Waterschap Rivierenland

WATERSCHAPSBLAD

Officiële uitgave van Waterschap Rivierenland.

Nr. 9601
11 december
2015

Privacybeleid waterschap Rivierenland

Het college van dijkgraaf en heemraden van Waterschap Rivierenland;

op voordracht van de directieraad van 7 september 2015;

gelet op het bepaalde in de Wet bescherming persoonsgegevens

B E S L U I T :

Artikel 1. Beleidsregel en bijlagen
1. Vast te stellen het Privacybeleid waterschap Rivierenland, opgenomen als bijlage 1 bij dit besluit.
2. Bij deze beleidsregel behoren de volgende bijlage(n):

a. Het Privacyreglement Waterschap Rivierenland
b. Het standaardformulier verwerking persoonsgegevens

Artikel 2. Inwerkingtreding
Deze beleidsregel treedt in werking met ingang van de eerste dag na bekendmaking in het Waterschapsblad.
Artikel 3. Citeertitel
Deze beleidsregel wordt aangehaald als Privacybeleid waterschap Rivierenland

Aldus vastgesteld in de vergadering van het college van dijkgraaf en heemraden van Waterschap Rivierenland van 22 september 2015 te Tiel.

de secretaris-directeur, ir. Z.C. Vonk
de dijkgraaf, ir. R.W. Bleker

BIJLAGE 1
Privacybeleid

•Samenvatting:
De Wet bescherming persoonsgegevens (Wbp) geeft regels voor het verwerken van persoonsgegevens. Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de Wbp, zoals naam, adres, woonplaats, e-mailadres, handtekening, telefoonnummer, godsdienst, inkomen, gezondheid en geslacht. De Wbp vereist dat al die gegevens behoorlijk en zorgvuldig worden verwerkt.

Beveiligingsvoorzieningen moeten voldoen aan geldende wet- en regelgeving en mogen niet meer inbreuk maken op de privacy dan strikt noodzakelijk is. De basis en daarmee ook het doel voor de verwerking van persoonsgegevens is het beschermen van de veiligheid van de gegevens van natuurlijke personen

Waterschap Rivierenland hecht veel waarde aan privacy en wil zorgvuldig omgaan met persoonsgegevens. Uiteraard worden de nodige beveiligingsmaatregelen genomen om persoonsgegevens te beschermen en hiermee te voldoen aan wettelijke regelgeving, maar tot nu toe ontbrak een eenduidig en samenhangend beleid over het omgaan met persoonsgegevens. In het bijgevoegde privacyreglement worden daarom nadere regels gesteld ter uitvoering van de Wet bescherming persoonsgegevens. Het reglement biedt een kader voor het omgaan met persoonsgegevens. In het bij het reglement behorende standaardformulier worden de afspraken ten aanzien van het gebruik en de beveiliging van persoonsgegevens vastgelegd.

•Hoofdpunten van het beleid:
Met het vaststellen van dit privacy beleid wil het waterschap 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 is getracht de privacy risico's, voor zover deze bekend zijn, in beeld te brengen en te beheersen. In het privacyreglement zijn de kaders voor het omgaan met persoonsgegevens vastgelegd en in de bijgevoegde standaard wordt per proces inzichtelijk welke

persoonsgegevens worden verwerkt, met welk doel, de inhoud van de gegevens, bron, beheer, taken en verantwoordelijkheden, veiligheidsmaatregelen, relatiebeheer en verbeterpunten.

•Inleiding
De hoeveelheid data die de overheid vergaart neemt steeds grotere proporties aan. En daarmee ook de roep om privacybeschermende maatregelen. Gegevens zijn een bron van informatie. Informatie is de basis van kennis en macht. Eén van de schaduwzijden van de informatiemaatschappij is de inbreuk op de persoonlijke levenssfeer die het gevolg kan zijn van een ongebreidelde vergaring, bewerking en verspreiding van persoonsgegevens. Het is daarom van belang dat rond de verwerking van persoonsgegevens regels worden gesteld. In artikel 10 van de Grondwet wordt het recht op eerbiediging van de persoonlijke levenssfeer erkend. De Wbp (en de Wet persoonsregistraties die hieraan vooraf ging) vloeit voort uit de opdracht in de Grondwet tot het geven van nadere regels over het omgaan met persoonsgegevens.

Doel van de Wbp is de bescherming van de persoonlijke levenssfeer van een ieder van wie persoonsgegevens worden verwerkt tegen misbruik van die gegevens en tegen een onjuiste verwerking van die gegevens. Daarbij moet worden voorkomen dat gegevens voor een ander doel worden verwerkt dan waarvoor ze worden verzameld en moeten de rechten van betrokkenen worden gewaarborgd.

De Wbp stelt eisen aan de wijze waarop persoonsgegevens door organisaties worden bewaard en verwerkt. Door het opstellen van een privacybeleid en de implementatie daarvan in de organisatie wordt getracht een juiste invulling te geven aan de gestelde verplichtingen in de Wbp.

Kader
• De Wet bescherming persoonsgegevens (Wbp);
• Privacyrichtlijn 95/46/EG;
• EVRM (art. 8);
• Grondwet (artt. 10 en 13)

(Verder is privacywetgeving o.a. vastgelegd in de Telecommunicatiewet, Archiefwet, Wet openbaarheid van bestuur, Algemene wet inzake rijksbelastingen, Wetboek van Strafrecht, Wet basisregistratie personen, Wet geneeskundige behandelingsovereenkomst)

En in de toekomst (mogelijke inwerkingtreding in 2018) de nieuwe Europese privacyrichtlijn waarin onder meer:
• versterking van de rechten van betrokkenen, waaronder het recht op dataportabiliteit;
• versteviging van onafhankelijkheid en bevoegdheden van nationale privacyautoriteiten (voor Nederland het College bescherming persoonsgegevens);
• Boetes;
• invoering van de verplichting voor organisaties om datalekken direct te melden;

Probleem
Het belang van de bescherming van persoonsgegevens wordt binnen de organisatie van het waterschap onderkend, maar tot op heden ontbrak het aan een duidelijk samenhangend beleid ten aanzien van dit onderwerp. Persoonsgegevens worden op diverse plaatsen binnen de organisatie verwerkt en daarbij worden privacybeschermende maatregelen genomen om te voldoen aan de daartoe in de diverse wetten gestelde regels, te denken valt aan de Archiefwet, de Wet bescherming persoonsgegevens, de Algemene wet inzake rijksbelastingen, maar ook aan de NEN Norm zoals vastgelegd in de Baseline Informatiebeveiliging Waterschappen. Met het vaststellen van dit privacybeleid en het daarbij behorende privacyreglement wordt een duidelijk kader gecreëerd voor het omgaan met persoonsgegevens binnen de organisatie.

Doelstelling
Een adequate privacybescherming realiseren in overeenstemming met de hiervoor geldende wettelijke regels en rekening houdend met toekomstige regelgeving op het vlak van de bescherming van de persoonlijke levenssfeer.

Randvoorwaarden:
Na vaststelling van het privacy beleid moet dit worden geïmplementeerd in de organisatie.

De belangrijkste bepalingen uit de Wbp over het rechtmatig omgaan met persoonsgegevens kunnen als volgt worden samengevat:
- persoonsgegevens mogen alleen in overeenstemming met de wet op een behoorlijke en zorgvuldige wijze worden verwerkt.

- persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.
- degene over wie gegevens worden verwerkt moet tenminste op de hoogte zijn van de identiteit van de verantwoordelijke en van het doel van de verwerking waarvoor de gegevens zijn bestemd.
- De gegevensverwerking moet op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

De verantwoordelijkheid voor het nemen van beveiligingsmaatregelen ligt bij de verantwoordelijke (zorgplicht). Dit is bij het waterschap het college van dijkgraaf en heemraden. Hij moet zorgen voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verrijking.

Ten behoeve van de implementatie van het privacybeleid zullen de diverse gegevensverwerkingen binnen de organisatie moeten worden geïnventariseerd en zal per gegevensverweking doel, inhoud, bron, bewaartermijn en veiligheidsmaatregelen moeten worden vastgesteld. 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, zodat wordt voldaan aan wet- en regelgeving.

Oplossing:
· Uitvoeren privacycheck (quickscan): Door de ambtelijke werkgroep privacy is een zogenaamde privacycheck uitgevoerd. Doel van de privacycheck was om inzichtelijk te krijgen hoe door het waterschap persoonsgegevens worden verwerkt en om bewustzijn te creëren over het belang van een zorgvuldige omgang met deze gegevens. Uit de privacy vragenlijst kon worden geconcludeerd dat het waterschap te kort schiet in haar wettelijke verplichtingen en dat het noodzakelijk is om over het onderwerp privacy beleid op te stellen.
· Vaststellen privacyreglement en standaardformulier ten behoeve van gegevensverwerking;
· Inventarisatie gegevensverwerkingen;
· Aanwijzen beheerders: proceseigenaren, systeemeigenaren en gegevenseigenaren.
· Selecteren en implementeren passende maatregelen: De Baseline Informatiebeveiliging Waterschappen (BIWA) bevat maatregelen die algemeen voorkomende informatiebeveiligingsrisico's bij de waterschappen afdekken. De baseline bevat een aantal minimale beveiligingsniveaus waaraan een waterschap zou moeten willen voldoen, maar is nog niet volledig. Voor risico's die niet door de baseline zijn afgedekt stelt het waterschap aanvullende maatregelen vast. De BIWA is gebaseerd op de NEN-norm en bevat waterschap specifieke maatregelen.
· Uitvoeren Privacy impact assessment (PIA): Door het uitvoeren van een PIA worden privacyrisico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld gebracht. Wat is de impact van het beoogde project op de privacy van de betrokkenen? Wat zijn de risico's voor de betrokkenen en voor de organisatie; Is er gegeven de doelstellingen van het project, ook een aanpak mogelijk die minder gevolgen heeft voor de privacy. Deze vragen komen aan de orde tijdens de implementatie bij uitvoering van een PIA. Over de uitkomst van de PIA's bij de verschillende projecten zal de ondernemingsraad worden geïnformeerd. Jaarlijks zal een overzicht worden verstrekt.
· Tijdens de implementatiefase zal een werkinstructie worden opgesteld voor de betreffende medewerkers, waarin de juiste manier van het omgaan met persoonsgegevens wordt beschreven;
· Invoeren meldplicht voor incidenten m.b.t. persoonsgegevens;
· Aanmelden van persoonsgegevensverwerkingen bij het CBP, voor zover de wet dit vereist;
· Controle op de naleving van maatregelen voor privacybescherming.
· T.z.t. aanstellen van een functionaris gegevensbescherming. (de nieuwe Europese richtlijn privacybescherming verplicht tot het aanstellen van een "data protection officer" voor alle overheden en grote organisaties.

