Bijlage 1.
Notitie Privacy en Informatieveiligheid

Privacybeleid

In het privacybeleidsplan worden de volgende onderdelen benoemd en geregeld:

1. Begripsbepaling
2. Hoeveelheid personeelsgegevens
3. Reikwijdte
4. Doelstellingen en het belang van informatiebeveiliging
5. Beheer en inzage van gegevens
6. Doelstellingen van de verwerking
7. Rechtmatige grondslag van de verwerking
8. Soorten van opgenomen persoonsgegevens en de wijze van verkrijging
9. Bewaring van persoonsgegevens
10. Verwijdering van persoonsgegevens
11. Rechtstreekse toegang tot persoonsgegevens
12. Verdere verwerking van persoonsgegevens
13. Beveiliging
14. Informatieplicht
15. Rechten van betrokkene
    - Recht op inzage
    - Recht op correctie
    - Recht van verzet

De meest relevante onderdelen worden hieronder uitgewerkt.

Begripsbepaling

De volgende begrippen zijn relevant:
Persoonsgegevens:
Dit is een cruciaal begrip in de Wbp. Hieronder wordt verstaan: elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon. Een persoon is identificeerbaar indien zijn of haar identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.
Voorbeelden van persoonsgegevens zijn:

- Naam, adres, burgerservicenummer;
- Een video-opname van een persoon;
- Gegevens over iemands telefoon- of computergebruik;
- Het kentekennummer of het brandstofgebruik van een dienstauto;
- Iemands ziekteverzuim en de redenen daarvan;
- Een registratie van gevolgde cursussen en opleidingen.

Verwerking van persoonsgegevens:
Onder ‘verwerking van persoonsgegevens’ wordt begrepen iedere handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Bijna elke handeling met betrekking tot persoonsgegevens moet daarmee worden beschouwd als ‘verwerking’.
In de praktijk betekent dit dat er bij het bepalen of er sprake is van ‘verwerking’ om gaat of al dan niet via een computersysteem feitelijke macht of invloed kan worden uitgeoefend over persoonsgegevens. De Wbp ziet op alle verwerkingen die geheel of gedeeltelijk geautomatiseerd zijn.

De wet is overigens eveneens van toepassing op verwerkingen die niet geautomatiseerd zijn, maar waarbij persoonsgegevens in een analoog bestand worden opgenomen. Concreet voorbeeld zijn de gegevens van onze bestuursleden. Deze worden in fysieke mappen bewaard.

Verantwoordelijke:
Met 'verantwoordelijke' wordt elk natuurlijk persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In ons geval is dit het dagelijks bestuur. Ondanks gemandateerde taken en bevoegdheden wordt het dagelijks bestuur aangemerkt als 'verantwoordelijke' in de zin van de Wbp.

Ontvanger:
Ontvanger is diegene aan wie de persoonsgegevens worden gegeven of meegedeeld. Dit begrip is met name van belang voor de informatieverplichtingen van de verantwoordelijke.
Concreet voorbeeld; het waterschap dat persoonsgegevens van eigenaren van woonschepen ter beschikking stelt aan de baggeraar van de stadswateren omdat deze anders zijn taak niet kan uitvoeren. In deze situatie moet het waterschap voorafgaande aan het ter beschikking stellen van de gegevens aan de baggeraar de eigenaren van de woonschepen hiervan op de hoogte stellen.

Bewerker:
De bewerker is een derde die voor de verantwoordelijke persoonsgegevens verwerkt. De bewerker is daarbij niet rechtstreeks aan het gezag van de verantwoordelijke onderworpen maar verwerkt gegevens ten behoeve van de verantwoordelijke. Concreet voorbeeld in een situatie dat het waterschap bij de verwerking van de salarissen of bij het samenstellen van het kiezersbestand bewerkers inschakelt.

Doeleinden
De verwerking van gegevens moet zijn gebaseerd op uitdrukkelijk omschreven en gerechtvaardigde doeleinden, te weten:
- Het doel waarvoor de gegevens worden verzameld, moet duidelijk vastgesteld zijn;
- Het doel moet zijn omschreven. Voordat begonnen wordt met de verwerking van gegevens;
- Wanneer met minder gegevens hetzelfde doel kan worden bereikt, is het verzamelen van extra gegevens niet gerechtvaardigd.

Voorwaarden voor verzamelen
Persoonsgegevens mogen overeenkomstig de Wbp enkel worden verwerkt als aan één van de genoemde voorwaarden wordt voldaan.
- De betrokkende heeft voor de verwerking toestemming verleend;
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- De verwerking is noodzakelijk om een wettelijke verplichting na te komen;
- De verwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkenen;
- De verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak;
- De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang.

Bewaartermijnen
Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor het uitvoeren van de doeleinden waarvoor zij worden verzameld of worden verwerkt. In de Wbp staan zelf geen concrete termijnen. Rekening moet worden gehouden met meerdere soorten wetgeving.

