Privacybeleid Waterschap Rivierenland 2018

Inhoudsopgave

Hoofdstuk 5: Implementatie privacybeleid en uitvoeringsprogramma privacy:

Management samenvatting

Met de intrede van de AVG krijgt WSRL een grotere verantwoordelijkheid voor de omgang met persoonsgegevens, zowel van burgers als van medewerkers en bestuurders. De AVG vraagt een grote mate van **transparantie** en vereist dat de organisatie de persoonsgegevens afdoende **afschermt** tegen verlies, misbruik of ongeoorloofde toegang. Bovendien moet de organisatie betrokkenen in staat stellen hun gegevens in te zien en waar nodig te **corrigeren** of verwijderen. Dit beleidsdocument beschrijft de wijze waarop WSRL invulling geeft aan de verplichtingen die voortkomen uit de AVG. De drie vet geschreven termen vormen de doelstellingen van de CIP Privacy Baseline, het normenkader dat onder dit beleid ligt.

Verwerking van persoonsgegevens binnen het waterschap
Het waterschap verwerkt in diverse processen persoonsgegevens. De verwerkende processen met grote hoeveelheden persoonsgegevens en/of een hoog risico zijn:

Binnen de afdeling Bedrijfsvoering

- Personeelsadministratie, hier worden persoonsgegevens verwerkt over het dienstverband
- Grondzaken, hier worden persoonsgegevens verwerkt over grondtransacties, waarde en eigendom onroerend goed

Binnen de afdeling Vergunningen

- Vergunningen, hierin worden persoonsgegevens over grondposities verwerkt

Binnen de afdeling Handhaving

- Handhaving, hier worden strafrechtelijke gegevens verwerkt

Verwerkende processen met incidenteel gebruik van persoonsgegevens en laag risico zijn:

- Processen m.b.t. Beheer en onderhoud, hier worden gegevens over grondeigendom verwerkt
- Processen m.b.t. Plannen, hier worden persoonsgegevens verwerkt om burgers te informeren over projecten van het waterschap.
-

Vrijwel elk werkproces van het waterschap verwerkt persoonsgegevens, maar de mate waarin en het risico verschilt. Prioriteit bij het nemen van maatregelen ligt bij de processen met een hoog risico en/of grote hoeveelheden persoonsgegevens.

Maatregelen

De AVG vraagt van persoonsgegevens verwerkende organisaties een zorgvuldige werkwijze. Persoonsgegevens zijn waardevol en betrokkenen hebben recht op bescherming tegen misbruik,

verlies of buitensporig gebruik van hun gegevens. Het waterschap dient aantoonbaar maatregelen te treffen om deze bescherming te borgen. Dit beleidsdocument beschrijft de maatregelen en de wijze waarop aantoonbaar wordt gemaakt dat het waterschap hieraan invulling geeft.

Afscherming
Het waterschap is verplicht passende technische en organisatorische maatregelen te treffen ter beveiliging van de verwerking van persoonsgegevens. Hier ligt een nadrukkelijke relatie met informatiebeveiliging. De IT organisatie is verantwoordelijk voor het inrichten van een IT-omgeving die voldoende beveiligd is om afscherming te kunnen garanderen. De Baseline Informatiebeveiliging Waterschappen (BIWA) reikt een norm aan om de beveiliging op het juiste niveau te brengen. Afscherming is echter niet alleen een verantwoordelijkheid van IT. Iedere individuele medewerker dient te zorgen voor afscherming van de persoonsgegevens die hij verwerkt. IT en de privacy specialisten reiken medewerkers tools aan om dit op een goede manier te kunnen doen.

Corrigeerbaarheid
Het waterschap dient aantoonbaar in staat te zijn om persoonsgegevens waarover zij beschikt te corrigeren of te verwijderen indien nodig. Hiervoor moet het waterschap weten over welke gegevens zij beschikt en waar deze zich bevinden. Onder meer door middel van het register van verwerkingsactiviteiten wordt overzicht gehouden over de gegevensverwerkende processen.

Transparantie
Verantwoordelijken moeten transparant zijn over de persoonsgegevens die zij verwerken. Betrokkenen hebben het recht te weten wat er met hun gegevens gebeurt. Zowel binnen de organisatie als daarbuiten, in opdracht van de verantwoordelijke. Door middel van onder meer privacy statements informeert het waterschap betrokkenen over de verwerking.

Verankering in de processen

Privacy dient duurzaam te worden geïmplementeerd in de bedrijfsvoering en beleidsprocessen. Bescherming van privacy is niet alleen een zaak voor de FG en de Privacy officer, maar is een uitgangspunt bij de uitvoering van alle processen. Het voldoen aan de wet is een verantwoordelijkheid van de proceseigenaren. Dat betekent dat ook binnen de processen kennis beschikbaar dient te zijn van de privacywetgeving en de toepassing daarvan binnen de processen. Zowel bij de proceseigenaren als bij de medewerkers in de processen.

Plan, do, check, act

Door middel van de beschreven maatregelen werkt WSRL de beginselen van de AVG uit in concrete normen, standaarden en richtlijnen. Deze worden periodiek getoetst en geëvalueerd op opzet, bestaan en werking. Aan de hand van de uitkomsten van de evaluatie worden beleid, standaarden, processen en procedures bijgesteld. Zo ontstaat een PDCA-cirkel die zorgt voor duurzame verankering van gegevensbescherming in de bedrijfsvoering van WSRL.

Erkend certificeringsmechanisme

De AVG moedigt organisaties aan bij het implementeren van maatregelen gebruik te maken van erkende certificeringsmechanismen. In Nederland heeft het CIP (Centrum Informatiebeveiliging en Privacybescherming) een baseline ontwikkeld voor de te nemen maatregelen, de CIP Privacy Baseline. Deze baseline vormt een uitstekend kader voor de te implementeren maatregelen. De maatregelen worden daarmee toetsbaar tegen een erkende norm en zo kan een methode van plando-check-act worden opgezet. Voor het uitwerken van maatregelen uit dit beleid en de evaluatie daarvan zal de CIP Baseline Privacy worden gehanteerd.

Evaluatie van het beleid

Ook dit beleidsdocument zal periodiek worden geëvalueerd en bijgesteld waar nodig.

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. Deze Europese verordening en de Nederlandse Uitvoeringswet AVG vervangen de Wet bescherming persoonsgegevens (Wbp) in Nederland. Er is vanaf 25 mei 2018 dus sprake van één gezamenlijk privacy-regime binnen de Europese Unie.

1.2 Achtergrond AVG:

Door snelle technologische ontwikkelingen en globalisering zijn er nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De mate waarin persoonsgegevens worden verzameld en gedeeld, is enorm gestegen. Dankzij de technologie kunnen bedrijven en overheden bij het uitvoeren van hun activiteiten meer dan ooit gebruikmaken van persoonsgegevens. Natuurlijke personen maken hun persoonsgegevens steeds vaker wereldwijd bekend. Technologie heeft de economie en het maatschappelijk leven ingrijpend veranderd en moet het vrije verkeer van persoonsgegevens binnen de Unie en de doorgifte aan derde landen en internationale organisaties verder vergemakkelijken en daarbij een hoge mate van bescherming van persoonsgegevens garanderen. [1]

Eén van de schaduwzijden van de informatiemaatschappij is dat een ongebreidelde vergaring, bewerking en verspreiding van persoonsgegevens kan leiden tot een inbreuk op de persoonlijke levenssfeer. Schendingen van privacy en het hacken van informatiesystemen waarin ook persoonsgegevens zijn opgenomen, komen dagelijks voor. Deze schending van privacy kan grote gevolgen hebben voor de persoonlijke en maatschappelijke veiligheid en daarnaast financiële risico's met zich meebrengen.

1.3 Wat verandert er als de AVG van toepassing is?

De AVG versterkt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacy rechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken, krijgen meer verplichtingen. De nadruk ligt – meer dan nu – op de verantwoordelijkheid van organisaties om aan te kunnen tonen dat zij zich aan de wet houden (verantwoordingsplicht).

1.4 Waarom privacybeleid?

[1] Overweging (6) uit de Algemene verordening gegevensbescherming 5419/16

Ook Waterschap Rivierenland heeft vanuit zijn wettelijke en dienstverlenende taken te maken met het verwerken van persoonsgegevens van derden, haar eigen medewerkers en bestuurders. Denk bijvoorbeeld aan het verlenen van vergunningen, de personeelsadministratie, het behandelen van bezwaren en klachten, aansprakelijkstellingen, kadastrale gegevens, publicaties op internet, etc. 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. Ook wanneer een andere organisatie taken voor het waterschap uitvoert, kan het waterschap verantwoordelijk zijn dat deze organisatie de privacy wet- en regelgeving correct naleeft.

Met het vaststellen van dit privacybeleid 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 privacybeleid geeft WSRL op organisatorisch en strategisch niveau duidelijkheid over de keuze van inrichting van privacy en waarborgen dat de verwerking op een rechtmatige wijze plaatsvindt. Daarmee voldoet WSRL aan de verantwoordingsplicht uit de AVG.[2] Verder draagt het privacybeleid er aan bij dat besluiten op grond van de AVG binnen het waterschap op een eenduidige manier worden genomen en dat ook de procedures eenduidig zijn. Hiermee wordt zowel intern als extern transparantie betracht. Betrokkenen moeten er op kunnen vertrouwen dat WSRL zorgvuldig en veilig met persoonsgegevens omgaat.

1.5 Reikwijdte:

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 privacybeleid is van toepassing op de hele organisatie, alle taken en processen, objecten, gegevensverzamelingen en onderliggende informatiesystemen waar het waterschap verantwoordelijk voor is. Bij de invoering van het beleid zullen de proceseigenaren, systeemeigenaren en gegevenseigenaren worden betrokken. Vanuit informatiebeveiliging is het belangrijk dat uiteindelijk passende maatregelen zijn genomen om te voldoen aan wet- en regelgeving.

Het beleid heeft betrekking op het verwerken van persoonsgegevens van betrokkenen, dat wil zeggen alle interne en externe relaties van Waterschap Rivierenland. Onder interne relaties worden in ieder geval

---

[2] Artikel 5 lid 2 AVG

verstaan betrokken burgers, (oud)werknemers, (oud)bestuursleden, en onder externe relaties leveranciers, gasten, bezoekers, inhuurkrachten etc. Dit beleid is in lijn met het algemene beleid van het waterschap en met de Europese en nationale wet- en regelgeving.

1.6 Opzet van het beleid:

In het privacybeleid worden de kaders voor het omgaan met persoonsgegevens vastgelegd en in het op te stellen register van verwerkingsactiviteiten wordt inzichtelijk gemaakt welke persoonsgegevens (wel/geen bijzondere persoonsgegevens) worden verwerkt, wat de grondslag en het doel is van de verwerking, welke categorieën van betrokkenen, de inhoud van de gegevens, bronnen, de bewaartermijnen, risicoclassificatie, verwerkers, taken en verantwoordelijkheden, veiligheidsmaatregelen etc.

Sommige onderwerpen zijn (of worden) verder uitgewerkt in afzonderlijke regelingen (bijv. het Protocol personeelsvolgsystemen en de procedure Meldplicht Datalekken). Daarnaast wordt in het beleid verwezen naar gedragscodes die door de Autoriteit Persoonsgegevens zijn vastgesteld en waarin de uitvoering van de AVG nader wordt geconcretiseerd. Het privacybeleid is te beschouwen als een levend document, dat regelmatig aangevuld en/of gewijzigd kan worden.

1.7 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 zijn in de Privacy Baseline als volgt omschreven:

<u>Afscherming:</u>
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.

<u>Corrigeerbaarheid</u>:
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.

<u>Transparantie</u>:
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 privacybeleid zullen deze criteria uit de Privacy Baseline van het CIP als uitgangpunt worden genomen.