Financieel
Met de vaststelling van het privacybeleid als zodanig zijn geen kosten gemoeid. Echter de kosten voor de implementatie van het privacybeleid zijn nog niet te overzien. Als tijdens de implementatie blijkt dat aanvullende privacybeschermende beveiligingsmaatregelen nodig zijn -(afhankelijk van de uitkomst van het privacy impact assessment (PIA))- zullen voor deze additionele kosten separate voorstellen worden ingediend.

Rekening moet worden gehouden met toekomstige nieuwe wetgeving (de Europese privacyverordening). Te zijner tijd moet worden geanticipeerd op de verplichtingen en kosten die hiermee gepaard gaan.

Communicatie
Het privacyreglement zal worden bekendgemaakt in het electronisch Waterschapsblad. Voorafgaand en tijdens de implementatie zal aandacht worden besteed aan de communicatie aan leidinggevenden en medewerkers.

Uitvoering
· Privacy beleid, Privacyreglement en standaardformulier ten behoeve van gegevensverwerking ter instemming voorleggen aan de OR;
· Informeren taakhoudersoverleg Middelen;
· Vaststellen Privacy beleid, Privacyreglement en standaardformulier door het college van dijkgraaf en heemraden;
· Toelichting in Managementoverleg door werkgroep Privacy;
· Aanwijzen en informeren proceseigenaren, systeemeigenaren en gegevenseigenaren;
· Inventarisatie gegevensverwerkingen door de betreffende beheerders/proceseigenaren;
· Selecteren en implementeren passende maatregelen door het team Informatievoorziening;
· Implementatie: Privacy Impact Assessment (PIA): De PIA legt in de eerste plaats de risico's bloot van projecten die te maken hebben met privacy, en dragen bij aan het vermijden of verminderen van deze privacy risico's. Op basis van de antwoorden van de PIA wordt op systematische wijze inzichtelijk gemaakt of er een kans is dat de privacy van de betrokkene wordt geschaad, hoe hoog deze is en op welke gebieden dit speelt. (Bij elk project nagaan of er privacy aspecten zijn; Worden er persoonsgegevens verwerkt?);
· Over de uitkomsten van de PIA's van de diverse projecten zal de OR worden geïnformeerd. Jaarlijks wordt een overzicht verstrekt.
· Voor de betreffende medewerkers wordt een werkinstructie opgesteld, waarin de juiste manier van het omgaan met persoonsgegevens wordt beschreven;
· Centraal beheer gegevensverwerkingen door het team Juridische zaken (te zijner tijd overdragen aan functionaris gegevensbescherming);
· Aanmelden van persoonsgegevensverwerkingen bij het CBP, voor zover de wet dit vereist, via het team Juridische zaken;

Tijdpad
20 april: voorlichting aan betrokken medewerkers in de organisatie
15 juni : Directieraad
18 juni : Informeren OR
23 juli : Voorleggen aan OR
28 augustus: vaststellen CDH
september: instemmen door OR
september: toelichting in Managementoverleg
september 2015: communicatie in organisatie aan leidinggevenden en betrokken medewerkers
najaar 2015 : start implementatie
1 juli 2016 : implementatie gereed

Evaluatie
Controle op de naleving van maatregelen voor privacybescherming.
Evaluatie privacy beleid (jaarlijks) audit uitvoeren
(T.z.t. aanstellen van een functionaris gegevensbescherming)

Conclusie
Geadviseerd wordt om het privacyreglement en het standaardformulier verwerking persoonsgegevens vast te stellen en te besluiten om het beleid te implementeren in de organisatie. De benodigde technische maatregelen treffen om de verwerking van persoonsgegevens adequaat te beschermen.

Bijlagen
1.1 Privacyreglement;
1.2 Standaardformulier gegevensverwerking **(Bijgevoegd als bijlage in de linkerkolom van dit waterschapsblad);**
1.3 Handreiking overzicht privacywetgeving binnen de overheid

Bijlage 1.1
Privacyreglement Waterschap Rivierenland

Het College van dijkgraaf en heemraden van Waterschap Rivierenland;

gelet op:
- het feit dat het wenselijk is een privacyreglement vast te stellen aansluitend bij en in aanvulling op de Wet bescherming persoonsgegevens (Staatsblad 2000, 302);
- het feit dat de hoeveelheid data die de overheid vergaart steeds grotere proporties aanneemt en daarmee ook de roep om privacybeschermende maatregelen;

- de bescherming van gegevens en privacy in overeenstemming met de relevante wet- en regelgeving moet worden bewerkstelligd.

Wettelijke grondslag of bevoegdheid waarop de regeling is gebaseerd
Wet bescherming persoonsgegevens

B E S L U I T:

Vast te stellen: het Privacyreglement Waterschap Rivierenland

Hoofdstuk 1: Begripsbepalingen, reikwijdte en doeleinden

Artikel 1: Begripsbepalingen
In dit Privacyreglement wordt verstaan onder:

- beheerder: degene die onder verantwoordelijkheid van de verantwoordelijke is belast met de dagelijkse zorg voor de verwerking van persoonsgegevens, voor de juistheid van de ingevoegde gegevens, alsmede voor het bewaren, verwijderen en verstrekken van gegevens. Beheerder is de proceseigenaar die verantwoordelijk is voor de privacy aspecten in haar/zijn proces.
- bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
- betrokkene: degene op wie de gegevens betrekking hebben: dit is altijd een natuurlijk persoon, individu (het data subject);
- bewerker: degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. (dus extern) De bewerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. De bewerker 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.
- bijzondere persoonsgegevens: persoonsgegevens als bedoeld in artikel 16 van de wet, zoals afkomst, godsdienst, medische toestand;
- CBP: College bescherming persoonsgegevens als bedoeld in artikel 51 van de wet;
- functionaris gegevensbescherming: de toezichthouder op de rechtmatige verwerking van persoonsgegevens (deze is er nog niet, t.z.t. nog te benoemen: In de Europese privacy verordening wordt dit een verplichting)
- gebruiker: degene die onder verantwoordelijkheid van de beheerder bevoegd is persoonsgegevens in te voeren, te wijzigen en/of te verwijderen of van enigerlei uitvoer van de verwerking kennis te nemen (hier gaat het om de gegevenseigenaar);
- persoonsgegeven: een gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon . Het is een gegeven dat invloed heeft op de manier waarop iemand in het maatschappelijk verkeer wordt beoordeeld of bejegend en dat van invloed kan zijn op hoe over iemand wordt gedacht of geoordeeld;
- reglement: dit reglement inclusief bijlagen;
- verantwoordelijke: college van dijkgraaf en heemraden van Waterschap Rivierenland. De verantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk (functioneel) degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De verantwoordelijke heeft de regierol (regie over het beheer van privacy in de keten);
- verstrekken van persoonsgegevens: het bekendmaken of ter beschikking stellen van persoonsgegevens;
- verwerking van persoonsgegevens: elke handeling, of elk geheel van handelingen met betrekking tot persoonsgegevens o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwisselen of vernietigen van gegevens (enz.). Elke handeling met betrekking tot persoonsgegevens (al dan niet geautomatiseerd);
- waterschap: Waterschap Rivierenland;
- wet: Wet bescherming persoonsgegevens;

Artikel 2: Reikwijdte

1. Dit privacyreglement is van toepassing op alle geheel of gedeeltelijke geautomatiseerde verwerkingen van persoonsgegevens, alsmede op de daaraan ten grondslag liggende documenten die

in een bestand zijn opgenomen. Dit reglement is voorts van toepassing op de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De afzonderlijke verwerkingen dan wel samenhangende verwerkingen zijn in de bijlagen beschreven. Deze bijlagen maken deel uit van dit reglement.

Artikel 3: Doeleinden

Dit reglement heeft tot doel:
1. De persoonlijke levenssfeer van ieder van wie persoonsgegevens worden verwerkt te beschermen tegen misbruik van die gegevens en tegen het verwerken van onjuiste gegevens.
2. Te voorkomen dat persoonsgegevens worden verwerkt voor een andere doel dan het doel waarvoor ze verzameld zijn.
3. De rechten van betrokkenen te waarborgen.

Artikel 4: Doelstellingen van de verwerking

Per afzonderlijke verwerking of samenhangende verwerkingen zijn in de bijlagen de doelen of de samenhangende doelen geformuleerd.
Privacy wordt benaderd vanuit de vraag wat het doel is om gegevens over een persoon te verwerken. (deze doelen worden geformuleerd door de betreffende beheerders op basis van hun vakinhoudelijke kennis).