Het Vrijstellingsbesluit noemt bijvoorbeeld voor personeelsadministraties een bewaartermijn van maximaal twee jaar nadat het dienstverband is beëindigd. Voor sollicitantenregistraties wordt een termijn genoemd van uiterlijk vier weken nadat de sollicitatieprocedure is beëindigd.

Geheimhoudingsplicht
De Wbp bepaalt dat een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf slechts gegevens verwerkt in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.
Deze personen zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen. Voor onze medewerkers geldt dat zij uit hoofde van hun ambt onder de geheimhoudingsplicht vallen (eed en belofte) en op basis van wettelijke voorschriften (Gedragscode Hunze en Aa's 2014).

Meldplicht
De Wbp bepaalt in algemene zin dat iedere verwerking van gegevens gemeld moet worden bij de Authoriteit Persoonsgegevens (AP, was voorheen het College Bescherming persoonsgegevens). Op deze meldplicht is een aantal uitzonderingen gemaakt, neergelegd in het Vrijstellingsbesluit. Voor ons geldt dat dat applicaties (systemen), met uitzondering van het verwerken van persoonsgegevens die het vakbondslidmaatschap of de aard van ziekte van werknemers behelzen, onder de vrijstelling vallen. De persoonsverwerkingen die met de waterschapsverkiezingen te maken hebben vallen ook niet onder het Vrijstellingenbesluit. Dit betekent uiteraard dat de genoemde applicaties nog wel onder de reikwijdte van de wet vallen.
De melding kan ook worden verricht aan de functionaris gegevensbescherming.

Informatieplicht
De verantwoordelijke heeft de plicht om betrokkenen wiens gegevens worden verwerkt tijdig en adequaat te informeren. Deze plicht houdt in dat de verantwoordelijke aan de betrokkene zijn identiteit moet aangeven en moet aangeven voor welk doel of welke doeleinden de gegevens verzameld en verwerkt worden

Rechten van betrokkene
De wet biedt de betrokkenen mogelijkheden om zijn persoonsgegevens in te zien of te laten wijzigen. Het gaat hierbij om:
- Recht op inzage:
  Een betrokkene mag met redelijke tussenpozen vragen of en zo ja, welke persoonsgegevens van hem verwerkt worden;
- Recht op correctie
  Als de gegevens feitelijk onjuist, onvolledig, niet er zake dienend of in strijd met een wettelijk voorschrift zijn, kan een betrokkene vragen om correctie ervan. Correctie houdt hier in: verbeteren, aanvullen, verwijderen, afschermen of op een andere manier zorgen dat de gegevens niet meer worden gebruikt.
- Recht van verzet
  Wanneer een bestuursorgaan gegevens verwerkt die noodzakelijk zijn voor de vervulling van zijn publiekrechtelijke taak of indien gegevens worden verwerkt voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke, kan de betrokkene hiertegen in verzet komen gelet op de voor hem geldende bijzondere persoonlijke omstandigheden.

Vergoeding kosten
De verantwoordelijke kan een vergoeding vragen voor de kosten die hij maakt bij het verstrekken van informatie de hoogte hiervan is vastgesteld bij AmvB.
Op dit moment staan wij dit niet voor.

Rechtsbescherming
Een aantal beslissingen dat wordt genomen in het kader van de Wbp worden aangemerkt als besluit in de zin van de Awb en zijn derhalve vatbaar voor bezwaar en beroep. Bijvoorbeeld een beslissing van een bestuursorgaan naar aanleiding van een op de wet gebaseerd verzoek van de betrokkene inzake een verzoek om inzage, correctie of verwijdering van gegevens.

Toezicht
Het toezicht op de naleving van de Wet is opgedragen aan de AP. Zij heeft de bevoegdheid, ambtshalve of op verzoek van een belanghebbende, om een onderzoek in te stellen naar de wijze waarop de wet wordt nageleefd. De beveiliging van persoonsgegevens is hierbij een essentieel aandachtspunt

Bestuursrechtelijke sanctiemiddelen
Het CBP kan, in geval van overtreding van het in de Wbp bepaalde, bestuursdwang toepassen of een last onder dwangsom opleggen. Ook heeft de AP per 1 januari 2016 uitgebreidere bevoegdheden gekregen om een bestuursrechtelijke boete op te leggen. Met de meldplicht datalekken (zie verder bij informatiebeveiliging) en de uitbreiding van de bestuurlijke boetebevoegdheid kan de AP een boete opleggen per wettelijk boetemaximum van € 810.000, € 450.000,- of € 20.250,-- ingedeeld in een aantal boete categorieën, en daaraan verbonden in zwaarte oplopende boetes. Een en ander is geregeld in 'Beleidsregels van het College bescherming persoonsgegevens' met betrekking tot het opleggen van bestuurlijke boetes (Beleidsregels Autoriteit Persoonsgegevens 2015). Tegen het opleggen van een bestuurlijke boete staat bezwaar en beroep open. De werking van de beschikking tot oplegging van een bestuurlijke boete wordt opgeschort totdat de bezwaar –en beroepstermijn is verstreken of, indien bezwaar is aangetekend respectievelijk beroep is ingesteld, op het bezwaar respectievelijk het beroep is beslist.