Onderstaand wordt eerst het juridisch kader geschetst en vervolgens wordt ingegaan op de basisbeginselen van de AVG en wordt verder aangegeven hoe WSRL deze in praktijk brengt.

1.8 Privacyrisico's

Het niet voldoen aan de privacywetgeving kan verregaande gevolgen hebben zowel voor betrokkenen als het waterschap.

Verkeerd gebruik, misbruik of verlies van persoonsgegevens kan een behoorlijke impact hebben op zowel iemands zakelijke als privéleven en leiden tot aanzienlijke schade, zowel materieel als immaterieel. 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 de organisatie kan het niet voldoen aan de privacywetgeving (of zelfs de schijn daarvan) leiden tot negatieve publiciteit en imagoschade. Daarnaast kan het kan leiden tot juridische consequenties, waaronder:

- 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.

2. Juridisch kader

2.1 De Algemene verordening gegevensbescherming

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 werden neergelegd in de Wet bescherming persoonsgegevens (Wbp) en in sectorspecifieke wetgeving. Met ingang van 25 mei 2018 wordt de Wbp vervangen door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG).

De verordening heeft directe werking. Dit betekent dat de bepalingen uit de verordening zonder verdere tussenkomst van de nationale wetgever in de lidstaten moet worden toegepast. Decentrale overheden moeten direct voldoen aan de regels in de Verordening, en burgers kunnen zich hier ook direct op beroepen. De meeste rechten en plichten vloeien dus rechtstreeks voort uit de AVG.

De wijzigingen die de AVG met zich meebrengt zijn geen principiële wijzigingen ten aanzien van de Wbp. De kernprincipes van doelbinding, dataminimalisatie, kwaliteit van gegevens en rechtmatige verwerking zijn ook neergelegd in de AVG. Wel is er een verschuiving van taken van de externe toezichthouder (Autoriteit Persoonsgegevens) naar de interne toezichthouder (de Functionaris Gegevensbescherming van het waterschap).

De belangrijkste veranderingen die de AVG met zich brengt zijn:

- De verplichting om privacybeleid op te stellen;
- De verplichte aanstelling van een Functionaris gegevensbescherming (FG);
- De verplichting om een register van verwerkingen van persoonsgegevens bij te houden;
- Versterking en uitbreiding van bestaande rechten van betrokkenen (recht op informatie, inzage, correctie en verzet), het recht om vergeten te worden en het recht op data portabiliteit;
- Streng toezicht door de Autoriteit Persoonsgegevens;
- Zeer hoge boetes bij het niet naleven van de wet (tot 20 miljoen euro);
- Verantwoordingsplicht: de organisatie moet aantoonbaar in control zijn met de wet., dat wil zeggen dat de organisatie moet kunnen aantonen welke organisatorische en technische maatregelen er zijn genomen om de persoonsgegevens te beschermen en daarmee de privacy van betrokkenen te borgen;
- Voor risicovolle gegevensverwerkingen is een gegevensbeschermingseffectbeoordeling (GEB) verplicht;
- Processen en systemen moeten worden ingericht volgens de principes van privacy by default en privacy by design.

Op de volgende verwerkingen is de AVG 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, die nog omgezet gaat worden in nationale wetgeving. 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 de richtlijn gegevensbescherming politie en justitie. Deze richtlijn wordt nog omgezet in nationale wetgeving.

Materiele scope:
Ten opzichte van de richtlijn en de Wbp is het materiële toepassingsgebied van de AVG gelijk gebleven: 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.

Uitzonderingen: activiteiten buiten de werkingssfeer van het Unierecht, zuiver persoonlijke of huishoudelijke activiteiten die geen enkel verband houden met een beroeps- of handelsactiviteit, gevaren voor de openbare orde, activiteiten als bedoeld in titel V, hoofdstuk 2 VEU.

2.2 Overige wetgeving

In diverse bijzondere wetten die ook voor het waterschap relevant zijn, zijn ook regels met betrekking tot privacy opgenomen. Bijvoorbeeld de Telecommunicatiewet, de Archiefwet, de Wet openbaarheid van bestuur, de Algemene wet inzake rijksbelastingen, het Wetboek van Strafrecht, de Wet basisregistratie personen enz. In deze bijzondere wetgeving kunnen afwijkende en aanvullende eisen staan. Deze wetten dienen in onderlinge samenhang met de AVG te worden bezien.

Door het in kaart brengen van de verwerkingen van persoonsgegevens per verwerking wordt beoordeeld welke bijzondere wetgeving een rol speelt en hoe aan de daarin neergelegde eisen ten aanzien van privacy tegemoet kan worden gekomen. In bijlage C wordt een overzicht gegeven van wet- en regelgeving met betrekking tot privacy die van toepassing is op de waterschappen.

In de bijlage D wordt de verhouding tussen de AVG en een aantal andere wetten kort behandeld. Over het algemeen geldt dat de AVG geldt als algemene wet waarvan de bepalingen niet van toepassing zijn wanneer er bijzondere wetgeving van toepassing is.

2.3 Overig beleid Waterschap Rivierenland

Diverse interne beleidsstukken hebben een relatie met dit privacybeleid of zijn hier een nadere uitwerking van. Daar waar in deze stukken wordt verwezen naar een zorgvuldige omgang met persoonsgegevens of bescherming van privacy wordt verondersteld dat dit beleid hieraan ten

grondslag ligt. Dit geldt onder meer voor het Protocol personeelsvolgsystemen, de gedragscode integriteit voor medewerkers, gedragscode gebruik online en offline middelen, de richtlijnen gebruik sociale media, de uitvoeringsregeling integriteitsbeleid, de servicenormen.

3. Uitgangspunten en normen voor de verwerking van persoonsgegevens

3.1 Kernbegrippen binnen de AVG

Voor een goed begrip van dit beleid is het noodzakelijk om een aantal begrippen nader te omschrijven. Bij de begripsbepaling wordt zoveel mogelijk uitgegaan van de definities opgenomen in de AVG. Een overzicht van de begrippen is opgenomen in bijlage B

3.2 Toepasselijkheid AVG:

De AVG is van toepassing op 'de geheel of gedeeltelijke geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen' (Artikel 2 AVG)

Dit betekent dat wanneer het waterschap persoonsgegevens per computer verwerkt, de AVG van toepassing is. Maar de AVG is ook van toepassing in situaties waarin handmatig wordt verwerkt, en er dus geen geautomatiseerde verwerking aan de orde is. Als er bijvoorbeeld sprake is van geschreven gespreksnotities van ambtenaren met burgers of derden verzameld in mappen, dan is de AVG ook van toepassing. De AVG is niet alleen van toepassing op de relatie tussen WSRL als overheid en zijn burgers, bedrijven en instellingen, maar ook op de verhouding die het waterschap als werkgever heeft met zijn werknemers.

3.3 Uitgangspunten en normen voor de verwerking van persoonsgegevens:

Feitelijk is de verantwoordingsplicht ('accountability') het centrale begrip binnen de AVG. Het is opgenomen in artikel 5 AVG. Het eerste lid van artikel 5 AVG somt de zes basisbeginselen van de AVG op. De essentie van de verantwoordingsplicht is dat de verwerkingsverantwoordelijke (het college van dijkgraaf en heemraden) verantwoordelijk is voor het naleven van deze beginselen en deze kan aantonen.

Deze principes zijn:

1. *Rechtmatigheid, behoorlijkheid, transparantie:*
   Het waterschap mag niet in strijd met de wet handelen, moet behoorlijk handelen en voor betrokkenen moet duidelijk zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt (Transparantiebeginsel). Alle communicatie richting betrokkene moet begrijpelijk zijn, ook met betrekking tot de rechten van betrokkenen. Verder moeten gegevens voldoende actueel en van goede kwaliteit zijn
   Een verwerking is alleen rechtmatig als aan één van de onderstaande voorwaarden is voldaan. (grondslagen limitatief benoemd in de wet):
   - de betrokkene heeft ondubbelzinnige toestemming gegeven, d.w.z. toestemming is expliciet, voordat de verwerking plaatsvindt, gevraagd en gecommuniceerd;

- de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;
- de verwerking is noodzakelijk om te voldoen aan een wettelijk verplichting die op het waterschap rust;
- de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan het waterschap is opgedragen;

de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van het waterschap of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. Het waterschap kan op deze rechtsgrond een beroep doen voor zover verwerkingen bedrijfsmatige handelingen betreffen, echter niet voor verwerkingen in het kader van de uitoefening van haar taken.

2. *Doelbinding:*
Persoonsgegevens worden alleen verwerkt daar waar dat strikt noodzakelijk is voor de uitvoering van vooraf duidelijk bepaalde en uitdrukkelijk omschreven gerechtvaardigde doelen op basis van de grondslagen zoals beschreven in de wet.

Doelen zijn voordat de verwerking plaatsvindt concreet en specifiek geformuleerd. Persoonsgegevens worden niet verder verwerkt voor andere doelen die hiermee onverenigbaar zijn. Het omschreven doel vormt een kader waaraan kan worden getoetst of de verwerking van de gegevens noodzakelijk is voor dat doel en/of verenigbaar is met een ander doel.

3. *Minimale gegevensverwerking (' dataminimalisatie'):*
De verwerking van persoonsgegevens moet worden beperkt tot die gegevens die voor het betreffende doel strikt noodzakelijk zijn. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.
Verder moet steeds worden gekeken of het doel niet op een minder ingrijpende wijze kan worden bereikt (principes van proportionaliteit en subsidiariteit)[3].

4. *Juistheid*:
Het is van belang dat voortdurend wordt nagegaan of de persoonsgegevens die het waterschap van betrokkenen verwerkt juist en actueel zijn. Als blijkt dat de gegevens niet meer correct zijn moeten ze door het waterschap worden gewijzigd of verwijderd).

---

3 Bij een verwerking van persoonsgegevens mag een inbreuk op de belangen van de betrokkene niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel. Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt de inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk beperkt.

5. *Opslagbeperking/ Bewaartermijnen*:
Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel van de verwerking. Hierbij worden de van toepassing zijnde (wettelijke) bewaar- en vernietigingstermijnen in acht genomen.

6. *Integriteit en vertrouwelijkheid*:
Het waterschap dient te zorgen voor een goede beveiliging van persoonsgegevens, door het nemen van passende technische of organisatorische maatregelen. Het waterschap moet er voor zorgen dat ongeoorloofde toegang tot- en gebruik van persoonsgegevens wordt voorkomen. Maatregelen zijn erop gericht om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen en zijn opgenomen in het informatiebeveiligingsbeleid (privacy by design). In geval van samenwerking met externe partijen waarbij sprake is van verwerking van persoonsgegevens worden afspraken gemaakt over de eisen waar gegevensuitwisselingssystemen aan moeten voldoen. Met verwerkers worden verwerkersovereenkomsten gesloten.

Aan al deze vereisten moet worden voldaan bij de verwerking van persoonsgegevens. Bij elke verwerking moet met deze beginselen rekening worden gehouden.

3.4 Invulling verantwoordingsplicht:

Het waterschap (strikt genomen het college van dijkgraaf en heemraden als verwerkingsverantwoordelijke) moet actief aantonen dat ze aan deze voorgaande zes beginselen voldoet. Er is sprake van een omgekeerde bewijslast. Het is niet zo dat een betrokkene of de toezichthouder moet aantonen dat het waterschap niet aan een verplichting voldoet. Dit vraagt dus om een actieve houding van het waterschap, waarbij aan de toezichthouder of betrokkene kan worden aangetoond dat de zes beginselen worden nageleefd. De invulling van de verantwoordingsplicht komt met name tot uiting in:

- *Beschermings- / beveiligingsbeleid:*.
Deze nota gaat voor een deel over de beveiliging van persoonsgegevens. Het informatiebeveiligingsbeleid van WSRL is verbonden met privacy beleid. Voor zover het gaat over de beveiliging van persoonsgegevens is het er een onderdeel van. In het informatiebeveiligingsbeleid is onder andere geregeld welke principes gehanteerd worden ten aanzien van te verlenen autorisaties. Alleen diegenen waarbij het noodzakelijk is dat zij met persoonsgegevens werken, krijgen een autorisatie voor de verwerking van deze gegevens (zie verder hoofdstuk 4).