Artikel 5: Rechtmatige grondslag van de verwerking

1. Het waterschap verwerkt persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de wet.
2. De rechtmatige grondslag voor de verwerking is gelegen in:
a. ondubbelzinnige toestemming van betrokkene;
b. contractuele verplichtingen, voor zover betrokkene partij is bij de uitvoering van een overeenkomst;
c. een wettelijke verplichting van de verantwoordelijke;
d. de goede vervulling van zijn publiekrechtelijke taak;
e. een vitaal belang van de betrokkene;
f. behartiging van een gerechtvaardigd belang van de verantwoordelijke, tenzij het belang of de fundamentele rechten en vrijheden van betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, doorslaggevend zijn (noodzakelijkheidscriterium).

Artikel 6: Verdere verwerking van persoonsgegevens

1. De te verwerken persoonsgegevens worden slechts verder verwerkt op een wijze die niet onverenigbaar is met het doel waarvoor ze zijn verkregen. Daarbij wordt tenminste rekening gehouden met de verwantschap van de doelen, de aard van de gegevens, de gevolgen van de verdere verwerking voor de betrokkene, de wijze waarop de gegevens zijn verkregen en de waarborgen ter bescherming van de persoonlijke levenssfeer.
2. Persoonsgegevens mogen verder worden verwerkt wanneer dat noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is of geschiedt met de ondubbelzinnige toestemming van de betrokkene.

Hoofdstuk 2: Verantwoordelijkheden en beheer

Artikel 7: Verantwoordelijkheden en beheer

1. Door de verantwoordelijke worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
2. Onder verantwoordelijkheid van de verantwoordelijke worden door de beheerder passende technische en organisatorische maatregelen ten uitvoer gelegd om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 8: Beheer van de persoonsgegevens

1. Per afzonderlijke verwerking of samenhangende verwerkingen is in de bijlagen aangegeven wie de beheerder (proceseigenaar) is, wie de gebruiker (gegevenseigenaar) is en – indien van toepassing – wie de bewerker.
2. Per afzonderlijke verwerking of samenhangende verwerkingen is in de bijlagen aangegeven van welke categorieën van personen persoonsgegevens worden verwerkt.

Artikel 9: Soorten en inhoud van de persoonsgegevens

1. Het vastleggen van persoonsgegevens beperkt zich tot die gegevens die noodzakelijk zijn voor de doeleinden van de verwerking als bedoeld in artikel 4.
2. Per afzonderlijke verwerking of samenhangende verwerkingen is in de bijlagen aangegeven welke soorten van persoonsgegevens ten hoogste worden verwerkt en op welke wijze deze gegevens worden verkregen.
3. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf;
4. Persoonsgegevens worden niet verzameld bij derden zonder de uitdrukkelijke toestemming van de betrokkene;
5. Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt;
6. Persoonsgegevens worden slechts verwerkt, voor zover ze, gelet op de in de bijlagen genoemde doeleinden, toereikend, ter zake dienend en niet bovenmatig zijn (proportionaliteit en noodzakelijkheid);
7. Bijzondere persoonsgegevens worden verwerkt met inachtneming van het bepaalde in de artikelen 16 tot en met 23 van de wet;
8. De beheerder (proceseigenaar) treft de nodige voorzieningen ter bevordering van de juistheid en volledigheid van de persoonsgegevens.

Artikel 10: Bewaring persoonsgegevens:

1. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwerkingsdoeleinden zoals deze in de bijlagen is aangegeven;
2. Voor iedere gegevensverwerking zal de bewaartermijn van de gegevens vastgesteld worden. Deze bewaartermijn zal beschreven worden in het voor deze beveiligingsvoorziening geldende beleid.
3. Persoonsgegevens die niet langer voor het doel noodzakelijk zijn, worden zo spoedig mogelijk verwijderd;
4. De vastgestelde bewaartermijnen worden niet in acht genomen indien:
   - een wettelijk voorschrift tot het bewaren van de persoonsgegevens verplicht;
   - de noodzaak tot het bewaren voortvloeit uit taken van verwerkers;
   - er sprake is van strafrechtelijk handelen;
   - de veiligheid van het waterschap, de Staat of natuurlijke personen in het geding is.

5. Verwijdering impliceert vernietiging of een zodanige bewerking dat het niet meer mogelijk is de persoon te identificeren.

Artikel 11: Melden van gegevensverwerkingen

De verwerkingen van persoonsgegevens zullen waar nodig worden gemeld aan het College bescherming persoonsgegevens.

Hoofdstuk 3: Rechtstreekse toegang en verstrekking van persoonsgegevens

Artikel 12: Rechtstreekse toegang tot persoonsgegevens

1. Uitsluitend de beheerder en de door de beheerder aangewezen gebruikers hebben, met het oog op de dagelijkse zorg voor het goed functioneren van de verwerking, rechtstreekse toegang tot persoonsgegevens;
2. De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens, waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Artikel 13: Technische werkzaamheden

Personen die belast zijn met de uitvoering van technische werkzaamheden zijn gehouden tot geheimhouding van alle persoonsgegevens waarvan zij kennis hebben kunnen nemen.

Artikel 14: Verstrekking van persoonsgegevens

1. Per afzonderlijke verwerking of samenhangende verwerkingen is in de bijlagen aangegeven aan welke personen binnen en buiten de organisatie welke persoonsgegevens kunnen worden verstrekt, gelet op het doel en de grondslag van de verwerking.
2. De verantwoordelijke informeert derden, die op vastgestelde wijze bepaalde persoonsgegevens verwerken, over de daaraan gestelde voorwaarden en beperkingen. De verantwoordelijke is aansprakelijk voor schade die de betrokkene lijdt door onrechtmatig gebruik door derden van door de verantwoordelijke rechtmatig aan die derden verstrekte persoonsgegevens.

Artikel 15: Doorgifte van persoonsgegevens naar landen buiten de Europese Unie

De verantwoordelijke geeft geen persoonsgegevens door naar een bedrijf of vestiging in een land buiten de Europese Unie, dat geen passend beschermingsniveau heeft, tenzij voldaan is aan tenminste één van de volgende voorwaarden:

a. met dat bedrijf of die vestiging is een contract gesloten overeenkomstig de door de Europese Commissie vastgestelde modelcontractbepalingen, welk contract voor wat betreft de verwerking van persoonsgegevens de instemming heeft van de ondernemingsraad;
b. de doorgifte is noodzakelijk in het kader van de arbeidsovereenkomst/het aanstellingsbesluit tussen de verantwoordelijke en de betrokkene;
c. de betrokkene heeft een verklaring ondertekend, waarin hij de verantwoordelijke toestemming geeft voor de doorgifte. Die verklaring is in eenvoudige, begrijpelijke taal opgesteld, met specifieke informatie over het betrokken bedrijf of de betrokken vestiging, de door te geven persoonsgegevens, het doel van de doorgifte en de duur van de periode, waarin die verklaring wordt gebruikt.

Hoofdstuk 4: Plichten van verantwoordelijke, beheerder en bewerker

Artikel 16: Beveiliging

1. De verantwoordelijke stelt in het informatiebeveiligingsbeleid richtlijnen op voor de technische en organisatorische beveiliging van de verwerking van persoonsgegevens en legt dit plan ter instemming voor aan de ondernemingsraad.
2. De verantwoordelijke doet het vastgestelde informatiebeveiligingsbeleid toekomen aan de beheerder. De beheerder verwerkt overeenkomstig de richtlijnen van dit beleid.
3. Indien gebruik wordt gemaakt van de diensten van een bewerker, legt de verantwoordelijke de wederzijdse verplichtingen met betrekking tot de omgang met persoonsgegevens schriftelijk in een overeenkomst met die bewerker vast. De bewerker verwerkt overeenkomstig diens overeengekomen verplichtingen.

Artikel 17: Informatieplicht

1. Indien de beheerder persoonsgegevens verkrijgt bij de betrokkene zelf, deelt hij de betrokkene vóór het moment van verkrijging zijn identiteit mee, alsmede het doel van de verwerking waarvoor de gegevens zijn bestemd, tenzij de betrokkene hiervan reeds op de hoogte is.
2. Indien de beheerder persoonsgegevens verkrijgt van een derde of door observatie van de betrokkene, deelt de beheerder de betrokkene op het moment van vastlegging zijn identiteit mee alsmede het doel van de verwerking waarvoor de gegevens zijn bestemd.
3. De beheerder verstrekt de in de leden 1 en 2 bedoelde informatie op een zodanige wijze dat de betrokkene er daadwerkelijk de beschikking over krijgt.
4. De verantwoordelijke verstrekt aan het personeel en aan de ondernemingsraad een overzicht van de doelen waarvoor en de manieren waarop persoonsgegevens van het personeel worden verwerkt, over de regels die daarvoor gelden, over de rechten die betrokkenen ten aanzien daarvan hebben en hoe zij die kunnen uitoefenen.

Hoofdstuk 5: Rechten van de betrokkene

Artikel 18: Algemeen

1. Iedere betrokkene heeft recht op informatie, inzage en correctie (verbetering, aanvulling, verwijdering en/of afscherming) alsmede recht van verzet, zoals geformuleerd in de volgende artikelen van dit hoofdstuk.
2. Het uitoefenen van die rechten kan in werktijd geschieden.
3. Aan het uitoefenen van die rechten zijn voor de betrokkene geen kosten verbonden.
4. Betrokkenen kunnen zich bij het uitoefenen van die rechten laten bijstaan.
5. De beheerder wijst betrokkenen op de mogelijkheden van rechtsbescherming en toezicht en op de rol daarin van het College bescherming persoonsgegevens (t.z.t. en van de functionaris gegevensbescherming).