Intermezzo

Zoals in de inleiding reeds is aangegeven treedt in 2016, met een invoeringsperiode van twee jaar, in 2018 de Europese Verordening gegevensbescherming in werking. De algemene verordening heeft rechtstreekse werking. In alle lidstaten is de verordening dus direct bindend. Bij de inwerkingtreding hiervan komt de Wbp te vervallen. Wachten op de invoering ervan om intern beleid vast te stellen is niet wenselijk en ook niet nodig. Niet wenselijk vanwege de directe koppeling van privacy c.q de bescherming van persoonsgegevens en informatieveiligheid. Aspecten rondom veiligheid moeten op basis van wettelijke termijnen wel geregeld worden.
Wachten is ook niet nodig omdat de wijzigingen die de Verordening met zich mee brengt geen principiële wijzigen betreffen. Het gaat met name om een aanscherping van verplichtingen van de verantwoordelijke en meer rechten van betrokkenen. De aanscherpingen zien met name op veiligheidsaspecten van persoonlijke gegevens.
De belangrijkste elementen worden hieronder uiteengezet. Geëindigd wordt met het beveiligingsdeel zodat dit onderdeel samen met de verplichtingen die uit de Wbp voortvloeien en de inwerkingtreding van de Wet datalekken samenkomt.

Versterken rechten betrokken
Betrokkenen hebben het recht om hun persoonsgeven te laten verwijderen indien:
- Er niet langer een noodzaak is om de gegevens te bewaren gelet op het doel waarvoor de gegevens verzameld zijn;
- De natuurlijke persoon zijn toestemming intrekt om de persoonsgegevens te bewaren

- De natuurlijke persoon bezwaar maakt tegen het gebruiken van zijn persoonsgegevens
  Dit geheel valt te vatten onder de inmiddels bekend geworden 'recht om vergeten te worden'

Versteviging bevoegdheden privacy autoriteit
Een nog aan te wijzen toezichthoudende autoriteit (waarschijnlijk de AP) wordt belast met de handhaving van de nieuwe regelgeving. Hiertoe krijgt deze autoriteit een aantal nieuwe bevoegdheden variërend van de bevoegdheid tot berisping van de verantwoordelijke tot de bevoegdheid om een algeheel verbod tot verwerking op te leggen.

Per 1 januari 2016 zijn de Boetebeleidsregels Autoriteit Persoonsgegevens 2015 in werking getreden. Voor de bepaling van het boetebedrag bij overtreding van de Wbp wordt gebruik gemaakt van de in het strafrecht geldende categorieën. Deze zijn onderverdeeld in categorie I (tot € 405,-), categorie II (tot € 4.050,-), categorie III (tot 8.100,-), categorie IV (tot € 20.250,-), categorie V (tot € 81.000,-) en categorie VI (tot € 810.000,-) zoals gesteld in artikel 23, vierde lid Wetboek van Strafrecht.
Bij de veroordeling van een rechtspersoon kan, indien de voor het feit bepaalde boetecategorie geen passende bestraffing toelaat, een geldboete worden opgelegd of ten hoogste het bedrag van de naast hogere categorie. Indien voor het feit een geldboete van de zesde categorie kan worden opgelegd en die boetecategorie geen passende bestraffing toelaat, kan een geldboete worden opgelegd tot ten hoogste 10 procent van de jaaromzet (Overeenkomstig de Verordening kan 5% van de wereldwijde jaaromzet met een maximum van € 100 miljoen worden opgelegd). Boetes worden opgelegd voor onder meer
- Niet tijdig of niet volledig informeren van natuurlijke personen;
- Niet melden of niet volledig melden van datalekken;
- Het niet voldoen aan een verzoek tot verwijdering of niet voorzien van de door een natuurlijk persoon opgevraagde informatie.

Versterking verantwoordelijkheden organisatie die persoonsgegevens verzamelen en gebruiken
Het wordt verplicht om het beleid rond de verwerking van persoonsgegevens transparant en eenvoudig toegankelijk te maken voor de personen waarvan de gegevens worden verwerkt.
Ook zal dit beleid controleerbaar moeten zijn voor de privacy-autoriteit in casu de AP. Uit de 'privacy' policy zal onder meer moeten blijken welke persoonsgegevens worden verwerkt en waarom alsmede welke maatregelen zijn genomen om aan de wetgeving te voldoen. Dit geldt ten aanzien van:

- Meldplicht datalekken (zie in bijlage 2 bij beveiliging);
- Verplichte Functionaris Gegevensbescherming voor de publieke sector.

