe een verplichting bestaat. Neem voor de verdere behandeling van dat verzoek contact op met het privacy team via privacy@wsr.nl
12. Niet alles is in regels vast te leggen. Los van bovenstaande spelregels, wordt op een verstandige en zorgvuldige manier omgegaan met alle persoonsgegevens die beschikbaar zijn om de werkzaamheden te kunnen uitvoeren.
13. Indien je een verzoek van iemand krijgt waarin een beroep wordt gedaan op de uitoefening van een in de AVG opgenomen recht, neem dan voor de verdere behandeling van dat verzoek contact op met het privacy team via privacy@wsr.nl
14. Zorg dat je periodiek deelneemt aan trainingen over privacy. Mocht je meer willen weten over privacy of trainingsmogelijkheden neem dan contact op met het privacy team via privacy@wsr.nl

6. Implementatie privacybeleid

6.1 Algemeen

Na vaststellingvan het privacybeleid dient dit beleid in de organisatie van het wtaerschap te worden geimplementeerd. Om dit te realiseren, vindt afstemming plaats met lde teamleiders, aangezien deze leidinggevenden de verantwoordelijkheid dragen voor een zorgvuldige verwerking van persoonsgegevens binnen hun team. Deze verantwoordelijkheid omvat ook de keuze van de maatregelen alssmede de uitvoering en de handhaving van deze maatregelen. Waterschap Rivierenland heeft daarmee in het kader van het zorgvuldig en veilig omgaan met persoonsgegevens gekozen voor een lijnverantwoordelijkheid.

6.2 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om het bewustzijn bij alle medewerkers voortdurend aan te scherpen, zodat kennis van privacy risico's wordt vergroot en het zorgvuldig en rechtmatig verwerken van persoonsgegevens wordt aangemoedigd.
Het privacy beleid en relevante privacyproducten worden gecommuniceerd via een vaste pagina/plaats op Stroom (intranet) en internet. Communicatie over het beleid is essentieel voor het creëren van draagvlak en het managen van verwachtingen ten aanzien van de privacy van personen. Het is van belang dat de urgentie van het privacy beleid om correct om te gaan met persoonsgegevens binnen de gehele organisatie blijvend wordt gevoeld. Daartoe worden regelmatig bewustwordingsactiviteiten en trainingen verzorgd. Daarnaast verleent het privacyteam waar nodig of gewenst ondersteuning bij de operationele priacyprocessen.

6.3 Controle en naleving

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen maken het noodzakelijk om periodiek te bezien of het privacybeleid al dan niet aanpassing behoeft. De FG houdt toezicht op de naleving van de privacywetgeving en het privacybeleid. Het privacyteam heeft periodiek overleg om actuele ontwikkelingen en gedane constateringen met elkaar te bespreken en te bezien of en zo ja welke vervolgacties nodig zijn.

7. Rechten voor betrokkenen

7.1 Inleiding
In de AVG zijn verschillende rechten voor betrokkenen opgenomen die zij tegenover de verantwoordelijke kunnen inroepen. Het gaat dan vooral om inzage en verbeterings- of verwijderingsrechten en het daaruit afgeleide "right to be forgotten", alsmede verzetsrechten met betrekking tot geautomatiseerde besluitvorming of direct marketing.
Op grond van artikel 12 AVG heeft de verwerkingsverantwoordelijke een algemene zorgplicht om passende maatregelen te nemen zodat de betrokkenen de informatie ontvangen in een begrijpelijke vorm. Als een betrokkene daarom verzoekt, verstrekt de verwerkingsverantwoordelijke kosteloos en zonder enige vertraging en uiterlijk binnen een maand de door hem verzochte informatie. De rechtsgrondslag van de verwerking moet expliciet vermeld worden en dat geldt ook voor de bron van de gegevens, wanneer dit nodig is om tegenover de betrokkene een eerlijke en transparante verwerking te waarborgen. De rechten van betrokkenen zijn bekend gemaakt in de privacyverklaring op de website van Waterschap Rivierenland (www.wsrl.nl). Daar het aantal verzoeken van betrokkenen vooralsnog gering is, wordt in de praktijk maatwerk geleverd ingeval een betrokkene een verzoek heeft ingediend om gebruik te maken van het uitoefenen van zijn rechten.

7.2 Uitgangspunten uitoefenen rechten voor betrokkenen
Bij het uitoefenen van de rechten door betrokkenen geldt dat:
- Communicatie
  informatie en communicatie over de rechten voor betrokkenen op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan betrokkene, waarbij het taalgebruik wordt afgestemd op de doelgroep;
- Behandelingstermijn
  op een verzoek van een betrokkene wordt zo spoedig mogelijk na indiening schriftelijk gereageerd, maar uiterlijk binnen vier weken. Hierbij zal de betrokkene in ieder geval worden geïnformeerd over het gevolg dat aan het verzoek is gegeven. Indien de termijn van vier weken redelijkerwijs niet haalbaar is, zal betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. In dat geval zal Waterschap Rivierenland binnen twee maanden na het verstrijken van de eerste termijn gevolg geven aan het verzoek van betrokkene.
- identiteit van betrokkene
  Waterschap Rivierenland stelt de identiteit van betrokkene vast alvorens het verzoek van betrokkene inhoudelijk te behandelen. Zo voorkomt het waterschap dat informatie niet in verkeerde handen valt.

7.3 Recht op informatie
De betrokkene heeft het recht om door Waterschap Rivierenland te worden geïnformeerd over bepaalde aspecten van de verwerking van zijn persoonsgegevens. Waterschap Rivierenland informeert betrokkene kosteloos over de verwerking van diens persoonsgegevens.