Artikel 19: Recht op informatie

De verantwoordelijke informeert betrokkene op diens verzoek tijdig en volledig over de doelen waarvoor en de manieren waarop persoonsgegevens van hem worden verwerkt, over de regels die daarvoor gelden, over de rechten die betrokkene ten aanzien daarvan heeft en hoe hij die kan uitoefenen. Daarbij wordt betrokkene ook geïnformeerd over de plaats waar de documenten, waarin bedoelde regels zijn opgenomen, kunnen worden ingezien dan wel opgevraagd.

Artikel 20: Recht op inzage

1. De beheerder deelt een ieder op diens verzoek, zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk mee of hem betreffende persoonsgegevens worden verwerkt.
2. Indien dat het geval is, verstrekt de beheerder de verzoeker desgewenst, zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk een volledig overzicht daarvan met informatie over het doel of de doelen van de gegevensverwerking, de gegevens of categorieën van gegevens waarop de verwerking betrekking heeft, de ontvangers of categorieën van ontvangers van de gegevens alsmede de herkomst van de gegevens. Indien de verzoeker dat wenst, verstrekt de beheerder tevens informatie over de systematiek van de geautomatiseerde gegevensverwerking.
3. De verzoeker heeft recht op een kopie van de gegevens die over hem zijn vastgelegd. Hij hoeft hiervoor niet te betalen.
4. Indien een gewichtig belang van de verzoeker dit eist, voldoet de beheerder aan het verzoek in een andere dan schriftelijke vorm, die aan dat belang is aangepast.
5. De beheerder draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.
6. De beheerder kan weigeren aan een verzoek te voldoen, indien en voor zover dit noodzakelijk is in verband met:
   a. de opsporing en vervolging van strafbare feiten;
   b. gewichtige belangen van anderen dan de verzoeker, de verantwoordelijke daaronder begrepen.

Artikel 21: Recht op correctie: verbetering, aanvulling, verwijdering en/of afscherming

1. Op schriftelijk verzoek van een betrokkene gaat de beheerder over tot verbetering, aanvulling, verwijdering en/of afscherming van de met betrekking tot de verzoeker verwerkte persoonsgegevens, indien en voor zover deze gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig, niet ter zake dienend of bovenmatig zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek behelst de aan te brengen wijzigingen.
2. De beheerder deelt de verzoeker zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk mee of hij daaraan voldoet. Indien hij daaraan niet of niet geheel wil voldoen, omkleedt hij dat met redenen.
3. De beheerder draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering en/of afscherming zo spoedig mogelijk wordt uitgevoerd.
4. De beheerder informeert in geval van verbetering, aanvulling, verwijdering en/of afscherming derden daarover en verzekert zich ervan dat die derden hun bestanden dienovereenkomstig aanpassen. De beheerder deelt de verzoeker mee aan welke derden hij die informatie heeft verstrekt.

Artikel 22: Recht van verzet

1. Indien de rechtmatige grondslag voor een bepaalde verwerking is gelegen in het

2. gerechtvaardigde belang van de verantwoordelijke, kan de betrokkene bij de beheerder te allen tijde bezwaar aantekenen tegen die verwerking in verband met zijn bijzondere persoonlijke omstandigheden.
3. Binnen vier weken na ontvangst van het bezwaar beoordeelt de verantwoordelijke of dit
4. verzet gerechtvaardigd is.
5. De beheerder beëindigt de verwerking terstond, indien de verantwoordelijke het verzet gerechtvaardigd acht. Verzet tegen de verwerking voor commerciële of charitatieve doelen is altijd gerechtvaardigd.

Hoofdstuk 6: Rechtsbescherming en toezicht

Artikel 23: Klachtenprocedure

1. Elke betrokkene heeft het recht bij de verantwoordelijke een klacht in te dienen
   a. tegen een beslissing op een verzoek als bedoeld in de artikelen 19, 20 en 21;
   b. tegen een beslissing naar aanleiding van de aantekening van verzet als bedoeld in artikel 22; alsmede
   c. tegen de wijze waarop de verantwoordelijke, de beheerder of de bewerker de in dit reglement opgenomen regels uitvoert.

2. De verantwoordelijke reageert zo spoedig mogelijk, maar uiterlijk binnen zes weken na ontvangst, schriftelijk en met redenen omkleed op de klacht.
3. Betrokkene kan zich bij de indiening en behandeling van zijn klacht laten bijstaan.
4. De verantwoordelijke kan tot het oordeel komen dat de klacht onterecht is, dan wel geheel
5. of gedeeltelijk terecht.
6. Indien de verantwoordelijke de klacht niet of slechts gedeeltelijk honoreert, kan de betrokkene een klacht indienen bij het Cbp. De verantwoordelijke informeert de betrokkene, wiens klacht hij niet of slechts gedeeltelijk honoreert, over die mogelijkheid en over het adres van het College.
7. Indien de verantwoordelijke oordeelt dat de klacht geheel of gedeeltelijk terecht is, beslist hij om
   a. (indien de klacht zich richt tegen een beslissing als bedoeld in lid 1 onder a.): het verzoek van betrokkene alsnog geheel of gedeeltelijk te honoreren;
   b. (indien de klacht zich richt tegen een beslissing als bedoeld in lid 1 onder b.): het verzet van betrokkene alsnog te honoreren;
   c. (indien de klacht zich richt tegen de wijze van uitvoering als bedoeld in lid 1 onder c.): alsnog uitvoering te geven aan de in het reglement opgenomen regels, hetgeen kan inhouden een handelen of een nalaten, waaronder begrepen een herstellen of een stoppen;
   d. de schade die betrokkene heeft geleden, waaronder eventuele immateriële schade, te vergoeden.

8. De verantwoordelijke maakt zijn oordeel schriftelijk aan betrokkene kenbaar.
9. Indien de verantwoordelijke niet binnen zes weken na het indienen van de klacht reageert, kan betrokkene een klacht indienen bij het Cbp.

Artikel 24: Toezicht op de naleving

Het College bescherming persoonsgegevens is op grond van de wet bevoegd toe te zien op de naleving van de in dit reglement opgenomen bepalingen.

Artikel 25: Scholing

De verantwoordelijke draagt zorg voor een regelmatige scholing van de beheerders en de gebruikers om te verzekeren dat ze de processen van persoonsgegevensverwerking, de daarvoor geldende regels en hun eigen rol daarin begrijpen.

Hoofdstuk 7: Slotbepalingen

Artikel 26: Onvoorzien

In gevallen waarin het reglement niet voorziet beslist de verantwoordelijke, zo mogelijk na instemming van de ondernemingsraad. In spoedeisende gevallen informeert de verantwoordelijke de ondernemingsraad achteraf.

Artikel 27: Publicatie

Het privacyreglement zal in het elektronisch Waterschapblad en op intranet worden gepubliceerd.

Artikel 28: Wijzigingen en aanvullingen

1. Wijzigingen in doel van de verwerking en in soort van inhoud, gebruik en wijze van verkrijging van de persoonsgegevens dienen te leiden tot wijziging van dit reglement.
2. Wijzigingen en aanvullingen van het reglement behoeven de instemming van de ondernemingsraad.

Artikel 29: Inwerkingtreding en citeertitel

1. Dit reglement treedt in werking met ingang van de eerste dag na bekendmaking
2. Dit reglement wordt aangehaald als Privacyreglement Waterschap Rivierenland.

Aldus vastgesteld in de vergadering van het college van dijkgraaf en heemraden van Waterschap Rivierenland van 22 september 2015 te Tiel.

de secretaris-directeur, ir. Z.C. Vonk
de dijkgraaf, ir. R.W. Bleker

Toelichting op het Privacyreglement Waterschap Rivierenland:

1. Algemeen:

Door snelle technologische ontwikkelingen zijn er steeds meer mogelijkheden om persoonsgegevens te verwerken. Overheden krijgen daardoor meer mogelijkheden om nieuwe diensten te ontwikkelen waar de burger veel voordeel van kan hebben. Aan de talrijke mogelijkheden die de moderne informatiemaatschappij kent, kleven echter ook gevaren. Eén van de schaduwzijden van de informatiemaatschappij is de inbreuk op de persoonlijke levenssfeer die het gevolg kan zijn van een ongebreidelde vergaring, bewerking en verspreiding van persoonsgegevens.
De hoeveelheid data die de overheid vergaart neemt steeds grotere proporties aan. En daarmee ook de roep om privacybeschermende maatregelen. Gegevens zijn een bron van informatie. Informatie is de basis van kennis en macht. Die macht kan zowel ten goede, als ten kwade worden aangewend. Het is daarom van belang dat rond de verwerking van persoonsgegevens regels worden gesteld. In artikel 10 van de Grondwet wordt het recht op eerbiediging van de persoonlijke levenssfeer erkent. De Wet bescherming persoonsgegevens (en de Wet persoonsregistraties die hieraan vooraf ging) vloeit voort uit de opdracht in de Grondwet tot het geven van nadere regels over het omgaan met persoonsgegevens

Uitgangspunten:
De Wet bescherming persoonsgegevens geeft regels voor het verwerken van persoonsgegevens. Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de Wbp, zoals naam, adres, woonplaats, e-mailadres, handtekening, telefoonnummer, godsdienst, inkomen, gezondheid en geslacht. De Wbp vereist dat al die gegevens behoorlijk en zorgvuldig worden verwerkt.

Uit gegevens van het College Bescherming Persoonsgegevens blijkt dat het verwerken, en dan met name het niet adequaat verwerken, van persoonsgegevens strijdig is met de wet en een bron van ergernis oplevert voor burgers. In uitzonderlijke gevallen kan het niet adequaat verwerken van persoonsgegevens zelfs leiden tot heel vervelende situaties, waarbij bijvoorbeeld iemands identiteit wordt ‘gestolen’ of misbruikt. Juiste toepassing van de wettelijke regels is daarom belangrijk.