De Wbp biedt de mogelijkheid om een interne toezichthouder aan te stellen. Het hebben van een dergelijke functionaris is nu niet verplicht maar wordt dat wel met de inwerkingtreding van de Europese Privacy verordening. Deze Functionaris voor de gegevensbescherming (FG) houdt binnen de organisatie toezicht op de toepassing en naleving van de Wbp.
De taken van een FG zijn onder meer:
- Toezicht houden;
- Inventarisatie van gegevensverwerkingen maken;
- Meldingen van gegevensverwerking bijhouden;
- Vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
- Interne regelingen ontwikkelen;

Nu nog moet een organisatie die gegevens verwerkt dit melden bij de AP. Als er een FG is aangesteld dan kunnen de verwerkingen bij de FG worden gemeld in plaats van bij de AP.

De wet stelt een aantal eisen aan FG's. Het moet een natuurlijk persoon zijn. Een FG moet voldoende kennis hebben van de organisatie en de privacywetgeving. De FG moet betrouwbaar zijn, wat zich onder meer uit in een geheimhoudingsplicht.
De FG heeft geen formele sanctiemogelijkheden. Maar de organisatie is wel wettelijk verplicht om de FG controlebevoegdheden te geven. Zo moet een FG bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen. De FG moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen de organisatie.
Het dagelijks bestuur heeft de bestuurskundige voorgedragen als FG bij de AP. De AP heeft hiervan bij brief van 12 oktober 2015 met instemming kennis van genomen.

Privacy en Beveiliging persoonsgegevens.
Een belangrijk aspect van privacybeleid is de beveiliging van persoonsgegevens. De beveiliging van persoonsgegevens is één van de onderdelen van informatiebeveiliging.

Bescherming persoonsgegevens als onderdeel van informatiebeveiliging

Hiervoor is ingegaan op informatiebeveiliging als 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. Artikel 13 van de Wbp bepaalt dat de verantwoordelijke de verplichting heeft om passende technische en organisatorische maatregelen ten uitvoer te brengen 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.

Een Privacy Impact Analye (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 in tien stappen worden bepaald in een hoeverre en organisatie risico's loopt op informatiebeveiligingsincidenten met persoonsgegevens.

De volgende elementen zijn hierbij relevant (een aantal zijn hierboven, onder privacybeleid uitgewerkt) Voor onderstaande onderdelen geldt dat deze na vaststelling van het veiligheidsplan en het privacybeleid nog nader moeten worden uitgewerkt (opgenomen in een activiteitenplan)

Dataminimalisatie
Een organisatie mag niet meer privacygevoelige data hebben dan nodig is voor de uitvoering van de taak.

Toegangsbeveiliging
In de Wbp zijn eisen opgenomen met betrekking tot de toegang tot informatiesystemen –en diensten. Er mag enkel toegang worden verleend die nodig is voor de uitoefening van de taak en om onbevoegde toegang tot deze informatiestromen te voorkomen. Deze eisen omvatten alle fases: van de instroom van medewerkers tot het moment dat deze de organisatie verlaten.

Data-integriteit
De informatie die een organisatie heeft, moet vanzelfsprekend voldoen aan de eisen ten aanzien van juistheid en volledigheid.

Data-vernietiging
In de Wbp is aangegeven dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk.

Melden datalekken
Indien een organisatie (per ongeluk) informatie lekt, moet dit direct, doch binnen twee werkdagen, zo volledig mogelijk worden gemeld bij de AP. Indien dit niet gebeurt dan riskeert de organisatie een boete.

Rechten van betrokkenen
Organisaties en bedrijven moeten bij betrokkenen expliciete toestemming vragen voor het vastleggen van zijn of haar gegevens en uitleggen waarom de gegevens worden vastgelegd.

Bewerkersovereenkomsten
Als een organisatie zijn gegevens laat opslaan door een derde en eventueel laat bewerken dan dient er een bewerkersovereenkomst te zijn overeen gekomen. De systemen met persoonsgegevens worden veel gehost door externe partijen. Op dit moment zijn er geen afspraken gemaakt ten aanzien van het omgaan met persoonsgegevens. Hieraan wordt in 2016 vorm gegeven.

Aanstellen Functionaris Gegevensbescherming
Hiervoor is hier reeds uitgebreid op ingegaan. De FG is inmiddels aangewezen. De invulling van de functie wordt, als onderdeel van het activiteitenplan in 2016 vormgegeven.

Uitwerking privacybeleid

Het privacybeleid is hiervoor uitgewerkt. De belangrijkste elementen zijn uiteen gezet en vormgegeven in een privacyreglement (bijlage 3). Ook zijn de elementen van het veiligheidsplan (informatiebeveiliging en bescherming persoonsgegevens) uitgewerkt en vormgegeven.
Een aantal onderdelen moeten in de loop van de tijd nog vorm krijgen danwel hebben continue aandacht nodig (zijn opgenomen in een activiteitenplan).

Om uitwerking te kunnen geven aan het privacy beleid en de bescherming van gegevens zijn er voor de privacyimpact analyse richtlijnen opgenomen.
Het doorlopen van deze stappen geeft een totaal beeld van de huidige ‘privacystaat’ en de onderdelen die nog nadere uitwerking behoeven. Deze staan beschreven in de Privacy Impact Analyse waar later in deze notitie nader op wordt ingegaan.