- *Verwerkingsregister:*
Het waterschap moet een register bijhouden van alle verwerkingsactiviteiten[4] die door of namens het waterschap plaatsvinden. In dit register moeten onder meer worden opgenomen: de categorieën van betrokkenen, de soorten persoonsgegevens en met wie deze gegevens gedeeld worden (zie verder paragraaf 5.10). Voor betrokkenen moet duidelijk zijn welke persoonsgegevens worden vastgelegd,

4 Artikel 30 AVG

verwerkt, waarom en door wie. Per verwerking wordt aangegeven wie de verwerkingsverantwoordelijke is, wie beheerder is en (indien van toepassing) wie verwerker is.

- *Gegegevensbeschermingseffectbeoordeling (GEB):*
  Wanneer een verwerking van persoonsgegevens waarschijnlijk veel risico's inhoudt voor betrokkenen, moet het waterschap vooraf beoordelen wat het effect hiervan is op bescherming van persoonsgegevens. Er moet dus van tevoren worden gekeken wat de risico's zijn en of die ondervangen kunnen worden.

- *Procedure datalekken:*
  Er is sprake van een datalek wanneer persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk gemaakt op een manier die in strijd is met de AVG. Wanneer er sprake is van een datalek, moet het waterschap, als verwerkingsverantwoordelijke, dit zo spoedig mogelijk melden bij de toezichthouder (de Autoriteit Persoonsgegevens) zo mogelijk binnen 72 uur. Wanneer er grote kans bestaat dat het datalek negatieve gevolgen heeft voor betrokkenen, moeten deze ook worden gewaarschuwd. Onder de Wbp bestond de meldplicht datalekken al. Het waterschap heeft hiervoor een calamiteitenplan niet-watergerelateerde zaken vastgesteld. Hoofdstuk 4 van dit calamiteitenplan gaat over datalekken. Dit plan zal ook worden gehanteerd onder de AVG.

3.5 Rechten voor betrokkenen

In de AVG krijgen betrokkenen allerlei rechten 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. Onder werking van de richtlijn en in de Wbp geeft het inzagerecht de betrokkene aanspraak op informatie over de doeleinden van de verwerkingen, de categorieën van de verwerkte gegevens en de ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt, alsmede de beschikbare informatie over de herkomst van de gegevens. Onder de AVG gaat het om al deze informatie, met in aanvulling daarop óók informatie over bewaartermijnen, klachtrechten en -procedures, gegevensdoorgiften naar landen buiten de Unie en de in dat verband getroffen waarborgen, en het bestaan van de mogelijkheid dat er geautomatiseerde besluitvorming en profilering plaatsvindt (art. 15 sub 1, 2 en 4 AVG).

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.

Verder voorziet de verordening in een aantal nieuwe rechten voor betrokkenen. Zoals het gegevenswissingsrecht, ofwel 'het recht op vergetelheid' en het recht op gegevensoverdraagbaarheid (art. 17 en art. 20 AVG). Het gegevenswissingsrecht houdt in dat de betrokkene van de verwerkingsverantwoordelijke kan verlangen dat zijn persoonsgegevens worden gewist als deze niet meer

relevant zijn of onrechtmatig worden verwerkt. In het geval deze gegevens openbaar zijn gemaakt door de verwerkingsverantwoordelijke, moet deze ervoor zorgen dat degenen die daardoor over de gegevens beschikken worden geïnformeerd over het verwijderingsverzoek (art. 17 lid 2 AVG).

De rechten van betrokkenen worden vertaald in heldere, laagdrempelige procedures en worden helder gecommuniceerd richting burger.

4 Organisatorisch Kader

De verwerkingsverantwoordelijke stelt vast welke persoonsgegevens worden verwerkt en wat het doel is van de verwerking. De verwerkingsverantwoordelijke neemt formeel en juridisch initiatief voor de verwerking van persoonsgegevens en is daar ook verantwoordelijk voor. Dat geldt ook voor het melden van datalekken.

Binnen Waterschap Rivierenland zijn bevoegdheden op basis van de Ambtelijke bevoegdhedenregeling gemandateerd aan de ambtelijke organisatie. Het CDH is eindverantwoordelijk en als zodanig de verwerkingsverantwoordelijke in de zin van de AVG.

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 verantwoordelijkheden onderkend. Uiteindelijk is het zorgvuldig omgaan met persoonsgegevens een verantwoordelijkheid voor iedereen in de organisatie.

4.1 Rollen en verantwoordelijkheden

Het College van dijkgraaf en heemraden (eindverantwoordelijke):

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 privacybeleid te waarborgen. Naleving van de privacywetgeving is de uitdrukkelijke verantwoordelijkheid van het College van dijkgraaf en heemraden en niet van de Functionaris Gegevensbescherming.

Portefeuillehouder privacy (uitvoeringsverantwoordelijke):

Het CDH wijst uit haar midden een portefeuillehouder Privacy aan die bestuurlijk verantwoordelijk is voor de uitvoering van het privacybeleid 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 er op toe dat privacy een vast onderdeel van de bedrijfsvoering wordt.

4.2 Taken FG, ISO, privacy-officer, Privacy Taskforce

Binnen WSRL is een aantal functionarissen aangewezen, dat zich bezighoudt met het thema privacy, te weten de Functionaris Gegevensbescherming (FG), de privacy officer/jurist privacy, de jurist opsporing, de ISO, de organisatie adviseur, de communicatie adviseur en privacy ambassadeurs. De taken waarmee deze functionarissen zijn belast, zijn in onderstaande paragrafen uitgewerkt.

De Functionaris Gegevensbescherming (onafhankelijk toezichthouder):

Binnen WSRL is een "dedicated" Functionaris Gegevensbescherming aangesteld als FG en aangemeld bij de Autoriteit Persoonsgegevens. Als plaatsvervangend FG is de privacy officer aangewezen.
De volgende taken zal de FG uitvoeren:

- 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 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 WSRL 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 taken[5] 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.
- De FG brengt rapporteert rechtstreeks aan het CDH.

5 De wettelijke taken zijn het informeren en adviseren van het betrokken personeel, toezicht op de naleving van de AVG, advisering m.b.t. 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.

Privacy Officer:

Om te voorkomen dat een FG zich te teveel met adviserende en uitvoerende taken bezighoudt, en daarmee in feite zijn eigen werkzaamheden controleert, worden deze taken bij Waterschap Rivierenland uitgevoerd door de 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 een jurist uit het Team Bestuurs- en Juridische Zaken.

De Privacy Officer is de uitvoerende rol in het privacybeleid. Taken van de Privacy Officer zijn:

- Schrijven en beheren van het privacy beleid van WSRL
- Schrijven en beheren van privacy-gerelateerde werkprocessen
- Adviseren over te nemen maatregelen voor AVG compliance, invulling geven aan de principes van Privacy by Design en Privacy by Default.

Privacy Jurist (PJ):

De Privacy Jurist maakt deel uit van het team Bestuurs- en Juridische Zaken en is gespecialiseerd op het privacy recht. Deze functionaris is belast met de uitvoering van verzoeken in het kader van de AVG. Daarnaast adviseert hij/zij de FG bij juridische vraagstukken. De PJ treedt op als waarnemer van de FG. Taken van de Privacy Jurist zijn:

- Uitvoeren van verzoeken van betrokkenen om inzage, correctie, wissing, etc.
- Adviseren van de FG bij juridische aangelegenheden
- Adviseren bij het sluiten van verwerkersovereenkomsten
- Beheren van het register van verwerkingsovereenkomsten
- Coördinatie en beheer van privacyincidenten. (procedure meldplicht datalekken)

Jurist Opsporing (JO):
De Jurist Opsporing adviseert over juridische aangelegenheden met betrekking tot opsporing in relatie tot privacy. De Jurist Opsporing treedt op als waarnemer voor de PJ.

Information Security Officer (ISO):

Binnen WSRL is een ISO aangesteld. Deze functie is beleidsmatig gericht en heeft als belangrijkste doel om binnen de WSRL voldoende organisatorische beveiligingsmaatregelen te initiëren, en wel zodanig dat de technische beveiligingsmaatregelen ook daadwerkelijk effectief zijn. Met andere woorden, er dient zorg gedragen te worden voor samenhang tussen de technische en organisatorische maatregelen.

- Verantwoordelijk voor het opstellen, bijstellen, vernieuwen en herzien van het informatiebeveiligingsbeleid en de daaruit voortvloeiende informatie(beveiligings)plannen.
- Initiëren of laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses.
- Opzetten en initiëren van (periodieke) informatiebeveiligingsbewustzijn programma's en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen).
- Coördineren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten.
- Aanspreekpunt voor de organisatie betreffende beveiliging en incidenten.
- Projecten leiden die als doel hebben beveiligingsmaatregelen te implementeren of de kwaliteit van de beveiliging op langere termijn te handhaven en waar nodig te verbeteren.
- Controleren van de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen.
- Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de portefeuillehouder.
- WSRL vertegenwoordigen in externe overleggremia.
- Rapportages op het gebied van beveiliging laten beoordelen.
- Optreden als informatiebeveiligingsadviseur (voor het management) bij nieuwe ICT-voorzieningen en bij ingrijpende veranderingen in de ICT-infrastructuur.

Organisatie adviseur (OA):
De Organisatie adviseur belast met privacy helpt bij het verbeteren van processen in relatie tot privacy in de breedste zin van het woord.

Communicatie adviseur (CA):
De Communicatie adviseur draagt zorg voor de uitvoering van het awareness programma privacy binnen de organisatie.

Privacy Ambassadeur (PA):
De privacy ambassadeurs zijn beleidsmedewerkers op een afdeling waar veelvuldig met persoonsgegevens wordt gewerkt. De privacy ambassadeur is de eerst aan te spreken persoon voor medewerkers van de betreffende afdelingen. Deze functionaris heeft affiniteit met en kennis van de privacy wetgeving en stimuleert de actieve toepassing van het privacybeleid van WSRL.

Teamleiders (uitvoeringsverantwoordelijke):
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 privacybeleid binnen de werkprocessen van de eigen afdeling.

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.

Privacy team

Om dit privacybeleid en de bijbehorende bijlagen up-to-date te houden komt iedere maand een privacy team bij elkaar (zie paragraaf 5.3 van hoofdstuk 5).

5 Implementatie privacybeleid en uitvoeringsprogramma privacy

5.1 Technische en organisatorische beveiligingsmaatregelen: (gedragscodes, normenkaders (BIWA), awareness programma)

Een belangrijk aspect van het privacybeleid is de beveiliging van persoonsgegevens. De beveiliging van persoonsgegevens is één van de onderdelen van informatiebeveiliging. Informatiebeveiliging slaat op het geheel aan maatregelen waarmee de organisatie informatie beveiligt. Het gaat hierbij om alle informatie die de organisatie verwerkt, zowel digitaal als niet-digitaal. Persoonsgegevens maken hier deel van uit. In de AVG wordt bepaald dat de verwerkingsverantwoordelijke de verplichting heeft om passende technische en organisatorische maatregelen uit te voeren om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bij de te nemen maatregelen die nodig zijn voor het garanderen van een passend beveiligingsniveau moet in ieder geval rekening gehouden worden met drie criteria:

1. Stand van de techniek;
2. Kosten van de tenuitvoerlegging: evenredigheid kosten beveiliging en het effect op de beveiliging van persoonsgegevens;
3. De risico' s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Privacybescherming en informatiebeveiliging overlappen elkaar deels op het gebied van beschikbaarheid, kwaliteit, integriteit en vertrouwelijkheid van data, waaronder persoonsgegevens, alsmede gegevensclassificatie, logische en fysieke beveiliging en incidentmanagement (datalekken). In het uitvoeringsprogramma van het Informatiebeveiligingsbeleid dienen de (verplichte) maatregelen uit de Richtsnoeren beveiliging persoonsgegevens van de Autoriteit Persoonsgegevens nader ingevuld te worden.