Doel:
Het waarborgen van de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, in bijzonder het recht op de persoonlijke levenssfeer.
Het wegnemen van belemmeringen m.b.t. het vrije verkeer van persoonsgegevens tussen lidstaten om redenen die verband houden met deze bescherming.

In de Wet bescherming persoonsgegevens is een aantal uitgangspunten verwerkt, dat bij de verwerking van persoonsgegevens in acht moet worden genomen.

Toepassing, reikwijdte en werking van de Wbp

Evenredigheidsbeginsel
(Proportionaliteit: privacy inbreuk mag niet onevenredig zijn in verhouding tot het belang waarvoor gegevens worden verwerkt).

Een eerste uitgangspunt dat gehanteerd wordt, is dat een inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene, niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Wanneer bij de uitoefening van een bevoegdheid tot het verkrijgen van persoonsgegevens een inbreuk op een grondrecht aan de orde is, zal de verwerker van de persoonsgegevens moeten toetsen of het evenredigheidsbeginsel in het geding is. Aan de hand van de omstandigheden van het concrete geval zal de verwerker van de persoonsgegevens deze afweging moeten maken.

Noodzakelijkheidscriterium
(Subsidiariteit: Belang kan niet op andere minder belastende wijze worden gerealiseerd)
Het doel waarvoor de persoonsgegevens worden verwerkt dient in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze te kunnen worden verwerkelijkt. Het noodzakelijkheidscriterium houdt in dat van de verwerking van persoonsgegevens moet worden afgezien als hetzelfde doel ook langs andere weg en met minder ingrijpende middelen kan worden gerealiseerd, bijvoorbeeld door de vergaring van anonieme gegevens. Wordt desondanks tot gegevensverwerking overgegaan, dan is van belang dat degene die gegevens wil verwerken in redelijkheid alle eventuele bestaande mogelijkheden benut om de inbreuk op de persoonlijke levenssfeer van betrokkenen te beperken.

Gelijkheidsbeginsel
Het gelijkheidsbeginsel wordt verwoord in artikel 1 van de Grondwet en is nader uitgewerkt in de Algemene wet gelijke behandeling (AWGB). Deze wet verbiedt het maken van onderscheid tussen personen op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat bij verschillende vormen van economisch en maatschappelijk verkeer, tenzij de wet het maken van onderscheid toestaat of het om indirect onderscheid gaat dat objectief gerechtvaardigd is. De meeste van de genoemde gronden worden ook vermeld in een aantal bepalingen in de Wet bescherming persoonsgegevens over de verwerking van bijzondere gegevens. Deze bepalingen – (de artikelen 16, 17, 18 en 19) – bieden extra waarborgen bij het verwerken van persoonsgegevens betreffende onder meer iemands godsdienst of levensovertuiging, ras, politieke gezindheid en seksuele leven. Het gelijkheidsbeginsel werkt dus ook door in deze wet. Een verwerking met de bedoeling om een ongerechtvaardigd onderscheid te maken, is onrechtmatig in de zin van artikel 6 van de WBP.

2. Artikelsgewijs:

Artikel 1 Begripsbepalingen:

Een aantal begripsbepalingen wordt hier nader toegelicht:

Betrokkene:
dat is degene op wie de gegevens betrekking hebben: dit is altijd een natuurlijk persoon, individu, ofwel het data subject
Verantwoordelijke:
heeft zeggenschap over doel en wijze van verwerking. Natuurlijk persoon of rechtspersoon, of bestuursorgaan. (controller) Dit is formeel, juridisch en feitelijk (functioneel) degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft over doel en middelen van verwerking. Degene die beslist over bewaartermijnen, verstrekking inzageverzoeken etc. Binnen de overheid zijn als verantwoordelijke te kwalificeren: de afzonderlijke ministers op rijksniveau, college van GS, CdK, college van B&W en binnen waterschappen het CDH.
Beheerder:
Dit is degene die onder verantwoordelijkheid van de verantwoordelijke is belast met de dagelijkse zorg voor de verwerking van persoonsgegevens, voor de juistheid van de ingevoegde gegevens, alsmede voor het bewaren, verwijderen en verstrekken van gegevens. Het gaat hier om de proceseigenaar die binnen haar/zijn proces verantwoordelijk is voor de privacybescherming.
Bewerker:
Dit is degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. (dus extern. Is nooit intern) (processor) De bewerker: verwerkt persoonsgegevens ten behoeve van en onder verantwoordelijkheid van de verantwoordelijke. Dat wil zeggen overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. Het bepalen van de doeleinden van de verwerking en de zeggenschap daarover zijn doorslaggevend. Of en in hoeverre een bewerker de details van verwerkingswijze van persoonsgegevens kan bepalen hangt in grote mate af van de overeenkomst met de verantwoordelijke. (artt. 12, 14 en 49 van de Wbp: de bewerker is zelden verantwoordelijk, tenzij het gaat om beveiliging). De bewerker 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.

Verplichtingen in de Wet bescherming persoonsgegevens liggen primair bij de verantwoordelijke. Daaronder valt het actief toezicht houden op de bewerker. In de overeenkomst met de bewerker van persoonsgegevens moeten afspraken gemaakt worden over geheimhouding en beveiliging.

CBP: College bescherming persoonsgegevens (data protection authority). Toezichthouder

Persoonsgegevens:
Persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. De vraag die daarbij gesteld moet worden is of het een onevenredige inspanning kost om aan de hand van het gegeven de desbetreffende natuurlijke persoon te identificeren. Als dat niet het geval is dan is er sprake van een persoonsgegeven.

Wanneer is sprake van een persoonsgegeven?
Aspecten die daarbij aan de orde komen zijn de volgende:
1. identiteit (individualiseren (single out: onderscheiden van anderen) is niet genoeg. Bijv. een ip-adres wisselt, hoeft niet altijd naar één persoon te herleiden te zijn.
2. redelijkheid: is identificeren redelijkerwijs mogelijk? Kost het een onevenredige inspanning om de identiteit te achterhalen?
3. relativiteit: Wat voor de ene organisatie een persoonsgegeven is, hoeft dat voor de andere organisatie niet te zijn. Of een gegeven als een persoonsgegeven kan worden aangemerkt hangt af van de context/omstandigheden van het geval.

Wel of geen persoonsgegeven?
1. verwerking van persoonsgegevens op naam (hoeft niet altijd sprake te zijn van een persoonsgegeven);
2. identiteit van betrokkene kan met beschikbare middelen (telefoonboek, kentekenregister enz.) alsnog worden achterhaald. VB: combinatie van beroep, woonplaats en leeftijd, of postcode, huisnr. Met abonneebestand enz.
3. Identificatie kan slechts met disproportionele aanwending van geld, mankracht enz. (identificatie door de computer kost vele dagen) In dat geval zal niet snel sprake zijn van een persoonsgegeven.

Persoonsgegevens in arbeidsrelaties zijn bijv.: adres van de werknemer, foto van werknemer, rapport met statistische gegevens over het bedrijf (waaronder gemiddelde salaris per functie), klantnummer werknemer bij bijv. pensioenfonds.

Bijzondere persoonsgegevens:
Hiervoor geldt een extra streng regime: godsdienst, politieke gezindheid enz.

- Het enkele gegeven dat iemand ziek is, is al een persoonsgegeven. Voor werkgevers geldt een uitzondering op dit verbod, maar uitsluitend voor zover de gegevens noodzakelijk zijn voor uitvoering van wet, pensioen, cao's, re-integratie of begeleiding in verband met ziekte of arbeidsongeschiktheid. Verwerking van deze gegevens mag alleen door personeel dat een geheimhoudingsplicht heeft. Schending van de geheimhoudingsplicht is een misdrijf!

In het eerste lid van artikel 2 van de Wbp wordt bepaald dat de wet van toepassing is op het geheel of gedeeltelijk automatisch verwerken van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Verwerking van persoonsgegevens:
Elke handeling m.b.t. persoonsgegevens: o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwisselen of vernietigen van gegevens (enz.). Dit zijn slechts voorbeelden; elke handeling met betrekking tot persoonsgegevens (al dan niet geautomatiseerd) is een verwerking van persoonsgegevens.
Het gaat er om of er enige feitelijke macht of invloed, al dan niet via een computersysteem, over de gegevens uitgeoefend kan worden. Kan er een handeling met de gegevens worden verricht? De Wbp noemt een aantal handelingen die als verwerking worden aangeduid:
Op grond van de Wbp mogen persoonsgegevens alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. Ook moet steeds worden nagegaan of het verwerken van persoonsgegevens noodzakelijk is voor het doel. Voor de uitvoering van diverse wetten zal in de betreffende wet dikwijls zijn aangegeven welke persoonsgegevens nodig zijn en dus verwerkt mogen worden. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, geldt dus het strikte regime van de Wbp.
(Proces van gegevensverwerking)

Persoonsgegevens moeten in overeenstemming met de wet op een behoorlijke en zorgvuldige wijze worden verwerkt (artikel 6 Wbp). Het begrip zorgvuldig sluit aan bij de zorgvuldigheidsnorm in het Burgerlijk Wetboek en het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur. Dit basisbegrip wordt verder uitgewerkt in diverse bepalingen van de Wbp.
Voor de verwerking van persoonsgegevens gelden op hoofdlijnen de volgende regels:

Bij het proces van gegevensverwerking moeten een aantal stappen worden onderscheiden. In hoofdstuk 2 van de Wbp worden voorwaarden gesteld voor de rechtmatigheid van de verwerking van persoonsgegevens.