Huidige situatie en te ondernemen stappen

Zoals gezegd wordt de huidige situatie bepaald op grond van de tien stappen uit de Privacy Impact Analyse. Per onderdeel wordt aangeven wat de huidige situatie is en welke stappen binnen welke termijn worden genomen om privacyproof te zijn.

1. Bepalen van de verantwoordelijke voor de verwerking van persoonsgegevens

In alle situaties is het dagelijks bestuur verantwoordelijk voor de verwerking van persoonsgegevens. De secretaris-directeur is verantwoordelijk voor de implementatie, toepassing en handhaving van informatiebeveiligingsbeleid. De vraag is of wij voldoende voorbereid en geëquipeerd zijn voor wat betreft de nodige voorzieningen en maatregelen waaronder middelen, beheer, taakverdeling, procedures en intern toezicht. Wij hebben het BRK (Basisregistratie kadaster) en het Handelsregister nu nog op onze eigen schijven opgeslagen. We willen ook een BRP (Basis Registratie Personen) koppeling invoeren voor het programma Waterpro waar de handhavers mee werken. Daar is het beveiligingsbeleid thans niet op ingericht.
Uit de uitgevoerde analyse blijkt dat de kennis en vaardigheden voldoende zijn. Op het gebied van taakverdeling, procedures en intern toezicht is echter nog te weinig omschreven.

2. Transparantie: het doel van het verwerken van persoonsgegevens

In stap 2 wordt aangegeven wat het doel is van het bewaren van persoonsgegevens. Er zijn wettelijke verplichtingen om bepaalde persoonsgegevens op te slaan, bijvoorbeeld ingevolge de Wet op de Loonbelasting en de Archiefwet. Ten aanzien van andere persoonsgegevens moeten vooraf de doelen worden bepaald die verwerken rechtvaardigen. Hierbij is van belang dat het doel van de verwerking zo nauwkeurig en volledig mogelijk wordt omschreven. Als er meerdere doelstellingen zijn, moeten deze afzonderlijk worden genoemd en getoetst op de noodzaak om met het oog hierop persoonsgegevens te verzamelen.
De specifieke doelen waarvoor wij persoonsgegevens verwerken zijn niet altijd bekend en niet in (detail) vastgelegd. Soms worden gegevens dubbel bewaard zonder dat hieraan een gerechtvaardigd doel ten grondslag ligt. Voor een aantal systemen geldt dat deze via een schaduwdossiers analoog onbeveiligd worden opgeslagen.
De andere systemen worden op interne harde schijven van het waterschap opgeslagen, gesynchroniseerd en verwerkt. Met andere woorden: de doelen waarvoor wij bepaalde gegevens opslaan zijn niet vastgelegd anders dan in de Wet op de Loonbelasting en de Archiefwet is bepaald en vanwege de publieke taak die wij hebben.

3. Rechtmatige grondslag omschrijven; welke data zijn nodig om dat doel te bereiken.

In deze stap wordt bekeken welke informatie wij moeten verzamelen om het doel zoals in stap 2 is bepaald te kunnen bewerkstelligen.
Ondanks het feit dat dat doelen niet danwel niet nauwkeurig genoeg beschreven zijn voor het verwerken van persoonsgegevens, met uitzondering van wettelijke verplichtingen, kan worden gesteld dat elk van de type persoonsgegevens direct van belang is voor de organisatie en de taken die daarbij horen.
Ten aanzien van inkoop moet bijvoorbeeld nog in beleid worden opgenomen hoe de informatiebeveiliging en privacy in het voortraject wordt getoetst door middel van een programma van eisen. De inkoopvoorwaarden worden aangevuld per aanbesteding met een alinea over informatiebeveiliging en privacy, zodat producten en diensten beter worden geselecteerd in het kader van de wetgeving en de gegevensbeveiliging ervan. Tevens wordt het hierdoor voor externe betrokkenen duidelijk welke eisen wij stellen met betrekking tot deze onderwerpen Om een rechtmatige grondslag te kunnen bepalen zouden alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen in kaart moeten worden gebracht zodanig dat hierdoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt.

4. Kwaliteit: in kaart brengen welke data wanneer nodig is.

In stap 4 wordt bezien of er niet meer gegevens worden verzameld dan nodig is om het doel te bereiken. De persoonsgegeven die door het waterschap worden verzameld betreffen veelal die van (toekomstige) medewerkers of (oud) bestuursleden. Dit is wettelijk geregeld. Daarnaast worden persoonsgegevens verwerkt voor het uitvoeren van onze publiekrechtelijke taak. Op onze website is een 'privacystatement' en cookiebeleid alsmede een disclaimer opgenomen. Daarin is opgenomen wanneer de persoonsgegevens van onze ingelanden wel of niet worden opgeslagen, anders dan zolang nodig is om de identiteit van de aanvragen van een product vast te stellen. Daarna worden de persoonsgegeven vernietigd.
In de memovelden en omschrijvingsvelden bij de schouwsloten worden persoonsgegevens opgenomen die noodzakelijk zijn voor de uitoefening van de taak. Dit wordt momenteel beoordeeld op legitimiteit en herzien waar nodig.