Privacybescherming gaat niet alleen over informatiebeveiliging in de zin van verlies van persoonsgegevens. De privacywetgeving stelt specifieke eisen aan het verwerken van persoonsgegevens die niet onder de werking van informatiebeveiliging vallen, zoals de beginselen van doelbinding, dataminimalisatie, proportionaliteit en subsidiariteit, privacy by design en de wijze van gegevensuitwisseling met andere organisaties binnen en buiten Europa. Wet- en regelgeving met betrekking tot privacy moet verankerd worden in de ondersteunende software van producten en diensten.

Daar waar het privacybeleid en het informatiebeveiligingsbeleid elkaar overlappen worden gezamenlijk prioriteiten gesteld. Afstemming op uitvoeringsniveau vindt structureel plaats tussen de CISO (Chief Information Security Officer), de privacy officer en de FG. De CISO is bij WSRL verantwoordelijk voor de realisatie, kaderstelling, beleidsvoorbereiding, implementatie,

coördinatie, sturing en handhaving van de maatregelen met betrekking tot het informatiebeveiligingsbeleid.

Om het privacybeleid en het Uitvoeringsprogramma Privacy op een efficiënte wijze te implementeren en op de agenda te houden is het van belang om goed samen te werken in de organisatie. Het is noodzakelijk om kennis/ bewustzijn van wat en wel en niet mag bij het verwerken van persoonsgegevens continu op het netvlies te houden om risico's te voorkomen. Het toepassen van privacybeleid is een continu proces dat zich in de hele organisatie afspeelt.

De hieronder beschreven maatregelen dragen er aan bij dat de verschillende activiteiten met betrekking tot persoonsgegevens in samenhang worden uitgevoerd.

5.2 Privacy programma Waterschappen (via Het Waterschapshuis HWH)

In de Commissie Bestuurszaken, Communicatie en Financiën (CBCF) van de Unie van Waterschappen is besloten om de samenwerking te zoeken ten aanzien van de implementatie AVG en het thema privacy op te nemen in het HWH beheerprogramma informatieveiligheid. Er is een Business Case Privacy programma Waterschappen opgesteld. Vanuit het HWH UO informatieveiligheid/UO Privacy wordt het privacyprogramma Waterschappen gecoördineerd en tevens zal de voortgang van de implementatie van de AVG bij de verschillende waterschappen gemonitord worden. De FG en de privacy officer van Waterschap Rivierenland nemen deel in het overleg CPW (Contactpersonen Privacy Waterschappen).

5.3 Privacyteam Waterschap Rivierenland

Structureel overleg tussen afdelingen is noodzakelijk om de samenhang in de organisatie met betrekking tot persoonsgegevensbescherming te borgen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens op elkaar af te stemmen.

Er wordt een intern privacyteam ingericht waar medewerkers van verschillende afdelingen in zijn vertegenwoordigd. In het privacyteam van Waterschap Rivierenland participeren in ieder geval: - de FG, Concerncontrol;

- de CISO, Concerncontrol;
- de ISO, team Informatiebeveiliging;
- de Privacy Officer, team Bestuurs- en Juridische Zaken;
- Medewerker team communicatie;
- Medewerker team Systeem-, Netwerk- en Werkplekbeheer.

Het privacyteam draagt zorg voor de implementatie van de AVG en bewaakt de naleving van de privacywet- en regelgeving. Het privacyteam heeft als voornaamste taken het ondersteunen van de FG bij het privacybeleid, de beoordeling van privacyincidenten (waaronder datalekken)en het bijdragen aan privacy bewustzijn van de organisatie. Het privacy team overlegt regelmatig met de portefeuillehouder Privacy.

5.4 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 privacyrisico's wordt vergroot en het zorgvuldig en rechtmatig verwerken van persoonsgegevens wordt aangemoedigd, bijvoorbeeld met regelmatig terugkerende bewustwordingscampagnes.

Het privacybeleid en relevante producten voortvloeiende uit het Uitvoeringsprogramma Privacy worden gecommuniceerd via een vaste pagina/plaats op intranet en internet. Communicatie over het beleid is essentieel voor het creëren van draagvlak. Het is van belang dat de urgentie van het privacybeleid om correct om te gaan met persoonsgegevens binnen de gehele organisatie gevoeld gaat worden.

5.5 Gegevensbeschermingseffectbeoordeling (GEB):

Een gegevensbeschermingseffectbeoordeling (GEB) of Privacy Impact Analyse (PIA) is een hulpmiddel om bij de ontwikkeling van beleid, en de daarmee gepaard gaande wetgeving, de bouw van ICT-systemen en de aanleg van databestanden en de privacy risico's op een gestructureerde en heldere wijze in kaart te brengen. Met dit instrument kan worden bepaald in hoeverre een organisatie risico's loopt op informatiebeveiligingsincidenten met persoonsgegevens. Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van natuurlijke personen, dan moet voorafgaand aan de verwerking een zogenaamde gegevensbeschermingseffectbeoordeling (een GEB-analyse) plaatsvinden. Dit is in ieder geval het geval bij:

- het systematisch en uitvoerig evalueren van persoonlijke aspecten, waaronder profiling;
- het op grote schaal verwerken van bijzondere persoonsgegevens; en / of
- het op grote schaal systematisch volgen van mensen in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

Op basis van de gegevensbeschermingseffectbeoordeling (GEB) kunnen maatregelen worden getroffen om mogelijke nadelige effecten voor betrokkenen te voorkomen of te beperken.

Het in een zo vroeg mogelijk stadium uitvoeren van een gegevensbeschermingseffect-beoordeling (GEB) en het nemen van maatregelen in de ontwerpfase voorkomt dat achteraf blijkt dat de gegevensverwerking niet voldoet aan de eisen van de AVG en dat alsnog maatregelen moeten worden genomen. Het nemen van beveiligingsmaatregelen bij de ontwikkeling van ICT systemen is goedkoper dan het achteraf aanpassen daarvan. Bovendien kunnen schadevergoedingen worden vermeden, omdat adequate maatregelen zijn genomen om te voorkomen dat voorzienbare risico's zich daadwerkelijk voordoen.

Een GEB is verplicht als de verwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen.

Data-vernietiging en bewaartermijnen:
In de AVG is aangegeven dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor de verwerking van de doeleinden waarvoor zij worden verzameld en vervolgens worden verwerkt. De bewaartermijn is dus geheel afhankelijk van het doel waarvoor de gegevens zijn verzameld. Het is aan de eigenaar van de gegevens om aan te geven hoe lang het noodzakelijk is om de gegevens te bewaren. Daarbij wordt rekening gehouden met wettelijke bewaartermijnen (zoals bijv. opgenomen in de Archiefwet).

Bij het inventariseren van de verwerkingen wordt de bewaartermijn per verwerking vastgesteld. Deze bewaartermijnen worden afgestemd met hetgeen in het Informatiebeveiligingsbeleid staat vermeld. Bij twijfel wordt advies gevraagd aan het privacy team. IB beleid zegt niets over bewaartermijnen.

Selectielijst Waterschappen:
In de Selectielijst voor de neerslag van de handelingen van de waterschappen staat beschreven hoe lang bepaalde documenten bewaard moeten worden. Hierin staat ook de wet- en regelgeving die de bewaartermijnen aangeeft.

5.6 Privacy by design en privacy by default

Privacy by design houdt in dat de organisatie al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht besteedt aan privacy verhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Daarnaast wordt rekening gehouden met dataminimalisatie: het zo min mogelijk verwerken van persoonsgegevens. Dit betekent dat alleen die gegevens die noodzakelijk zijn voor het doel van de verwerking, worden verwerkt. Op deze manier wordt een zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afgedwongen.

Bij Waterschap Rivierenland wordt al bij het begin van de ontwikkeling van verwerkingsprocessen en informatiesystemen en diensten rekening gehouden met privacy (het “Privacy by design” principe). Er wordt dus zeer kritisch gekeken naar onder andere dataminimalisatie en het gebruik van privacy verhogende maatregelen. Daarbij zijn de volgende uitgangspunten van toepassing: [6]

[6] Voor meer informatie over Privacy by Design zie de CIP Handleiding Privacy by Design van het Centrum Informatiebeveiliging en Privacybescherming.

Uitgangspunt	Beschrijving
Proactief en preventief	Privacy is vanaf de initiatie een aandachtspunt en niet alleen achteraf. Begin met privacy in een zo vroeg mogelijk stadium, dus bij de beleidsvorming en de eerste opzet van de systeemarchitectuur.
Privacy by default	Als de betrokkene een keuze kan maken uit meerdere opties, dan is de default keuze om de privacy zo goed mogelijk te beschermen. De betrokkene hoeft standaard zelf niets te doen om de privacy te beschermen.
Privacy geïntegreerd in het ontwerp	Privacy maatregelen zijn integraal onderdeel van de informatieverwerking. Dit geldt voor de technische systemen én de organisatorische processen.
Volledige functionaliteit – win/win in plaats van compromissen	Het waarborgen van de privacy is een verantwoordelijkheid van alle betrokkenen partijen. Het zorgt voor een systeem dat in zijn geheel beter functioneert.
Bescherming tijdens de volledige levenscyclus	Privacy by Design waarborgt de privacy, inclusief de beveiliging, gedurende de gehele levenscyclus van de persoonsgegevens van collectie/creatie tot vernietiging. Het is geen eenmalige actie.
Zichtbaarheid en transparantie: hou het open	Inzicht en transparantie over hoe persoonsgegeven worden verwerkt moet mogelijk zijn voor zowel de betrokkene, de eigen organisatie en de toezichthouder.
Respect voor de privacy: de betrokkene staat centraal	Technische en organisatorische maatregelen zijn pas effectief, wanneer zij de persoonlijke levenssfeer van eenieder als uitgangspunt nemen.

Privacy architectuur:

Hierin worden de relaties beschreven tussen processen, applicaties en data. De architectuur vormt de basis voor het register van verwerkingsactiviteiten.
Een aantal principes die hierbij gehanteerd worden:

- *Het Privacy by Design principe wordt gehanteerd.*

Bij initiatie van projecten met een ICT of data impact, wordt gebruik gemaakt van een PSA;

een project start architectuur. Onderdeel daarvan is een PIA; een privacy impact assessment. De PIA is een verplicht instrument om vooraf na te denken over de privacy-risico's van een bepaalde gegevensverwerking. Wanneer er sprake blijkt van privacy gegevens in een project, wordt ernaar gestreefd om de risico's zo veel mogelijk te verkleinen.

- *Dataminimalisatie* wordt toegepast bij alle persoonsgegevens.
  Alleen de nodige gegevens worden verwerkt.
- De gegevens worden *beschermd tegen ongeautoriseerd* gebruik.
  Hiermee zijn zowel op applicatie niveau als op data niveau de gegevens beschermd tegen misbruik en manipulatie.
- De gegevens worden maximaal volgens de *bewaartermijn* van de wet bewaard.
  De bewaartermijnen die in het systeem worden gehanteerd hebben een wettelijke grondslag. Zodra de gegevens de bewaartermijn hebben bereikt, worden ze uit het systeem verwijderd.
- Services van anderen worden niet vertrouwd. Bij een ingekochte component zijn afspraken gemaakt over hoe de gegevens worden opgeslagen. Ook hier staat centraal de risico's rond privacy zo klein mogelijk te houden.