Artikel 2.
Er zijn verschillende soorten van verwerkingen, die allemaal hun eigen doeleinden hebben. Sommige van die verwerkingen komen in (vrijwel) alle organisaties voor, maar dat hoeft niet voor alle verwerkingen zo te zijn. Het kan, bij wijze van voorbeeld, gaan om verwerking in het kader van werving en selectie, de personeelsadministratie, de salarisadministratie, ziekteverzuim, controle op e-mail en internetgebruik, controle op telefoongebruik, veiligheid in de onderneming, personeelsbeoordeling, administraties betreffende aanspraken op uitkeringen in verband met de beëindiging van het dienstverband, pensioen of vervroegde uitkering. Maar eveneens moet worden gedacht aan registraties in verband met klachten of bezwaren, registraties in verband met toezicht en handhaving, vergunningverlening of grondzaken. De meest voorkomende soorten van verwerkingen zijn opgenomen als bijlagen bij dit Privacyreglement. Combinaties zijn ook mogelijk, mits ten aanzien van elk van de onderdelen van de combinatie wordt voldaan aan de daarvoor geldende bepalingen.

Artikel 4
Voor de bescherming van persoonsgegevens is de vaststelling van het doel van de verwerking, dus de verzameling en het verder gebruik daarvan, cruciaal. Het doel bepaalt namelijk welke gegevens minimaal en maximaal verwerkt mogen worden en waarvoor deze mogen gebruikt (doelbinding). Er mogen niet meer gegevens worden verwerkt dan nodig is voor het doel. De gegevens mogen niet bovenmatig, niet te gedetailleerd en zij moeten ter zake dienend, dus relevant zijn. Gegevens die door een misverstand of een verkeerd begrip door de werknemer verder gaan dan waarom is gevraagd of die voor het doel van die vraag irrelevant zijn, mogen niet worden verwerkt.
Is het voor het doel niet nodig om persoonsgegevens te verwerken, kan dus dat doel langs een andere weg worden bereikt, dan is de verwerking niet toegestaan. De gegevens, die voor een bepaald doel verwerkt worden, moeten toereikend zijn. Als te weinig gegevens worden verwerkt om het doel te kunnen bereiken is die verwerking geen geschikt middel om het doel te bereiken en daarom niet toegestaan. Er mag niet begonnen worden met het verzamelen van gegevens voordat het doel daarvan is vastgesteld. Het doel mag niet tussentijds veranderd worden.

Artikel 5
De WBP schrijft voor dat er voor elke verwerking van persoonsgegevens een rechtmatige grondslag moet zijn. Tenminste één van de volgende grondslagen moet aanwezig zijn:
1. ondubbelzinnige toestemming van de betrokkene;
2. noodzakelijk ter uitvoering van een overeenkomst, voor zover betrokkene partij is bij de uitvoering van een overeenkomst;
3. noodzakelijk voor het nakomen van een wettelijke verplichting van de verantwoordelijke;
4. noodzakelijk voor de goede vervulling van zijn publiekrechtelijke taak;
5. noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene; Het gaat hierbij met name om een dringende medische noodzaak. Een werknemer wordt onwel en verliest zijn bewustzijn. Het kan dan van levensbelang zijn om persoonsgegevens te verwerken, terwijl de werknemer niet in staat is toestemming te verlenen of te onthouden voor noodzakelijk medisch optreden.
6. noodzakelijk ter behartiging van een gerechtvaardigd belang van de verantwoordelijke, tenzij de belangen of de fundamentele rechten van de betrokkene prevaleren.

Berust de verwerking uitsluitend op de laatste grondslag, dan kan de betrokkene daartegen verzet aantekenen. Zie ook artikel 22. Een gerechtvaardigd belang is bijvoorbeeld een goede bedrijfsvoering. Het verwerken van persoonsgegevens moet gerechtvaardigd kunnen worden ten aanzien van elke individuele betrokkene. Het is bijvoorbeeld niet toegestaan om alle werknemers af te luisteren om te achterhalen of bedrijfsgeheimen aan derden worden verstrekt, wanneer slechts bepaalde werknemers een risico vormen.

Artikel 6
Persoonsgegevens worden verzameld voor een bepaald doel. Ze mogen in beginsel niet gebruikt worden voor een ander doel dan dat waarvoor ze verzameld zijn. Dat mag echter wel als het gebruik voor een ander doel niet onverenigbaar is met het oorspronkelijke doel. Of de verdere verwerking onverenigbaar is, hangt af van verschillende factoren. Eén daarvan is de verwachting die de betrokkene

heeft ten aanzien van het gebruik van zijn persoonsgegevens. Een camera die geïnstalleerd is ter bescherming van loketmedewerkers mag niet tevens worden gebruikt ter beoordeling van die medewerkers. Een andere factor is de mate van verwantschap tussen het oorspronkelijke doel en het doel van de verdere verwerking. Hoe dichter de doelen bij elkaar liggen, hoe eerder de verdere verwerking verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Persoonsgegevens die worden verzameld in de vorm van 'tijdschrijven' om een beter beeld te krijgen van de globale tijdsbesteding van het personeel om vervolgens de organisatie beter te kunnen aansturen, mogen bijvoorbeeld niet gebruikt worden voor aanwezigheidsregistratie of beoordeling van de individuele personeelsleden. Een hanteerbare praktische stelregel om te beoordelen of een bepaald doel verenigbaar is met het oorspronkelijke doel, is dat protest tegen of vragen over het gebruik van het verdere doel wijst op onverenigbaarheid van dat doel met het oorspronkelijke doel. De beide doelen liggen dan tenminste niet zonder meer in elkaars verlengde.
Ook de aard van de gegevens is van belang. Hoe gevoeliger de gegevens, hoe minder snel de gegevens ook voor een ander doel gebruikt mogen worden. Gegevens over naam, adres en woonplaats mogen bijvoorbeeld eerder voor een ander doel gebruikt worden dan salarisgegevens.
De gevolgen van de beoogde (verdere) verwerking voor de betrokkene zijn eveneens relevant. Als die bijvoorbeeld tot gevolg heeft dat een bepaalde beslissing over de betrokkene wordt genomen, is al snel sprake van onverenigbaarheid. Een ziektekostenverzekeraar die medische gegevens over de betrokkene heeft verkregen, mag die gegevens bijvoorbeeld niet gebruiken om daarop een beslissing te baseren om met betrokkene al dan niet een levensverzekering aan te gaan.
Een factor is verder de wijze waarop de gegevens zijn verkregen. Een werkgever die kan aantonen dat het voor de bestrijding van fraude noodzakelijk is om zonder vooraankondiging telefoongesprekken van werknemers op te nemen, mag deze vervolgens niet zomaar gebruiken voor de beoordeling van die werknemers. Relevant is ook de mate waarin passende waarborgen voor de betrokkene zijn genomen.

Artikel 8
De verwerking kan betrekking hebben op iedereen die in dienst is van de verantwoordelijke of anderszins ten behoeve van de verantwoordelijke werkzaam is, zoals werknemers en oud-werknemers, soms ook om stagiaires, oproepkrachten, uitzendkrachten of vrijwilligers. Daarnaast worden in het kader van de taakuitoefening door het waterschap persoonsgegevens verwerkt.

Artikel 9
Bij soorten van gegevens gaat het in de meeste gevallen om gegevens over iemands naam, adres en woonplaats. Maar ook telefoonnummers, kentekens en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. De verwerking van bijzondere persoonsgegevens is in principe verboden. Als bijzondere gegevens worden aangemerkt gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, vakbondslidmaatschap alsmede strafrechtelijke gegevens. De wet noemt uitzonderingen op het verbod van verwerking van bijzondere persoonsgegevens. Het is bijvoorbeeld wel toegestaan gegevens over iemands ras te verwerken in het kader van een voorkeursbeleid. En onder bepaalde voorwaarden mogen verzekeraars gegevens verwerken over iemands gezondheid. Persoonsgegevens over het lidmaatschap van een vakbond mogen uitsluitend door vakbonden en vakcentrales verwerkt worden, voor zover dat gelet op hun doelstelling noodzakelijk is. Voor verstrekking van die gegevens aan derden is altijd toestemming van het betrokken vakbondslid nodig.

Dat de persoonsgegevens ‘toereikend’ moeten zijn voor het doel van de verwerking houdt in dat de verantwoordelijke ook niet te weinig gegevens mag verwerken. Alle gegevens die voor het doel noodzakelijk zijn, moeten worden verwerkt. Als te weinig gegevens worden verzameld, kan een onvolledig beeld van de betrokkene ontstaan.

Artikel 10
Persoonsgegevens mogen niet langer worden bewaard dan nodig is voor het doel waarvoor de gegevens worden verzameld of (verder) verwerkt.
Vernietiging van gegevens betekent veelal het fysiek vernietigen van de gegevensdragers waarop ze staan dan wel het wissen van gegevens op gegevensdragers.

Artikel 12
Essentieel voor de bescherming van de privacy is de toegang tot de gegevens. Wat betreft de rechtstreekse toegang tot persoonsgegevens is het de beheerder die bepaalt welke gebruikers bevoegd zijn bepaalde handelingen met bepaalde persoonsgegevens te verrichten. Voor al deze personen geldt een geheimhoudingsplicht. Ook de verantwoordelijke, bijvoorbeeld in de persoon van de algemeen directeur, heeft als zodanig toegang tot persoonsgegevens, maar deze dient de organisatie zo in te richten dat hij niet zonder noodzaak en ongevraagd met die gegevens wordt geconfronteerd.