Beveiligingstechnisch gezien worden in enkele applicaties/systemen logbestanden bijgehouden. Zo kan tot op de medewerker nauwkeurig worden nagegaan welke documenten worden geprint en door wie er welke websites worden bezocht. De wijze waarop hiermee wordt omgegaan is beschreven in het Protocol E-mail en internetgebruik en Social Media.

5. De expliciete toestemming van de eigenaar van de persoonsgegevens analyseren/opvragen

Om persoonsgegevens te mogen verwerken moet iedere natuurlijke persoon of instelling (betrokkene) expliciet toestemming hebben gegeven, voordat gestart wordt met de verzameling en het beheer van persoonsgegevens. Voor het gebruik van gegevens uit de basisregistratie Personen (BRP, voorgeen GBA) bestaan in de BRP vrijstellingen. De gegevens worden opgevraagd via de landelijke database (GBA-V (Gemeentelijke BasisAdministratie persoonsgegevens Verstrekkingsvoorziening). In deze stap worden bekeken in hoeverre toestemming moet worden gegeven aan ons voor de verwerking en welke wet- en regelgeving hierop van toepassing is.
In de disclaimer op onze website is aangegeven welke gegevens wel en niet worden verzameld. Dit dekt niet de volledige lading. Daarnaast komen gegevens vanuit de BRP binnen via andere overheidsinstanties. Deze mogen wij vanwege de uitoefening van onze publieke taak verwerken. Burgers kunnen kennis nemen van de over hun verzamelde gegevens door een verzoek om inzage in te dienen. Er zijn thans geen procedures opgenomen inzake het verbeteren, aanvullen, verwijderen of afschermen van deze gegevens. Bij de gemeente kan een verzoek worden ingediend om inzake etc. wanneer het om BRP gegevens gaat.

6. Gegevenstransport: in kaart brengen van datastromen naar leveranciers/derden

De resultaten van de eerste vijf stappen kunnen worden gebruikt om privacystatements te formuleren. Inzichtelijk moet worden gemaakt hoe de datastromen van persoonsgegevens naar leveranciers en externen zijn.
We werken met diverse programma's en databases waarin persoonsgegevens worden verwerkt/opgeslagen. Geïnventariseerd is welke verwerkingen van persoonsgegevens worden uitgevoerd door te bekijken welke applicaties/programma's er zijn en welke verwerkingen er worden toegepast.

7. Doelbinding: Onderzoeken en in kaart brengen of data ook alleen voor het specifieke en gerechtvaardigde doel wordt gebruikt.

Wanneer persoonsgegevens voor een bepaald doel worden verzameld, is het niet toegestaan om deze gegevens te gebruiken voor een ander doel. In deze stap wordt bezien of alle verzamelde gegevens voor het gerechtvaardigde doel worden gebruikt. Het doel van de informatieverzameling bij de verschillende onderdelen is niet vastgelegd behalve in JOIN (postregistratiesysteem) indien het gaat om inkomende mails en poststukken. Voor het overige geldt dat deze niet formeel zijn vastgesteld.

8. In kaart brengen hoe de beveiliging van deze gegevens is geregeld (welk soort gegevens zijn hoe beveiligd)

Persoonsgegevens die worden verwerkt en/of beheerd dienen voldoende beveiligd te worden. In deze stap wordt bekeken hoe persoonsgegevens zijn beveiligd en of dat voldoend eis.
Er zijn geen periodieke controles die beleid toetsen aan de wet op juistheid, nauwkeurigheid en actualiteit. De kans dat gegevens terecht komen bij onbevoegden is altijd aanwezig. De meest gevoelige gegevens zijn opgeslagen in PIMS (personeelsinformatiemanagementsysteem), Verzuimsignaal, TIM Enterprise (Tijdregistratie), Topdesk (incidentenregistatie-tool), ACS/2Bsure (pasjessysteem), Waterpro (Kadaster, Handelsregister), JOIN (postsysteem) en WHAAS (systeem loopbaanontwikkeling medewerkers). Daarnaast kan door externe beheerders worden ingelogd voor technische doeleinden. Zij hebben de mogelijkheid om de persoonsgegevens in de desbetreffende systemen in te zien. Hierop is geen controle anders dan het meekijken van een medewerker tijdens het uitvoeren van de bewerkingen.
Gevoelige persoonsgegevens worden niet extra beveiligd anders dan dat rechten zijn toegekend aan specifieke medewerkers die mogen werken met bepaalde gegevens.