5.7 Beveiliging van de verwerking, pseudonimisering, crypto en anonimisering.

Informatiebeveiliging is het geheel van preventieve, detectieve, repressieve en correctieve maatregelen, alsmede procedures en processen om eventuele gevolgen van beveiligingsincidenten tot een (acceptabel) vooraf bepaald niveau te beperken. De maatregelen zijn gebaseerd op risicoanalyses en wettelijke verplichtingen (waaronder de AVG). Doel van de beveiliging van de verwerking van persoonsgegevens is om persoonsgegevens te beschermen tegen verlies, onbeschikbaarheid, corruptie en enige vorm van onrechtmatige of onnodige verzameling en (verdere) verwerking.

Persoonsgegevens worden binnen WSRL organisatorisch beveiligd door middel van maatregelen voor de inrichting van de organisatie die zijn opgenomen in het Informatiebeveiligingsbeleid.
Voor de inrichting van informatiebeveiliging steunt WSRL op de Baseline Informatiebeveiliging Waterschappen (BIWA).

De maatregelen waarborgen een passend beveiligingsniveau en bevatten onder meer:

- Pseudonimisering en versleuteling van persoonsgegevens;
- Technische maatregelen in en rondom informatiesystemen, zoals toegangscontroles, vastlegging van gebruik en back up, wachtwoordbescherming en encryptie. De beveiliging is niet beperkt tot de eigen informatiesystemen, maar strekt zich uit tot extern geplaatste back-up en de opslag en verwerking bij en door derden.
- Het vermogen om de vertrouwelijkheid, integriteit, beschikbaarheid van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een (fysiek of technisch) incident de beschikbaarheid en toegang tot de persoonsgegevens tijdig te herstellen;

- Een procedure voor het testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.
  Gebruik te maken van BIV classificatie. Gevoeligheid van de data bepaalt de zwaarte van de maatregelen. Middels een BIV classificatie wordt de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van informatie en systemen aangegeven.

Geheimhouding
Via de BIWA zijn de medewerkers al verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen. De geheimhoudingsplicht is voor vaste werknemers van WSRL verankerd in de ambtseed of –belofte. Tijdelijke krachten (gedetacheerde medewerkers en stagiaires) die toegang hebben tot persoonsgegevens moeten een geheimhoudings- en integriteitsverklaring ondertekenen.

Verwerkersovereenkomsten
In de verwerkersovereenkomsten die worden gesloten met verwerkers zijn specifieke technische en organisatorische maatregelen benoemd om de persoonsgegevens die worden verwerkt ten dienste van het waterschap te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. (zie verder in par. 5.9)

5.8 Meldplicht datalekken

We spreken van een incident als er een inbreuk is op de beveiliging van informatie. Bij een datalek zijn er persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden (Autoriteit Persoonsgegevens, 2016).

WSRL heeft bij een datalek een meldplicht naar de Autoriteit Persoonsgegevens. Deze meldplicht houdt in dat WSRL binnen 72 uur een melding moet doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek constateert. Als het datalek negatieve gevolgen heeft of kan hebben voor de betrokkene(-n) (bijvoorbeeld financiële fraude of identiteitsfraude) meldt WSLR het datalek ook “onverwijld” aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

In het Calamiteitenplan niet-watergerelateerde zaken is in hoofdstuk 4 de procedure voor het melden van datalekken omschreven. De stappen, taken en verantwoordelijkheden bij het melden van een datalek zijn hierin opgenomen.

Voor meldingen met betrekking tot beveiligingsincidenten met of zonder persoonsgegevens is er een eenduidig loket (de IT-servicedesk i.s.m. de calamiteitenorganisatie) dat openstaat voor interne en externe meldingen.

De Autoriteit Persoonsgegevens heeft aangegeven dat er geen incidenten gemeld mogen worden die geen datalek zijn. De keuze voor de classificatie ‘datalek’ moet dus zorgvuldig gemaakt worden. Datalekken die worden gemeld aan de Autoriteit Persoonsgegevens worden geregistreerd als zaaktype “Melding datalek” in Verseon.

De uiteindelijke verantwoordelijkheid voor het (niet) doen van een datalekmelding ligt bij het College van dijkgraaf en heemraden. De FG adviseert hierin het CDH.

5.9 Verwerkersovereenkomsten

Waterschap Rivierenland kan taken en processen uitbesteden aan externe verwerkers die daarvoor de beschikking krijgen over persoonsgegevens waar zij verantwoordelijk voor is. Gedacht kan worden aan een callcenter dat wordt ingeschakeld of een bureau dat een dienst verleent in opdracht van het waterschap. De verwerker is daarbij niet direct aan het gezag van de verantwoordelijke onderworpen maar verwerkt de gegevens ten behoeve van de verantwoordelijke. Met deze verwerkers worden afspraken gemaakt over de privacy en informatiebeveiliging conform de AVG en de BIWA. Met iedere verwerker moet vóór de verwerking start een verwerkersovereenkomst zijn afgesloten.

Verwerkersovereenkomst
Een verwerkersovereenkomst bestaat altijd naast een contract voor product en/of dienstverlening.

In opdracht van HWH is een modelverwerkersovereenkomst opgesteld. Deze is vastgesteld in het Coördinatorenoverleg Privacy waterschappen en wordt als model gehanteerd. Het model wordt jaarlijks geëvalueerd en waar nodig op basis van eventuele nieuwe wetgeving en/of jurisprudentie aangepast. De privacy officer kan ondersteuning bieden aan de procesmanager en/of contracteigenaar bij het opstellen van de verwerkersovereenkomst.

De verwerkersovereenkomst wordt altijd samen met het contract geregistreerd in Verseon . De verwerkersovereenkomsten worden onder een eigen zaaktype ‘verwerkersovereenkomst’ geregistreerd. Tevens worden beide opgevoerd in het contractenregister bij inkoop, zodat altijd een goed overzicht bestaat van de geldende (en aflopende) afspraken met verwerkers. Tevens wordt bij een inkoopmelding aangegeven of het een inkoop betreft met privacy- of informatiebeveiligings-elementen. Op basis van deze inkoopmelding wordt advies gegeven over het te volgen traject.

5.10 Register van verwerkingsactiviteiten, aanleg en onderhoud

Om de naleving van de AVG aan te kunnen tonen, moet de verwerkingsverantwoordelijke een register bijhouden van verwerkingsactiviteiten die onder zijn verantwoordelijkheid hebben plaatsgevonden. Dit kan via een gegevensmanagement worden vastgelegd. De vastlegging maakt duidelijk hoe de verschillende organisatieonderdelen de bedrijfsprocessen ondersteunen en welke beveiligingsmaatregelen (op hoofdlijnen) zijn getroffen voor de verwerkers en betrokkenen. Het register maakt toezicht op de verwerkingsactiviteiten mogelijk. Het register moet een actueel en samenhangend beeld geven van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens. Het doel van een “Register van verwerkingsactiviteiten” is inzicht te verstrekken in de gegevensstromen binnen de organisatie en bij partijen die namens het waterschap zorgen voor de verwerking van persoonsgegevens.
Het register van verwerkingen bevat de volgende gegevens:

1) Naam en contactgegevens van:

a) De verwerkingsverantwoordelijke en evt. gezamenlijke verwerkingsverantwoordelijken, en:
b) In voorkomend geval:
   - van de vertegenwoordiger van de verwerkingsverantwoordelijke, en:
   - de FG;

2) De verwerkingsdoeleinden
3) Een beschrijving van de categorieën van betrokkenen;
4) Een beschrijving van de categorieën van persoonsgegevens;
5) De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt.
6) De beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens moeten worden gewist (indien mogelijk);
7) Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

6. Controle op de naleving en evaluatie

De AVG verplicht het waterschap om steeds te kijken of het beleid nog voldoet en of het aangepast moet worden. Technologische en maatschappelijke ontwikkelingen volgen elkaar snel op. Dit kan reden zijn om het beleid aan te passen. Het privacybeleid moet daarom in ieder geval eens per twee jaar worden geëvalueerd. Er is immers sprake van nieuwe wetgeving, die volop in beweging is en waar door de rechtspraak en de toezichthouder nog nader invulling aan zal worden gegeven.

Het privacybeleid mag geen papieren tijger worden en in een digitale bureaulade verdwijnen. Daarom is controle op de naleving van enorm belang. Het organiseren van controle en naleving is bovendien een verplichting op grond van de AVG. Controle en evaluatie van het privacybeleid wordt op onderstaande wijze geborgd.

Managementproces Waterschap Rivierenland
Het voldoen aan de AVG wordt als prestatie-indicator opgenomen in de Voorjaarsnota van Water schap Rivierenland . Op deze wijze is privacy opgenomen in de PDCA-cyclus van het Waterschap.

PDCA-cyclus
Plan: De plan-fase van de cyclus is de fase van beleidsvorming. In het beleid legt het waterschap de doelstellingen, uitgangspunten en beginselen vast bij de verwerking van persoonsgegevens. Auteur van het beleid is de privacy officer, geadviseerd door het privacy team, het bestuur stelt het beleid vast. *Do*: tijdens de Do-fase worden de uitgangspunten en beginselen vertaald naar concrete procesinrichting en worden deze geïmplementeerd. Implementatie van maatregelen is de verantwoordelijkheid van het lijnmanagement, het privacy team heeft hierbij een adviserende rol.
Check: in de Check-fase stellen we vast in hoeverre de geïmplementeerde maatregelen effectief zijn om de doelstellingen uit de planfase te bereiken. De FG is leidend in het (laten) uitvoeren van deze audit en wordt daarbij ondersteund door het privacy team.
Act: In deze laatste fase van de cyclus worden bijstellingen gedaan naar aanleiding van bevindingen uit de Check-fase. Ook wordt input verzameld voor de Plan-fase van de volgende cyclus. Het bijstellen van procesinrichting is een lijnverantwoordelijkheid, het privacy team heeft ook hierbij een adviserende rol.

Monitoring voortgang implementatie AVG door het Waterschapshuis (HWH)
Vanuit het HWH wordt de voortgang van de implementatie van de AVG gemonitord, mogelijk door middel van een gezamenlijke privacy audit. De FG en de PO participeren in de werkgroep binnen HWH.

Toezicht en controle door de FG
De FG toetst de naleving en de werking van het Privacybeleid en of dit afdoende binnen het waterschap is ingericht. Hij heeft vrij toegang tot alle systemen en processen van het waterschap. De FG draagt zorg voor een jaarlijkse evaluatie van het Privacybeleid, doet daarvan verslag aan het CDH en geeft aanbevelingen voor een verdere optimalisering van de uitvoering van het privacybeleid. De FG stimuleert het waterschap om te werken in lijn met de beginselen van de AVG en geeft specifieke adviezen om de rechten en

vrijheden van betrokkenen te beschermen. In lijn met de AVG draagt de FG actief bij aan het ontwikkelen van een branchegericht normenkader voor privacy, waarop WSRL getoetst kan worden.

Verklaring privacy teamleiders en afdelingshoofden
Afdelingshoofden zijn proceseigenaar van verwerkende processen binnen het waterschap. Teamleiders zijn operationeel verantwoordelijk voor de uitvoering van de processen. In het kader van de reguliere controlcyclus wordt vastgesteld of processen worden uitgevoerd conform de voorschriften in dit beleid. Over dit onderzoek wordt gerapporteerd aan het afdelingshoofd. Hieruit voortkomende acties worden opgenomen in de voortgangsrapportage.

Werkoverleg
Leidinggevenden en medewerkers maken privacy tot een onderdeel van het werkoverleg. Bevindingen of vragen kunnen worden voorgelegd aan de FG. De FG sluit periodiek en op verzoek aan bij werkoverleggen van afdelingen.

7. Financiële consequenties

Met het implementeren en het uitvoeren van het Privacybeleid dient rekening te worden gehouden met extra kosten. Voor een groot deel zijn deze kosten al voorzien in de begroting onder bedrijfsvoering.