7.4 Recht op inzage
Iedere betrokkene heeft het recht om te informeren of zijn persoonsgegevens worden verwerkt en, indien dat het geval blijkt, het recht op inzage in hem betreffende verwerkte persoonsgegevens. Daarnaast kan betrokkene een kopie van de betreffende persoonsgegevens vragen. Het verstrekken van één kopie van deze gegevens is kosteloos.

7.5 Recht op rectificatie, aanvulling, verwijdering of beperking van de verwerking
Iedere betrokkene kan met betrekking tot over hem opgenomen persoonsgegevens bij het waterschap verzoeken deze gegevens te corrigeren, aan te vullen, te verwijderen of de verwerking ervan te beperken. Bij het recht op beperking worden de persoonsgegevens tijdelijk afgeschermd en niet meer door het waterschap verwerkt. Indien blijkt dat de opgenomen persoonsgegevens van de betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, zal de gegevensbeheerder (dat kan zowel de functioneel beheerder als de verwerker zijn) deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken. De gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De uitvoering hiervan is kosteloos voor betrokkene.

7.6 Recht van bezwaar
Betrokkene kan een bezwaarschrift bij Waterschap Rivierenland indienen indien hij van mening is dat de verwerking van zijn gegevens door het waterschap in strijd met wet- en regelgeving plaatsvindt.

8 Incidenten met betrekking tot Persoonsgegevens

8.1 Algemeen
Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens door Waterschap Rivierenland is een privacy incident. De bekendste vorm van zo'n incident is een datalek.

8.2. Melding en registratie
Medewerkers (zowel intern als extern) van Waterschap Rivierenland zijn verplicht om een (vermoedelijk) datalek en andere privacy incidenten direct te melden. De melding wordt gedaan via Stroom-meldingen-melding maken datalek
Van elk incident en de afhandeling daarvan wordt een registratie bijgehouden. Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen persoonlijke consequenties heeft voor de melder. Een melder dient zolang het incident nog niet is afgehandeld vertrouwelijk met de melding om te gaan en hierover niet verder te communiceren dan met de leidinggevende, de FG of de privacy officers.

8.3 Afhandeling melding
De afhandeling van incidenten heeft als doel het probleem op te lossen, de schade te beperken en de wetgeving na te leven. De behandeling van een melding vindt plaats door het privacyteam (bestaande uit de FG en de twee PO's). De melder wordt in beginsel telefonisch benaderd om een toelichting te geven op de gedane melding. Zolang de melding openstaat wordt de melder tussentijds geïnformeerd over de voortgang in de afhandeling van de melding.
Per melding wordt beoordeeld of er al dan niet sprake lijkt te zijn van een datalek. Indien de melding een datalek betreft dan wordt beoordeeld of daarvan melding dient te worden gedaan bij de Autoriteit Persoonsgegevens (AP). Een melding aan de AP dient onverwijld binnen 72 uur na constatering plaats te vinden, tenzij het niet waarschijnlijk is dat het datalek (de inbreuk op de privacy) redelijkerwijs een risico voor de betrokkene met zich brengt.
Wanneer het informeren van betrokkenen verplicht is conform de regels van de AP of anderszins gewenst is, wordt de communicatie, in samenspraak met de behandelaar van de melding, vanuit de melder verzorgd.

8.4 Evaluatie incidenten
Het is van belang om te leren van incidenten. Registratie van incidenten en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van persoonsgegevens. De rapportage(s) over incidenten met betrekking tot persoonsgegevens maken daarom een vast onderdeel uit van het jaarverslag privacy van de FG.

9 Verantwoordingsplicht

9.1 Inleiding
In het kader van de AVG geldt dat het waterschap een verantwoordingsplicht heeft ten aanzien van de verwerking van persoonsgegevens. Hierna, onder 9.2, wordt schematisch een overzicht opgenomen met daarin opgenomen de verplichting, een toelichting en het proces of product dat daarbij hoort.

9.2 Overzicht verplichtingen met bijbehorend proces of product
In onderstaande tabel is aangegeven welke verplichtingen dat zijn en welke processen en producten daarmee samenhangen.

Verplichting	Toelichting	Processen en producten
Noodzakelijkheid, rechtmatigheid en doelbinding	Beoordeling van de noodzaak, de rechtmatigheid en de doelbinding van de verwerking van persoonsgegevens	Privacy-beleid
Juistheid en volledigheid van de persoonsgegevens	maatregelen om de juistheid en de volledigheid van de persoonsgegevens te waarborgen	Dpia
Inzet externe verwerker	bij de verwerking van persoonsgegevens kunnen externe partijen betrokken zijn	Verwerkersovereenkomst met externe verwerker
Bewaartermijnen	Selectielijst Waterschappen	Proces voor verwijdering, vernietiging en archivering
Rechten van betrokkene	Systematiek om rechten te kunnen uitoefenen	Privacyverklaring over de verwerking van persoonsgegevens

Register van verwerkingsactiviteiten	Overzicht van verwerkingen	Register van verwerkingsactiviteiten
incidentenbeheer	verantwoording	Proces voor melden en registreren van datalekken
Functionaris voor Gegevensbescherming	Interne toezichthouder en adviseur privacy	Aanstellingsbesluit Functionaris voor Gegevensbescherming

9.3 Evaluatie privacybeleid

Het privacybeleid wordt na twee jaar geevalueerd en indien nodig wordt dit beleid vervolgens geactualiseerd.

10 Afsluiting

Dit besluit treedt in werking met ingang van 1 juli 2022.

Aldus vastgesteld in de vergadering van het college van dijkgraaf en heemraden van Waterschap Rivierenland van 21 juni 2022 te Tiel.

de secretaris-directeur,
ir. Z.C. Vonk

de waarnemend dijkgraaf,
M.H.M. Gremmen