9. In kaart brengen hoe (persoons)gegevens worden gearchiveerd (welke worden wel/niet bewaard en hoe)

Indien een activiteit afgerond is, moeten persoonsgegevens gearchiveerd worden op een veilige en beheersbare manier. Gearchiveerde data mogen niet opnieuw worden gebruikt zonder toestemming van de betrokkene. In deze stap wordt bekeken in hoeverre er veilig en beheersbaar wordt gearchiveerd en of data enkel met toestemming van de betrokkende uit archieven wordt gehaald.
In het Vrijstellingsbesluit Wbp is opgenomen hoe lang de verschillende persoonsgegevens bewaard mogen worden, Niet alle persoonsgegeven mogen even lang bewaard worden Dit verschilt van zes maanden tot twee jaar. De termijn van bewaring wordt conform de Archiefwet uitgevoerd via een vast protocol. Financiële stukken moeten volgens de Archiefwet bijvoorbeeld zeven jaar worden bewaard. De digitale en analoge vernietiging gebeurd nog niet overal juist en volledig. Zo worden persoonsgegevens niet altijd volledig vernietigd. Het is soms mogelijk om via back-up tapes de voor vernietiging vatbare gegevens terug te zetten. Laatstgenoemde gegeven maken echter onderdeel uit van een bulk aan gegevens die niet te splitsen zijn. Derhalve zijn de persoonsgegevens hier niet uit te filteren. Deze back-up tapes zijn echter voldoende beveiligd.

10. Persoonsgegevens die worden opgeslagen en gearchiveerd zijn analyseren en laten bepalen welke wel/niet verwijderd kunnen worden

Wanneer een activiteit of een dienstcontract is afgelopen dienen persoonsgegevens die niet meer nodig zijn te worden verwijderd. In geval van gegevens uit de BRP gelden andere voorwaarden. In stap 10 wordt bekeken of overbodige gegevens ook definitief verwijderd en vernietigd worden.

De uitkomsten van de Privacy Impact Analyse worden geleidelijk ingebed in de organisatie. De stappen die moeten worden genomen zijn veelal onderdeel van een groter proces, ook in relatie tot het thema informatiebeveiliging. De verwachting is dat de (volledige) inbedding van deze uitkomsten gelijk vallen met de afronding van het informatie beveiligingsplan in 2016.

Personeelvolgssytemen

In alle sectoren van de samenleving en binnen de meeste organisaties zijn personeelvolgsystemen meer gemeengoed dan uitzondering geworden. Deze systemen worden gebruikt of zijn in elk geval geschikt voor toezicht op aanwezigheid, gedrag en prestaties van werknemers. Op zich is dit geen probleem. Op het moment echter dat beelden of gegevens uit die systemen worden gebruikt om het gedrag van medewerkers te controleren dan zal dit op zijn minst als onwenselijk worden beschouwd.

Controle van personeel is niet verboden. Maar werkgevers moeten daarbij wel rekening houden, met de privacy van werknemers. Werkgevers mogen hun werknemers niet zomaar de hele dag volgen. Controle van personeel is toegestaan als dit af en toe gebeurt en de werkgever daarbij voldoet aan de voorwaarden uit de Wbp. Gebeurt de controle in het geheim, dus zonder dat de medewerkers dit weten, dan gelden er extra regels. Binnen ons waterschap beschikken we over meerdere personeelvolgsystemen dan wel systemen die kunnen worden gebruikt danwel geschikt zijn om als personeelvolgsysteem gebruikt te worden. Geen van de systemen die door ons waterschap worden gebruikt wordt als personeel volgsysteem gebruikt maar dienen andere doelen. Hieronder wordt nader ingegaan op de verschillende systemen, werkwijze en doelen ervan. Dit is ook terug te vinden in het Protocol. Hierin is ook opgenomen hoe de systemen worden gebruikt (en dus ook waarvoor niet) en wie toegang hebben tot de systemen (bewerkers). Op dit moment beschikken we over een Protocol e-mail- en internetgebruik en Social media en over een Protocol cameratoezicht. Het is wenselijk om bepalingen inzake personeelvolgsystemen op te nemen in een algemeen protocol personeelvolgsystemen. Dit met name omdat de bepalingen vrijwel identiek zijn. Het Protocol e-mail- en internetgebruik en Social media maakt onderdeel uit van onze integriteitregelingen en blijft als zodanig van kracht. Een concept Protocol personeelvolgsystemen is als bijlage bijgevoegd

Protocol e-mail- en internetgebruik en Social media van het waterschap Hunze en Aa's
Dit protocol is in 2015 herzien. In het protocol zijn bepalingen opgenomen over deugdelijk gebruik van e-mail en internet en de (voorwaarden voor) controle hierop door de werkgever. Ook zijn er sancties opgenomen indien de in het protocol opgenomen bepalingen worden overtreden. Er is voor gekozen om het Protocol e-mail- en internetgebruik aan te vullen met richtlijnen voor onder meer Social Media

Alle gegevens omtrent internetgebruik worden op persoonsniveau geregistreerd. Algemene overzichtsrapportages zijn echter niet tot personen herleidbaar. Op incidentele basis kunnen vanwege zwaarwichtige redenen controles van persoonsgegevens over internetgebruik plaatsvinden. Van zwaarwichtige redenen is in ieder geval spraken indien er een reëel vermoeden bestaat dat in strijd met dit protocol opgenomen regels wordt gehandeld. Een verzoek om een controle als hier bedoeld kan uitsluitend door de secretaris-directeur worden ingediend bij het hoofd PFB. Het verzoek gebeurt

schriftelijk. De Ondernemingsraad wordt hierover door de secretaris-directeur onverwijld in kennis gesteld.