Overzicht Kosten:	Begroot
In de begroting Bedrijfsvoering:	
- Interne bewustwordingscampagnes privacy bestendig werken	€ 10.000
- Ondersteuning	€ 50.000
In de begroting Concerncontrol:	
- Privacy audit	€ 20.000

Bijlage A : Afkortingenlijst

AP - Autoriteit Persoonsgegevens

AVG - Algemene Verordening Gegevensbescherming

BIWA - Baseline Informatiebeveiliging Waterschappen

BRP - Basisregistratie Persoonsgegevens

BSN - Burgerservicenummer

CISO - Chief Information Security Officer

FG - Functionaris Gegevensbescherming

GBA - Gemeentelijke Basisadministratie Persoonsgegevens

GIS - Geografisch Informatiesysteem

IBAN - Internationaal Bank Account Nummer

NAW - Naam, Adres en Woonplaats

OR - Ondernemingsraad

PIA - Privacy Impact Analyse

Wbp - Wet bescherming persoonsgegevens

Wob - Wet openbaarheid bestuur

WOR - Wet op ondernemingsraden

Bijlage B: Begrippenlijst

Autoriteit Persoonsgegevens (AP):
De Autoriteit Persoonsgegevens is de toezichthoudende autoriteit, bedoeld in artikel 51, eerste lid van de AVG, die tot taak heeft toe te zien op de naleving van de verordening en op de verwerking van persoonsgegevens overeenkomstig hetgeen is bepaald bij en/of krachtens de AVG en de Uitvoeringswet AVG.

AVG:
Algemene Verordening Gegevensbescherming, (EU) 2016/679 goedgekeurd door het Europees parlement de Europese Raad op 27 april 2016.

Bestand:
Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Betrokkene:
Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft. Dit is zowel een natuurlijke persoon als een éénmanszaak.

Datalek:
Een inbreuk op de beveiliging waarbij persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Wanneer de inbreuk op de persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen meldt de verwerkingsverantwoordelijke deze binnen 72 uur nadat hij van de inbreuk kennis heeft genomen aan de AP. Wanneer er sprake is van een hoog risico deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk onverwijld mee en de AP binnen 72 uur.

Dataportibaliteit:
Betrokkenen hebben recht op persoonsgegevens die een organisatie van hen heeft. Organisaties moeten op verzoek van betrokkenen de persoonsgegevens verstrekken in een vorm die het voor betrokkenen makkelijk maakt om hun gegevens te hergebruiken en door te geven aan een andere organisatie. Organisaties zijn daarom wettelijk verplicht om de gegevens in een gestructureerd, veelgebruikt en machineleesbaar formaat te verstrekken.

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

Gegevensbeschermingeffectbeoordeling (GEB):
Een toetsmodel in de vorm van vragenlijsten die de privacy risico's van een specifieke verzameling, de (verdere) verwerking en bewaring van persoonsgegevens op systematische wijze identificeert en lokaliseert (voorheen Privacy Impact Analyse).

Ontvanger:
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

Persoonsgegevens:
Alle informatie over een geïdentificeerde of identificeerbare natuurlijk 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 of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

(zie verder toelichting bijzondere en gevoelige persoonsgegevens)

Privacy by default:
Privacy by default houdt in dat er technische en organisatorische maatregelen genomen moeten worden om ervoor te zorgen dat, als standaard (by default), alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het bereiken van het specifieke doel.

Privacy by design:
Privacy by design houdt in dat al tijdens de ontwikkeling van producten en diensten aandacht wordt besteed aan privacy verhogende maatregelen. Ook wordt er rekening gehouden met dataminimalisatie (dat wil zeggen dat alleen die persoonsgegevens verwerkt worden die noodzakelijk zijn voor het doel van de verwerking).

Privacyincident:
Iedere vraag, klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen waterschap Rivierenland wordt beschouwd als een privacyincident. De bekendste vorm van een privacyincident is een datalek.

Privacy Enchancing Technologies (PET):
Een verzamelnaam voor een aantal technieken voor privacybescherming die kunnen worden toegepast. Een centraal principe van PET is het verminderen van de herleidbaarheid van persoonsgegevens naar de betrokkene, met anonimisering van gegevens als zwaarste vorm: na anonimisering zijn de gegevens niet meer te herleiden tot de oorspronkelijke gegevens.
Een vergelijkbare techniek is pseudonimisering. De AVG definieert pseudonimisering als "het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, op voorwaarde dat deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. [7]

Toestemming van de betrokkene:
Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van

[7] Artikel 4 lid 5 AVG

een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

Verstrekken van persoonsgegevens:
Het bekend maken of ter beschikking stellen van persoonsgegevens.

Verwerking:
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd door geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiden of andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens. In feite iedere handeling t.a.v. persoonsgegevens.

Verwerker:
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke gegevens verwerkt. Een voorbeeld is de organisatie die zorgt voor de verwerking van de salarisadministratie, of bedrijven die ondersteunende diensten leveren ten aanzien van personeelsmanagementsystemen, etc.

Verwerkersverantwoordelijke:
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van de middelen voor de verwerking van Waterschap Rivierenland persoonsgegevens vaststelt. Wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen, In het geval van Waterschap Rivierenland is dit het dagelijks bestuur. Ondanks gemandateerde taken en bevoegdheden wordt het dagelijks bestuur aangemerkt als Verwerkingsverantwoordelijke in de zin van de AVG.

Verwerkersovereenkomst:
De uitvoering van een verwerking door een verwerker wordt geregeld in een verwerkersovereenkomst, overeenkomstig het bepaalde in artikel 28 AVG. Dat wil zeggen, indien een organisatie persoonsgegevens voor waterschap Scheldestromen verwerkt, is er een verplichting om naast de bestaande dienstverleningsovereenkomst ook een aparte verwerkersovereenkomst te sluiten. De verwerkersovereenkomst behelst expliciet afspraken met betrekking tot verwerken van persoonsgegevens en ook de procedure rond de meldplicht datalekken.

Bijlage C: Overzicht Wet- en Regelgeving

Hieronder een overzicht van weg- en regelgeving met een privacy component die van toepassing is op waterschappen.

A. Internationaal/Europees

- Artikel 17 van het VN verdrag voor Burgerlijke en Politieke rechten
- Artikel 8 van het Europees Verdrag voor de Rechten van de Mens
- Art.7 Handvest grondrechten van de Europese Unie
- Algemene Verordening gegevensbescherming
- Richtlijn Netwerk en informatiebeveiliging (NIB)
- Richtlijn gegevensbescherming politie en justitie
- Europese Verordening e-identity en vertrouwensdiensten
- E-privacyrichtlijn (wetgeving met betrekking tot cookies)
- (concept) E-privacyverordening (vervangt E-privacyrichtlijn)

B. Landelijk

- Artikelen 10 tot en met 13 van de Nederlandse Grondwet
- Uitvoeringswet Avg
- Awb (hoofdstuk 5)
- Algemene wet inzake rijksbelastingen
- Wet Politiegegevens
- Wet justitiële en strafvorderlijke gegevens
- Wetboek van Strafrecht
- Wetboek van Strafvordering
- Archiefwet (selectielijst waterschappen)
- Belastingwet
- Wet elektronische bekendmaking 2012
- Jaarrekeningrecht: Jaarverslag: verantwoording privacybeleid en security.
- Wet openbaarheid van bestuur
- Wet hergebruik overheidsinformatie
- Telecommunicatiewet (hoofdstuk 11)
  Wet gegevensverwerking en meldplicht cybersecurity
- Wet op de ondernemingsraad (instemmingsrecht)
- Portretrecht
- Auteursrecht
- Kieswet
- Wet geneeskundige behandelingsovereenkomst
  Wet basisregistratie personen en regelgeving die daarop gebaseerd is, bijvoorbeeld

1. Aanpassingsbesluit Politiewet 2012
2. Aanpassingsbesluit Zorgverzekeringswet
3. Aanpassingsregeling Zorgverzekeringswet
4. Beleidsregel UWV gebruik adresgegevens
5. Besluit basisregistratie personen
6. Besluit burger servicenummer

7. Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling
8. Regeling basisregistratie personen

C. Beleid Autoriteit Persoonsgegeven

De AP heeft diverse richtlijnen gepubliceerd, waaronder:

- Richtsnoeren beveiliging van persoonsgegevens
- Beleidsregels Meldplicht datalekken
- Richtlijnen actieve openbaarmaking persoonsgegevens
- Richtlijnen publicatie persoonsgegevens op internet
- Richtlijnen recht op dataportabiliteit
- Richtlijnen voor functionarissen voor de gegevensbescherming
- Richtlijnen De zieke werknemer
- Richtlijnen kopie identiteitsbewijs.

D. Richtlijnen en gedragscodes WSRL

Protocol personeelsvolgsystemen;
Calamiteitenplan niet-water gerelateerde zaken;
Gedragscode gebruik online en offline middelen;
Gedragscode integriteit voor medewerkers 2011;
Gedragscode integriteit voor politieke ambtsdragers;
Klokkenluidersregeling 2011;
Richtlijnen gebruik sociale media;

(Verder aanvullen)

Bijlage D: De AVG in relatie tot overige wetten

1. AVG versus BRP

Wet basisregistratie personen (Wet BRP)

De Wet basisregistratie personen (Wet BRP) is de opvolger van de gemeentelijke basisadministratie persoonsgegevens (GBA).) In de basisregistratie personen (BRP) zijn de persoonsgegevens van alle inwoners van Nederland vastgelegd. De Wet BRP regelt het juiste gebruik zoals het correct opnemen, wijzigen en verstrekken van persoonsgegevens. De Wet BRP kent een eigen stelsel van regels. Op de verwerking van persoonsgegevens die in de BRP staan, is de AVG niet van toepassing (Artikel 2 UAVG). De wet BRP heeft een eigen, streng, privacy-regime.

In het 'autorisatiebesluit Waterschap Rivierenland, Rijksdienst voor Identiteitsgegevens' staat aangegeven over welke gegevens WSRL mag beschikken en voor welke doeleinden. Daarnaast geeft het besluit aan of dit gaat om een geautomatiseerde verstrekking aan WSRL, of dat de gegevens opgevraagd dienen te worden (Autorisatiebesluit, 20..).

Stelsel van Basisregistraties
Het Stelsel van basisregistraties bestaat uit 12 basisregistraties. Een basisregistratie is een door de overheid officieel aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit, die door alle overheidsinstellingen verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken (Digitale overheid, 2016).

- BRP - Basisregistratie personen (bestaat uit ingezetenen en niet-ingezetenen);
- HR – Handelsregister;
- BAG - Basisregistraties Adressen en Gebouwen (bestaat uit twee basisregistraties);
- BRT - Basisregistratie Topografie;
- BRK - Basisregistratie Kadaster;
- BRV - Basisregistratie Voertuigen (kentekenregister);
- BLAU - Basisregistratie voor Lonen, Arbeidsverhoudingen en Uitkeringen;
- BRI - Basisregistratie Inkomen;
- WOZ - Basisregistratie Waarde Onroerende Zaken;
- BGT - Basisregistratie Grootschalige Topografie (voorheen GBKN);
- BRO - Basisregistratie Ondergrond (voorheen ook wel DINO).

2. AVG versus de Wet openbaarheid van bestuur

De Wet openbaarheid van bestuur (Wob) bepaalt dat burgers recht hebben op informatie van de overheid. Informatie over hoe de overheid handelt en waarom en hoe besluiten genomen worden. Met het oog op een goed en democratisch bestuur zijn de regels over de openbaarheid van bestuur zoveel mogelijk in de Wob opgenomen. Het uitgangspunt van de Wob is dat overheidsinformatie openbaar is, tenzij in de Wob of andere wetgeving bepaald is dat de informatie niet geschikt is om openbaar te maken. De overheid verschaft uit eigen beweging informatie over het beleid en de uitvoering daarvan. Geheimhouding is dus de uitzondering op de regel en moet bovendien worden gemotiveerd. Ook zijn er nadere regels opgesteld met betrekking tot de uitvoering van de wet.