Artikel 13

Indien aan de technische apparatuur waarmee persoonsgegevens worden verwerkt reparaties of onderhoudswerkzaamheden moeten worden verricht, schrijft dit artikel voor dat alleen personen de werkzaamheden mogen uitvoeren die een geheimhoudingsverklaring hebben ondertekend.

Artikel 14
Bij verstrekking buiten de organisatie gaat het bijvoorbeeld om de fiscus, de uitvoeringsinstelling, de Arbodienst of de verzekeringsmaatschappij waarmee individuele of collectieve verzekeringen zijn afgesloten, het pensioenfonds of het CPB in verband met bedrijfsvergelijkingen.
Gegevens mogen zonder toestemming van de werknemer worden doorgegeven indien dit geschiedt op grond van een wettelijk voorschrift.
Indien tot de arbeidsverhouding employee benefits behoren, kunnen die gegevensverstrekking aan bijvoorbeeld een verzekeraar meebrengen. Dit hangt onder meer af van de vraag op welke wijze en met welk doel die gegevens zijn verzameld. Voorts hangt dit af van de aard van de gegevens en van de vraag of de werknemer gerichte schriftelijke toestemming daartoe gegeven heeft. Ook is van belang of het verstrekken van die gegevens min of meer direct voortvloeit uit de arbeidsverhouding (noodzakelijk is voor de uitvoering van de arbeidsovereenkomst). Dit is weer afhankelijk van kwesties of de employee benefits in bepaalde mate onderdeel uitmaken van de arbeidsverhouding dan wel iets extra's inhouden daarnaast of daarboven en of sprake is van een verplichte dan wel een vrijwillige deelname aan de betreffende collectieve arrangementen.
Staat het de werknemer bijvoorbeeld vrij om deel te nemen aan een collectieve particuliere ziektekostenverzekering, dan mag de werkgever de betrokken verzekeraar geen lijst met namen en adressen van de belanghebbende werknemers verschaffen. Hij zal de eerste mailing zelf moeten verzorgen. Pas indien één of meer werknemers naar aanleiding van die mailing te kennen geeft deel te willen nemen, ontstaat er - mits de werknemer daarover vooraf is geïnformeerd - een relatie tussen de verzekeraar en de werknemer en zal de verzekeraar in beginsel aan die werknemer(s) een tweede mailing mogen verzorgen.
Soms vraagt een verzekeraar aan de werkgever of deze namens die verzekeraar reclamepost wil verzenden, bijvoorbeeld voor het afsluiten van een (andere) voordelige collectieve verzekering. In dit geval moet de werkgever het personeel vooraf op de hoogte stellen van zijn voornemen om dit te doen en het in de gelegenheid stellen om bezwaar te maken. Zo wordt bereikt dat alleen de geïnteresseerde personeelsleden reclamepost ontvangen.
Doorgifte van personeelsgegevens in verband met de mogelijke overname van het bedrijf mag alleen als die gegevens eerst geanonimiseerd worden.

Artikel 15
Het verstrekken van persoonsgegevens binnen één bedrijf, dus van de ene vestiging aan de andere, wordt gezien als het verstrekken van persoonsgegevens aan een derde. Er is dus niet sprake van één en dezelfde verantwoordelijke. Een verstrekking aan een bedrijf of vestiging in een land buiten de Europese Unie wordt aangeduid als doorgifte. Een dergelijke doorgifte is in beginsel alleen geoorloofd als zo'n land een passend beschermingsniveau heeft. Dat zo'n land dat heeft kan de minister van Justitie bij ministeriële beschikking bekend maken. Dat oordeel is bijvoorbeeld uitgesproken over Zwitserland en Hongarije.
Door middel van een contract kan worden bereikt dat een bedrijf of vestiging in een land zonder passend beschermingsbureau als bedrijf of vestiging voor de overeengekomen verwerkingen wel een passend beschermingsniveau biedt. Een dergelijk contract moet dan wel aan verschillende voorwaarden voldoen. Daarvoor heeft de Europese Commissie modelcontractbepalingen vastgesteld.

Artikel 16
De verantwoordelijke is gehouden tot het treffen van de nodige voorzieningen. Zo moet hij een beveiligingsplan op te stellen, inclusief gedragsregels met betrekking tot de omgang met gegevens. Deze voorzieningen moeten worden uitgewerkt en gecontroleerd door de beheerder.

Artikel 17
Uitgangspunt van de wet is volledige openheid met betrekking tot alle verwerkingen die plaatsvinden. Dit artikel schrijft voor dat, wanneer de betrokkenen nog niet op de hoogte zijn, zij actief geïnformeerd moeten worden over de doeleinden van de verwerking.
De verantwoordelijke mag er na toezending of uitreiking vanuit gaan dat betrokkenen op de hoogte zijn. Het is onvoldoende dat de betrokkenen redelijkerwijs op de hoogte hadden kunnen zijn, bijvoorbeeld omdat door onderzoek te achterhalen is wie de verantwoordelijke is en voor welke doeleinden de gegevens worden verwerkt. Ook een expliciete verwijzing door de verantwoordelijke naar elders verkrijgbare informatie is onvoldoende.
Nadere informatie moet verschaft worden als dat tegenover de betrokkene nodig is om een behoorlijke en zorgvuldige verwerking te waarborgen. Of dat zo is hangt af van de aard van de gegevens, de omstandigheden waaronder deze worden of zijn verkregen en het gebruik dat ervan gemaakt wordt. Hoe gevoeliger de gegevens voor de betrokkene, hoe meer reden er is de betrokkene gedetailleerd te informeren over de gegevensverwerking.

Een voorbeeld: de werkgever vraagt aan de werknemer informatie in het kader van een collectieve aanvullende ziektekostenverzekering. Om statistische redenen of met het oog op toezending van geadresseerde reclame door de betreffende ziektekostenverzekeraar wordt daarbij informatie van de werknemer gevraagd, die niet essentieel is voor deelname aan de collectieve verzekering. Het verstrekken van de informatie kan achterwege blijven zonder dat daarmee het gevraagde deelnemerschap in gevaar komt. In een dergelijk geval behoort de werkgever de werknemer daarvan vooraf in kennis te stellen. Dat wil zeggen: hij moet duidelijk maken voor welke doelen hij de informatie vraagt, welke gegevens voor welk doel zijn bestemd en wat de gevolgen zijn als bepaalde gegevens niet worden verstrekt. Als de gegevens bij de betrokkene zelf worden verkregen, moet de verantwoordelijke de betrokkene vóór de verkrijging informeren. De relevante informatie kan bijvoorbeeld op het door betrokkene in te vullen formulier worden opgenomen. Dit is vanzelfsprekend het geval als de werknemer bij indiensttreding de nodige formulieren ten behoeve van de personeels- en salarisadministratie invult.

Werknemers moeten weten dat over hen persoonsgegevens worden verzameld, vastgelegd en verder verwerkt. Dit is een belangrijk deel van de privacybescherming. Hierin past dat de OR betrokken wordt bij de besluitvorming over de verwerking van persoonsgegevens – met instemmingsrecht – maar dit is onvoldoende. Het is nodig dat werknemers zonder dat zij daarom hoeven te vragen worden geïnformeerd over het feit dat over hen informatie wordt verwerkt, door wie, hoe en met welk doel. De werkgever moet de werknemers bijvoorbeeld ongevraagd informeren over het feit dat hij in een magazijn een videocamera heeft opgesteld om bepaalde daar aanwezige dure apparatuur te bewaken. Het besluit om in bepaalde gevallen voor bepaalde doelen camera's te plaatsen is onderworpen aan het instemmingsrecht van de OR.

De informatieplicht van de verantwoordelijke geldt uiteraard niet alleen ten opzichte van medewerkers van het waterschap, maar ten opzichte van alle betrokkenen waarvan persoonsgegevens worden verwerkt.

Artikel 18
De beheerder wijst betrokkenen op de mogelijkheden van rechtsbescherming en toezicht en op de rol daarin van het College bescherming persoonsgegevens en de privacyfunctionaris, alsmede van de onderlinge relatie tussen laatstgenoemden.

Artikel 19
De verantwoordelijke is niet alleen verplicht om ongevraagd informatie te verstrekken, zoals omschreven in artikel 17. Hij is ook verplicht om desgevraagd de betrokkene te informeren.
De betrokkene hoeft op zijn beurt niet af te wachten wanneer de verantwoordelijke hem uit eigen beweging informeert, maar heeft ook het recht om de verlangde informatie zelf op een door hem gewenst moment op te vragen.

Artikel 20
De betrokkene mag te allen tijde, uiteraard met redelijke tussenpozen, verzoeken kennis te nemen van de eigen persoonsgegevens. Een dergelijk verzoek wordt ingediend bij de beheerder. Op grond van uitzonderlijke omstandigheden kan de verlangde inzage (deels) worden geweigerd, bijvoorbeeld omdat door inzage de privacy van anderen wordt geschonden of omdat in het kader van een opsporingsonderzoek inzage op dat moment niet wenselijk is.

N.B. De beheerder doet dit, zoals alles, onder verantwoordelijkheid van de verantwoordelijke.
Blijft de beheerder in gebreke, dan kan dus ook de verantwoordelijke daarop worden aangesproken.

Artikel 21
Correctie houdt behalve verbeteren, aanvullen en verwijderen ook in: afschermen of op een andere manier ervoor zorgen dat de onjuiste gegevens niet langer worden gebruikt. Als het technisch niet mogelijk is de gegevens te verbeteren, kan de beheerder bijvoorbeeld een bestand met aanvullingen en verbeteringen opnemen.