Camerabeveiliging
Op dit moment beschikken wij over een protocol cameratoezicht. Hierin is opgenomen wat het doel is van camerabeveiliging, de locaties van de camera's, wie toegang heeft tot de beelden, en hoe de beveiliging is geregeld, Op dit moment is er nog één camera is bedrijf, namelijk een draaibare camera bij gemaal Rozema. In het waterschapshuis zijn twee camera's actief, namelijk in de patch en in serveruimte va de ICT-afdeling.

GPS-tracking
Het ligt in de planning om in de tractoren en kranen van onze buitendienstmedewerkers een trackingsysteem in te bouwen. Deze zitten op dit moment wel al in de dienst- en lease auto's. Een dergelijk systeem mag worden gebruikt om personeel te controleren onder de voorwaarden die zijn beschreven in de Wbp. De belangrijkste voorwaarde voor het plaatsten van een trackingsysteem is dat de werkgever een legitieme reden (gerechtvaardigd belang) heeft. En dat het plaatsen van een trackingsysteem, zoals een gps-systeem hierbij noodzakelijk is.

Tractoren/kranen
Het volgsysteem zal niet worden gebruikt als personeelsvolgsysteem.
Het doel van een dergelijk systeem is om productie uren, productiemeters en werksoorten digitaal te verwerken. Ook kunnen met een dergelijk systeem andere urensoorten (overleg, verlof) bijgehouden worden. Deze gegevens kunnen eenvoudig overgezet worden naar een planningstool.
Daarnaast is het systeem van belang voor de veiligheid van de medewerkers (de medewerkers in de buitendienst zijn vaak solo op pad).

Dienstauto's
In de dienstauto's zijn locators (een type trackingsysteem) aangebracht. Deze locator heeft enkel als doel om de gemaakte kilometers te registeren ten behoeve van de Belastingdienst. De gegevens worden opgeslagen in de locator applicatie en worden gebruikt ter onderbouwing van het feit dat de gereden kilometers ten behoeve van de uitoefening van de functie zijn gemaakt. Indien dit niet kan worden aangetoond dan wordt het waterschap c.q. de berijder voor bijtelling aangeslagen. De locator is door de Belastingdienst aangemerkt als de te hanteren applicatie.

Smartphones en tablets
Met de smartphones en tablets kan de locatie inzichtelijk worden gemaakt indien ingelogd wordt in een specifiek systeem. Op alle smartphones die door het waterschap worden uitgegeven wordt MobileIRON geïnstalleerd. Daarnaast moeten medewerkers MobileIRON op hun privé apparaat installeren als zij de zakelijke mail en/of agenda in willen zien. Via een beheertool op de website van MobileIRON kunnen alle bedrijfsgegevens van de apparaten worden gewist bij verlies, diefstal of misbruik van bedrijfsgegevens. Tevens kan de exacte locatie van het toestel worden bepaald. Ook wordt locatietoegang door diverse bedrijfsapplicaties gebruikt waarbij locatiegegevens zorgen voor het sneller toegankelijk zijn van de juiste informatie, zoals over een perceel of sloot.

Aan- en afwezigheidsregistratie
Bij het betreden van het waterschapskantoor dient de medewerker zich te melden met een pasje. Deze houdt hij voor een kaartlezer. Dit komt binnen via het ACS-systeem (Access Control System), zodat door de receptie gezien kan worden wie in het gebouw aanwezig is. Tevens wordt een ACS lijst uitgedraaid in geval van een calamiteit ten behoeve van de Bedrijfshulpverlening (BHV).

De zuiveringen in Assen, Veendam en Scheemda beschikken ook over een pasjessysteem vanwege de aanwezigheid van een biogasinstallatie. Ook het laboratorium in Assen beschikt over een pasjessysteem.

Printers
In totaal beschikken wij in het kantoor in Veendam over 14 zogenaamde follow-me printers. Het laboratorium in Assen heeft twee en de werkplaats Veele één. Het doel van deze printers is het realiseren van kostenbesparingen op het uitprinten. De prints komen pas uit de printer wanneer de medewerker ze daadwerkelijk ophaalt. Daarnaast is het mogelijk om de documenten bij een andere printer op te halen (‘follow me’). In onze situatie komen de documenten uit de printer wanneer een code wordt ingevoerd. Het is mogelijk om per gebruiker na te gaan hoeveel er wordt geprint. Op individueel niveau wordt dit pas manifest op moment dat er zwaarwegende redenen zijn om nader onderzoek te doen. De gegevens worden minimaal 1 jaar bewaard zodat van een heel jaar kan worden bezien hoe de printerkosten verlopen. De overzichten kunnen worden ingezien per machine, per kostenplaats, per afdeling of per groep gebruikers.