De Wob is van toepassing op verzoeken tot openbaarmaking van informatie over bestuurlijke aangelegenheden bij de hiervoor in de wet aangewezen bestuursorganen. Iedereen kan een dergelijk verzoek indienen. Daarbij hoeft de verzoeker bij de openbaarmaking geen belang te hebben.

Zowel het recht op 'openbaarheid' als het recht op 'privacy' zijn grondrechten. Er treedt een spanning op als er gevraagd wordt om persoonsgegevens openbaar te maken. Het is niet zo dat het ene recht belangrijker is dan het andere. Er moet een belangenafweging plaatsvinden. Aan de ene kant het belang van de openbaarmaking en aan de andere kant het belang van de privacy van betrokkenen. De factoren van belangen zijn beschreven in Bijlage E.

3. AVG versus Archiefwet

De AVG kent een aantal specifieke uitzonderingen voor verwerking van persoonsgegevens met het oog op archivering in het algemeen belang. Een aantal uitzonderingen werkt rechtstreeks, zie artikel 89 AVG: "Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden'.

Bij verwerkingen met betrekking tot onderzoek en archivering moeten de rechten van betrokkenen worden gewaarborgd. Het accent hierbij ligt bij het beginsel van gegevensminimalisering (dataminimalisatie). Niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk is voor het doel. Zodra het mogelijk is om het archiveringsdoel te halen met ontkoppelde gegevens (ofwel geanonimiseerde gegevens, niet langer herleidbaar tot een natuurlijke persoon en dus niet langer persoonsgegevens) moet deze ontkoppeling worden uitgevoerd. Als tussenvorm mag gewerkt worden met pseudonimisering waarbij koppeling nog wel mogelijk is, maar de daarvoor benodigde informatie niet direct beschikbaar is.

Artikel 89 lid 3 AVG bevat een specifieke bepaling op grond waarvan de lidstaten kunnen afwijken van enkele voorschriften van de AVG. Het gaat hier om de mogelijkheid om af te wijken van de artikelen 15 (het recht op inzage), 16 (het recht op rectificatie), 18 (het recht op beperking van de verwerking), 19 (kennisgevingsplicht), 20 (het recht op overdraagbaarheid van de gegevens) en 21 (het recht op bezwaar).Er is voor gekozen om op grond van artikel 89 lid 3 AVG een aantal uitzonderingen op te nemen in artikel 45 van de UAVG[8] voor verwerking van persoonsgegevens die deel uitmaken van archiefbescheiden die berusten in een archiefbewaarplaats. Daarbij wordt aangesloten bij de begrippen zoals deze gedefinieerd zijn in de Archiefwet 1995.

Het waterschap moet kritisch blijven kijken binnen de eigen werkprocessen voorafgaand aan archivering en deze toetsen op dataminimalisatie, zodat kan worden aangetoond dat ook voor wat betreft het archief van het waterschap voldaan is aan de vereiste passende waarborgen die voortkomen uit de AVG en de UAVG.

1. De AVG versus de Wet politiegegevens

Daarnaast hebben wetten als de Wet politiegegevens een eigen privacy regime. De AVG is hierop niet van toepassing. [9]

---

8) Memorie van Toelichting Uitvoeringswet Algemene Verordening Gegevensbescherming.

9) Artikel 2 lid 2 onderdeel d AVG.

Bijlage E: Factoren die een rol spelen bij de belangenafweging Wob

De Wob bepaalt dat een ieder (burgers, bedrijfsleven) recht heeft op informatie van de overheid (bestuursorganen). De Wob zorgt ervoor dat burgers inzage hebben in het handelen van de overheid. Zo kan de burger beslissingen controleren. Het uitgangspunt van de Wob is dat documenten bij de overheid openbaar zijn. Uitzonderingen gelden alleen als de Wob of bijzondere wetten bepalen dat de gevraagde informatie niet geschikt is voor openbaarmaking.

De Wob kent enkele weigeringsgronden en beperkingen. Er bestaan twee weigeringsgronden met betrekking tot de persoonlijke levenssfeer. De ene is een absolute weigeringsgrond. Het bestuursorgaan is gehouden geen gegevens openbaar te maken betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, mogelijke strafrechtelijke achtergrond en iemands persoonlijk identificatienummer. De andere weigeringsgrond is een relatieve weigeringsgrond. Deze betreft een afweging van twee belangen: Het belang van miljoenen Nederlanders om iets te weten over één persoon versus het belang van de betrokken persoon om met rust te worden gelaten. Deze belangenafweging wordt gedaan door het bestuursorgaan, dat daarbij een grote vrijheid heeft.

In artikel 10, tweede lid, aanhef en onder e van de Wob, bevat de zogenaamde relatieve weigeringsgrond. Dat artikellid luidt*: "Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen: e. de eerbiediging van de persoonlijke levenssfeer*"

Bij een absolute weigeringsgrond hoeft alleen maar vermeld te worden dat het gaat om een gegeven als bedoeld in artikel 10, eerste lid, aanhef en onder d van de Wob. Het is niet nodig te melden om wat voor gegeven het gaat, en een motivering blijft achterwege. Het betreft uitsluitend een vaststelling dat een bepaald gegeven aan de orde is.

Bij andere persoonsgegevens moet een belangenafweging plaatsvinden: Aan de ene kant het publieke belang van een goede en democratische bestuur voering (wordt verondersteld aanwezig te zijn) en aan de andere kant het privacybelang van de betrokkene. In een dergelijk geval moet dus een motivering volgen. Dat vereist een kwaliteitstoets.

Belangrijke factoren bij de belangenafweging zijn:

- Is sprake van een persoonsgegeven?
- Is sprake van een inbreuk op een persoonsgegeven?
- Is deze inbreuk bij wet voorzien?
- Is deze inbreuk te rechtvaardigen vanuit een legitiem doel?
- Is deze inbreuk noodzakelijk in een democratische samenleving? Daarbij kan worden gelet op de volgende factoren (niet limitatief):
- De aard van de gegevens waarvan openbaarmaking wordt gevraagd;

- De gevolgen van de beoogde verwerking voor de betrokkene wiens gegevens openbaar gemaakt zouden moeten worden;
- De wijze waarop de gegevens van de betrokkene zijn verkregen.

Bijlage F: Toelichting op een aantal begrippen en beginselen uit de AVG

1. Persoonsgegevens:

De AVG[1°] formuleert persoonsgegevens als volgt*: "alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; 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 of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon"*

Alle gegevens die informatie kunnen verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de AVG, zoals naam, adres, woonplaats, een vingerafdruk, e-mailadres, handtekening, telefoonnummer, BSN, kenteken, alsmede zogenaamde bijzondere persoonsgegevens over onder meer godsdienst, inkomen, gezondheid, vakbondslidmaatschap en geslacht, seksuele geaardheid. De AVG vereist dat al die gegevens behoorlijk en zorgvuldig worden verwerkt. Voor het verwerken van bijzondere persoonsgegevens geldt een verbod.

Een postcode alleen is bijvoorbeeld niet direct herleidbaar tot een natuurlijke persoon. Er is meer informatie nodig om dat te kunnen doen. Bijvoorbeeld een huisnummer. Of de verwerkingsverantwoordelijke de middelen en de mogelijkheden heeft om iemand te kunnen identificeren, is niet doorslaggevend. Er moet gekeken worden naar alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon. Een kenteken is een persoonsgegeven, maar dus zelfs ook wanneer de verwerkingsverantwoordelijke zelf geen toegang heeft tot de bestanden van de Rijksdienst voor het Wegverkeer.

1.1 Bijzondere persoonsgegevens (artikel 9 AVG)

De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en de verwerking van genetische of biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

In de AVG wordt een aantal categorieën van persoonsgegevens gehanteerd, die extra privacygevoelig zijn. In principe is het verboden om deze gegevens te verwerken. De AVG en de Uitvoeringswet AVG bepalen in welke gevallen bijzondere of gevoelige gegevens verwerkt mogen worden. Er zijn uitzonderingen op dit verbod, bijvoorbeeld in het geval betrokkene uitdrukkelijke toestemming heeft gegeven, of in het geval de

---

1° Artikel 4 lid 1 AVG

gemeente de gegevens moet verwerken voor het uitvoeren van een wettelijke taak[11]. Het waterschap zal uiterst zorgvuldig omgaan met bijzondere persoonsgegevens.

Nieuw is dat genetische en biometrische gegevens tot de bijzondere persoonsgegevens worden gerekend. Bij biometrische gegevens moet gedacht worden aan een pasfoto op een rijbewijs of paspoort, of een vingerafdruk. Het wordt enkel gebruikt om iemand te identificeren. Ook hier geldt dus: verwerking is verboden, tenzij.

Net als onder de Wbp behoren strafrechtelijke gegevens tot de bijzondere persoonsgegevens (artikel 10 AVG). Persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1 AVG, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid.

Ook al wordt het onder de AVG geen bijzonder persoonsgegeven genoemd, voor het burgerservicenummer (BSN) blijft gelden dat het enkel gebruikt mag worden wanneer het door de wet is voorgeschreven, en enkel voor de doeleinden gebruikt mag worden die die wet bepaalt 29 . Nederland gaat hier dus verder dan de AVG, en heeft gebruik gemaakt van de beleidsvrijheid die de AVG biedt[12].

Gezien het risico van het verwerken van bijzondere persoonsgegevens voor betrokkenen, zal het waterschap deze niet door derden laten verwerken, tenzij er zwaarwegende belangen zijn. Dit ter beslissing van de FG. Indien desondanks bijzondere persoonsgegevens bij een verwerker worden verwerkt, dient het beschermingsniveau gegarandeerd te zijn.

1.2 Gevoelige persoonsgegevens

Onder gevoelige persoonsgegevens worden ten eerste de bijzondere persoonsgegevens gerekend. Daarnaast behoren financiële persoonsgegevens tot de gevoelige gegevens (bijvoorbeeld salarisstroken, etc). Verder persoonsgegevens op grond waarvan mensen kunnen worden ‘nagewezen’ (stigmatisering), zoals gegevens over een goksverslaving. Tenslotte worden wachtwoorden, inloggegevens, burger servicenummers, kopieën van identiteitsbewijzen, en bankrekeningnummers tot de gevoelige gegevens gerekend. Indien iemand ten onrechte toegang krijgt tot deze gegevens, kan daarmee identiteits-fraude gepleegd worden. Dat is een groot risico.

Of een persoonsgegeven gevoelig van aard is speelt onder andere een rol bij de bepaling of het waterschap persoonsgegevens die voor een bepaald doel zijn verzameld ook mag verwerken voor een ander doel (zie paragraaf). Hoe gevoeliger het persoonsgegeven, hoe minder snel het waterschap mag aannemen dat er sprake is van een verenigbaar doel.

---

11) Zie artikel 9 lid 2 AVG, samen met artikel 22 e.v. Uitvoeringswet AVG (UAVG).
12 Zie artikel 46 UAVG

2. Verwerking (van persoonsgegevens)

De AVG definieert verwerking als volgt*: 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens*[13]*.'*
Kort gezegd: iedere handeling met persoonsgegevens geldt als verwerken. De lijst die wordt opgesomd in de definitie is niet limitatief.

2.1 Verwerkingsgrondslagen

Een van de eisen die de AVG stelt is dat persoonsgegevens rechtmatig worden verwerkt. Artikel 6 AVG geeft in dat kader de grondslagen voor verwerking. Persoonsgegevens mogen alleen worden verwerkt indien één van die grondslagen van toepassing is.

a) Toestemming van de betrokkene
b) Noodzakelijk voor de uitvoering van de overeenkomst
c) Noodzakelijk in verband met het voldoen aan een wettelijke verplichting
d) Bescherming van een vitaal belang
e) Vervulling van een taak van algemeen belang of de uitoefening van openbaar gezag
f) Gerechtvaardigd belang

sub a). Toestemming van de betrokkene:
De AVG verstaat onder toestemming 'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.'

Wat wordt verstaan onder toestemming van de betrokkene?

- Je moet kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. Het moet gaan om toestemming voor de verwerking van zijn of haar persoonsgegevens voor één of meer specifieke doeleinden. Dat wil zeggen: deze mag niet te ruim en algemeen geformuleerd zijn, en het moet voor de betrokkene duidelijk zijn welke persoonsgegevens voor welke doeleinden verwerkt worden. Toestemming is ondubbelzinnig wanneer er geen onduidelijkheid kan bestaan of de betrokkene daadwerkelijk toestemming heeft gegeven voor een specifieke verwerking.;
- De betrokkene kan ten allen tijde zijn toestemming weer intrekken. Voordat hij zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het is even eenvoudig om

[13] artikel 4 lid 2 AVG

toestemming in te trekken als om toestemming te geven. Als toestemming wordt ingetrokken betekent dit dat er dan geen grondslag voor verwerking overblijft. (Toestemming is dus een risicovolle grondslag).

- Soms geeft een betrokkene toestemming in het kader van een schriftelijke verklaring die ook op andere aangelegenheden betrekking heeft. Het verzoek om toestemming moet dan in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig worden gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met die andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend.
- Bij de beoordeling van de vraag of toestemming vrijelijk kan worden gegeven, wordt onder meer rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst.

Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt. Hiertoe zou kunnen behoren het klikken op een vakje bij een bezoek aan een internetwebsite, het selecteren van technische instellingen voor diensten van de informatiemaatschappij of een andere verklaring of een andere handeling waaruit in dit verband duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens. Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag niet als toestemming gelden. De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen. Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend. Indien de betrokkene zijn toestemming moet geven na een verzoek via elektronische middelen, dient dat verzoek duidelijk en beknopt te zijn en niet onnodig storend voor het gebruik van de dienst in kwestie.

Nieuw is dat het waterschap zal moeten kunnen aantonen dat de betrokkene toestemming heeft gegeven. Een verleende toestemming moet dus goed worden vastgelegd. Het is daarbij ook van belang het verzoek om toestemming zo eenvoudig, duidelijk en specifiek mogelijk te formuleren. Verder is van belang dat degene die toestemming verleent hiervoor een duidelijke actieve handeling moet verrichten. Bijvoorbeeld: het op een webformulier vast aanvinken van het hokje ‘ik verleen toestemming’ is niet toegestaan. Betrokkene moet zelf het vinkje zetten.

Sub b) Noodzakelijk voor de uitvoering van een overeenkomst:
De verwerking kan noodzakelijk zijn in verband met de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

sub c) Noodzakelijk in verband met het voldoen aan een wettelijke verplichting:
Het moet dan gaan om een gegevensverwerking die noodzakelijk is om te kunnen voldoen aan een wettelijke plicht van de verantwoordelijke. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag.

Hiervan is bijvoorbeeld sprake als het waterschap een bij wet geregelde - publiekrechtelijke - taak uitvoert. Er moet sprake zijn van een typische overheidstaak.[14]

Doorgaans is de wettelijke verplichting tot verstrekking van persoonsgegevens zeer precies vastgesteld in sectorspecifieke regelgeving. In sommige gevallen geldt er echter een zorgplicht, waardoor de verwerkingsverantwoordelijke een grotere eigen verantwoordelijkheid heeft inzake het beoordelen van de noodzakelijkheid van de verwerking in het licht van het voldoen aan de wettelijke verplichting.

sub d) Bescherming van een vitaal belang:
De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

sub e) Vervulling van een taak van algemeen belang of openbaar gezag.

sub f) Gerechtvaardigd belang:
Let op!!: Deze grondslag geldt niet voor de verwerking van gegevens door overheidsinstanties in het kader van de uitoefening van hun taken. Er mag door overheden dus geen beroep op worden gedaan voor zover het gaat om de uitoefening van de taken van het waterschap. Voor bedrijfsprocessen die niet direct gerelateerd zijn aan een wettelijke taak mag de grondslag "gerechtvaardigd belang" wel gebruikt worden. (Bijvoorbeeld een bezoekersregister).

2.2 Doelbinding

Persoonsgegevens mogen enkel voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Verzamelen is ook verwerken! Voordat er aan verwerking van persoonsgegevens gedacht kan worden, moet er dus eerst duidelijkheid zijn over een specifiek en concreet, dus precies omschreven doel . Wanneer er geen wettelijke grondslag is, is er in ieder geval geen sprake van een gerechtvaardigd doel.

Vervolgens kunnen deze persoonsgegevens verder worden verwerkt (bijvoorbeeld door het verstrekken aan derden). Dat mag alleen maar wanneer het doel voor deze verdere verwerking verenigbaar is met het met het doel waarvoor de gegevens aanvankelijk zijn verzameld. Dit bij elkaar wordt doelbinding genoemd.

---

[14] Als de verwerking wordt verricht omdat de verwerkingsverantwoordelijke hiertoe wettelijk is verplicht of als de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of voor een taak in verband met de uitoefening van het openbaar gezag, moet de verwerking een grondslag hebben in het Unierecht of het nationale recht. De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verschillende verwerkingen op grond van een wettelijke verplichting die op de verwerkingsverantwoordelijke rust, of voor verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang of voor een taak in het kader van de uitoefening van het openbaar gezag. Het moet ook het Unierecht of het recht van de lidstaat zijn die het doel van de verwerking bepaalt. Dat recht zou een nadere omschrijving kunnen geven van de algemene voorwaarden van de AVG waaraan de persoonsgegevensverwerking moet voldoen om rechtmatig te zijn, en specificaties kunnen vaststellen voor het bepalen van de verwerkingsverantwoordelijke, het type verwerkte persoonsgegevens, de betrokkenen, de entiteiten waaraan de persoonsgegevens mogen worden vrijgegeven, de doelbinding, de opslagperiode en andere maatregelen om te zorgen voor rechtmatige en behoorlijke verwerking.

Verdere verwerking ziet dus op alle verwerkingen van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld[15] Dit kan verwerking door één en dezelfde verwerkingsverantwoordelijke zijn, maar kan ook de basis zijn voor verstrekking van gegevens aan een andere verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke die de gegevens ontvangt, zal voor de verwerking van de ontvangen gegevens ook weer een zelfstandige grondslag nodig hebben.

3. Verwerkersverantwoordelijke en verwerker:

Binnen de AVG wordt onderscheid gemaakt tussen de verwerkingsverantwoordelijke en de verwerker.

3.1 Verwerkingsverantwoordelijke (artikel 4 lid 7 AVG):

De verwerkingsverantwoordelijke is de entiteit (natuurlijke persoon, rechtspersoon, instantie of (bestuurs)orgaan) die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen. In het geval van Waterschap Rivierenland is dit het dagelijks bestuur. Ondanks gemandateerde taken en bevoegdheden wordt het dagelijks bestuur aangemerkt als verwerkingsverantwoordelijke in de zin van de AVG. [16]
De verwerkingsverantwoordelijke dient te zorgen voor passende waarborgen voor het naleven van de AVG. Dat de waarborgen zijn ingesteld moet door de verwerkingsverantwoordelijke kunnen worden aangetoond. In feite is de verwerkingsverantwoordelijke aanspreekbaar op het handhaven van de zes basisbeginselen binnen de AVG (zie paragraaf 2.1.2).

3.2 Verwerker (artikel 4 lid 8 AVG jo. Artikel 28 AVG)

Een verwerker is een entiteit (natuurlijke persoon, rechtspersoon, instantie of (bestuurs)orgaan) die een verwerking uitvoert binnen het doel en middelen die de verwerkingsverantwoordelijke heeft vastgesteld. Een verwerker heeft geen zeggenschap over de wijze van verwerken, en werkt strikt onder instructie en in opdracht van de verwerkingsverantwoordelijke. Een verwerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens etc.[17]

---

15 (artikel 6 lid 4 AVG).

16 *De AVG kent ook de figuur van de 'gezamenlijke verwerkingsverantwoordelijken'. In dat geval stellen twee of meer verwerkingsverantwoordelijken doel en middelen van de verwerking vast. In die gevallen waarbij Waterschap Rivierenland is betrokken bij samenwerkingsovereenkomsten (samenwerking in de keten) waarbij er sprake is van meerdere verwerkingsverantwoordelijken, dan dient te worden vastgesteld welke partij welke verantwoordelijkheden op zich neem. (artikel 26 AVG). Hiervoor zal een overeenkomst opgesteld moeten worden. In deze overeenkomst moeten onder andere afspraken worden opgenomen over de vraag waar betrokkenen terecht kunnen voor hun recht op inzage et cetera. Uiteraard moet deze informatie ook aan betrokkenen zelf worden verstrekt.*

17 Het onderscheid tussen de verwerkingsverantwoordelijke en de verwerker is niet altijd makkelijk te maken. Het is dus zaak om daar in een zo vroeg mogelijk stadium advies over in te winnen van de afdeling Juridische Zaken. Vaak is het zo dat een verwerker zelf zijn software kiest. In zo'n geval moet dan ook worden gekeken naar wie het doel van de verwerking bepaalt. Als het waterschap bijvoorbeeld de salarisadministratie uitbesteedt aan een marktpartij, dan is het nog steeds het waterschap dat bepaalt voor welk doel de marktpartij haar software dient te gebruiken: het uitvoeren van de salarisadministratie volgens de instructies en de wensen van het waterschap.

Het is om meerdere redenen van belang om te bepalen wie verwerkingsverantwoordelijke is en wie verwerker. De AVG legt de meeste verantwoordelijkheden bij de verwerkingsverantwoordelijke neer: deze is aanspreekbaar op de verantwoordingsplicht, is aanspreekpunt voor wat betreft de rechten van betrokkenen, is aanspreekbaar op (het melden van) datalekken etc. Zodra een verwerker zelf het doel en de middelen van de verwerking gaat vaststellen wordt deze automatisch verwerkingsverantwoordelijke[18]

3.3 Verwerkersovereenkomst

De uitvoering van een verwerking door een verwerker wordt geregeld in een verwerkersovereenkomst, overeenkomstig het bepaalde in artikel 28 AVG. Dat wil zeggen, als een organisatie persoonsgegevens voor waterschap Rivierenland verwerkt, is er een verplichting om naast de bestaande dienstverleningsovereenkomst ook een aparte verwerkersovereenkomst te sluiten. De verwerkersovereenkomst behelst expliciet afspraken met betrekking tot verwerken van persoonsgegevens en ook de procedure rond de meldplicht datalekken.

Het onderscheid is wel van belang: Een verwerkersverantwoordelijke is in beginsel voor alle schade aansprakelijk, ongeacht of die door hem of de verwerker wordt veroorzaakt (Artikel 82 lid 2 AVG). Een verwerker is daarentegen slechts aansprakelijk voor de schade die door een verwerking is veroorzaakt wanneer bij die verwerking niet is voldaan aan de specifieke verplichtingen binnen de AVG die zijn gericht tot verwerkers (bijvoorbeeld het toepassen van een passend beveiligingsniveau), of wanneer de schade is ontstaan doordat de verwerker zich niet aan de instructies van verwerkingsverantwoordelijke houdt (Artikel 82 lid 2 AVG).

Een ieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, heeft het recht om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade. Zowel verwerker als verwerkingsverantwoordelijke kunnen voor het geheel van de schade worden aangesproken (artikel 82 lid 1 AVG). Er bestaat tussen verwerker en verwerkersverantwoordelijke wel een mogelijkheid om de vergoede schade te verhalen op de ander. (artikel 82 lid 5 AVG).

18 Artikel 28 lid 10 AVG