Artikel 22
De betrokkene kan in een aantal gevallen bezwaar maken tegen een gegevensverwerking. De WBP noemt dat het recht van verzet. De betrokkene heeft een relatief recht van verzet als het verwerken van zijn persoonsgegevens plaatsvindt op de grondslag dat de verwerking noodzakelijk is voor een gerechtvaardigd belang van de verantwoordelijke. Dat verzet dient te worden gehonoreerd indien bijzondere persoonlijke omstandigheden van de betrokkene zwaarder moeten wegen dan het belang van de verantwoordelijke. De betrokkene heeft een absoluut recht van verzet als het verwerken van zijn persoonsgegevens plaatsvindt voor direct marketingdoelen. In dat geval moet de verwerking zonder meer worden beëindigd.

Artikel 23

De betrokken werknemer die schade lijdt doordat de verantwoordelijke werkgever in strijd handelt met de WBP en/of dit reglement, kan deze schade op de werkgever verhalen, ook eventuele immateriële schade. De verantwoordelijke is ook aansprakelijk voor schade die is ontstaan doordat de beheerder of de bewerker een overtreding begaat.
In het uiterste geval, wanneer de betrokken werknemer zich genoodzaakt ziet zich tot de rechter te wenden, kan de rechter de werkgever een schadevergoeding en/of een verbod of gebod opleggen.
In spoedeisende gevallen, bijvoorbeeld bij dreigende schade, kan betrokkene zich direct tot de rechter wenden. Die kan bijvoorbeeld de verantwoordelijke verbieden bepaalde gegevens aan een derde te verstrekken of hem gebieden bepaalde gegevens uit zijn systeem te verwijderen.

Informatie over de behandeling van een klacht door het College bescherming persoonsgegevens is te vinden op de website van het College.

Artikel 25
De bedoelde scholing houdt onder meer in dat de gebruikers het belang van zorgvuldige verwerking inzien en de mogelijke gevolgen van een onzorgvuldige verwerking. Betrokkenen mogen op geen enkele wijze nadeel ondervinden van het niet, onjuist of incompleet verstrekken van persoonsgegevens.

Artikel 27
Het opstellen van een reglement bevordert de transparantie van de verwerkingsprocessen in de organisatie. Het reglement behoort voor een ieder ter inzage te liggen. Een ieder moet ook in kennis worden gesteld van het ter inzage liggen.

Bijlage 1.3 van bijlage 1
Handreiking overzicht privacywetgeving binnen de overheid

Ontwikkeling van privacywetgeving:
1948: Universele verklaring (art. 12) (echter niet afdwingbaar);
1950: EVRM (art. 8) (wel afdwingbaar) : communicatiegeheim:
Art. 8 EVRM: Recht op eerbiediging van privéleven, familie en gezinsleven
Lid 1: een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleen, zijn woning en zijn correspondentie.
Lid 2: geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale vrijheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.
Bovenstaande zijn fundamentele rechten.

1995: Privacyrichtlijn 95/46/EC: Richtlijn ter bescherming van de interne markt.
Implementatie nodig. Dat is gebeurd via de Wbp en de Data Protection Act 1998.

Privacyrichtlijn 95/46/EG
Grondslag art. 95 (100 A) EG: maatregelen inzake onderlinge aanpassing van de wettelijke en bestuurlijke bepalingen die de instelling van de interne markt betreffen.
Doelen:
Waarborgen van de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen. Recht op persoonlijke levenssfeer. Wegnemen belemmeringen m.b.t. vrije verkeer van persoonsgegevens tussen lidstaten om redenen die verband houden met deze bescherming.

Toekomstige Europese regelgeving:
2014: wetsvoorstel voor een General regulation on Data Protection (art. 14(2), 116 lid 1 VwEU):
De Algemene Verordening Gegevensbescherming

Wetsvoorstel 33662: Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken)

ePrivacyrichtlijn 2002/58/EG
In de Wet bescherming persoonsgegevens is de privacyrichtlijn 95/46/ EG geïmplementeerd.. De Wbp heeft een omnibuskarakter. Kaderwet met gelaagd karakter.

Juridisch kader Wet bescherming persoonsgegevens:
Er zijn meerdere wetten die zien op hoe we moeten omgaan met privacygevoelige gegevens. De Wet bescherming persoonsgegevens (Wbp) en ook de Wet openbaarheid van bestuur (Wob) zijn de belangrijkste. Ook geeft de Archiefwet regels over onder meer bewaartermijnen.

In 2001 werd de Wet persoonsregistraties vervangen door de Wbp. De Wbp is op hoofdlijnen gelijk aan de Europese richtlijn 95/46/EG die op 25 oktober 1995 werd aangenomen. Deze richtlijn beschrijft de wijze waarop in de lidstaten moet worden omgegaan met persoonsgegevens. Inmiddels wordt gewerkt aan een nieuwe richtlijn.

Naast de Wbp wordt privacy geregeld o.a. in Grondwet.
Eerbiediging van de persoonlijke levenssfeer is een van de grondslagen van onze rechtsorde. Het recht op eerbiediging van de persoonlijke levenssfeer is vastgelegd in artikel 10 van de Grondwet.
artikel 10 Grw.
1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van de persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens;
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hem vastgelegde gegevens en van het gebruik dat daarvan gemaakt wordt, alsmede op verbetering van zodanige gegevens.

Art. 13 Grw: briefgeheim, (ook hierin is het right to be left alone verankerd)
1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

- EVRM (hierin geregeld privacy en communicatiegeheim) (art. 8)
- Telecommunicatiewet: verkeers- en locatiegegevens, spyware, cookies, spam en telemarketing enz.
- De Algemene wet inzake rijksbelastingen
- Wet geneeskundige behandelingsovereenkomst (Wgbo)
- Wet openbaarheid van bestuur (Wob)
- WvSr., WvSv
- Awb
- Wet basisregistratie personen (de Wet BRP) en regelgeving die daarop gebaseerd is, denk aan:

1. Aanpassingsbesluit Politiewet 2012
2. Aanpassingsbesluit Zorgverzekeringswet
3. Aanpassingsregeling Zorgverzekeringswet
4. Beleidsregel UWV gebruik adresgegevens
5. Besluit basisregistratie personen
6. Besluit burgerservicenummer
7. Besluit Jeugdwet
8. Besluit uitvoering Pensioenwet en Wet verplichte beroepspensioenregeling
9. Regeling basisregistratie personen

De Wet bescherming persoonsgegevens is overigens niet van toepassing op de verwerkingen door het waterschap van gegevens uit de Gemeentelijke Basisadministratie (dat is een uitgezonderde verwerking). In de Beheerregeling BRP zijn specifieke GBA-normen opgenomen.
Hoofdlijnen Wbp

Doel:
Het waarborgen van de bescherming van de fundamentele rechten en vrijheden van natuurlijke personen, in bijzonder het recht op de persoonlijke levenssfeer.
Het wegnemen van belemmeringen m.b.t. het vrije verkeer van persoonsgegevens tussen lidstaten om redenen die verband houden met deze bescherming.

Achtergrond:
Door snelle technologische ontwikkelingen zijn er steeds meer mogelijkheden om persoonsgegevens te verwerken. Overheden krijgen daardoor meer mogelijkheden om nieuwe diensten te ontwikkelen waar de burger veel voordeel van kan hebben. Aan de talrijke mogelijkheden die de moderne informatiemaatschappij kent, kleven echter ook gevaren. Eén van de schaduwzijden van de informatiemaatschappij is de inbreuk op de persoonlijke levenssfeer die het gevolg kan zijn van een ongebreidelde vergaring, bewerking en verspreiding van persoonsgegevens.
De hoeveelheid data die de overheid vergaart neemt steeds grotere proporties aan. En daarmee ook de roep om privacybeschermende maatregelen. Gegevens zijn een bron van informatie. Informatie is de basis van kennis en macht. Die macht kan zowel ten goede, als ten kwade worden aangewend. Het is daarom van belang dat rond de verwerking van persoonsgegevens regels worden gesteld. In artikel 10 van de Grondwet wordt het recht op eerbiediging van de persoonlijke levenssfeer erkent. De Wet

bescherming persoonsgegevens (en de Wet persoonsregistraties die hieraan vooraf ging) vloeit voort uit de opdracht in de Grondwet tot het geven van nadere regels over het omgaan met persoonsgegevens

Uitgangspunten:
De Wet bescherming persoonsgegevens geeft regels voor het verwerken van persoonsgegevens. Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de Wbp, zoals naam, adres, woonplaats, e-mailadres, handtekening, telefoonnummer, godsdienst, inkomen, gezondheid en geslacht. De Wbp vereist dat al die gegevens behoorlijk en zorgvuldig worden verwerkt.

Uit gegevens van het College Bescherming Persoonsgegevens blijkt dat het verwerken, en dan met name het niet adequaat verwerken, van persoonsgegevens strijdig is met de wet en een bron van ergernis oplevert voor burgers. In uitzonderlijke gevallen kan het niet adequaat verwerken van persoonsgegevens zelfs leiden tot heel vervelende situaties, waarbij bijvoorbeeld iemands identiteit wordt 'gestolen' of misbruikt. Juiste toepassing van de wettelijke regels is daarom belangrijk.

In de Wet bescherming persoonsgegevens is een aantal uitgangspunten verwerkt, dat bij de verwerking van persoonsgegevens in acht moet worden genomen.

Toepassing, reikwijdte en werking van de Wbp

Evenredigheidsbeginsel
(Proportionaliteit: privacyinbreuk mag niet onevenredig zijn in verhouding tot het belang waarvoor gegevens worden verwerkt).
Een eerste uitgangspunt dat gehanteerd wordt, is dat een inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene, niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Wanneer bij de uitoefening van een bevoegdheid tot het verkrijgen van persoonsgegevens een inbreuk op een grondrecht aan de orde is, zal de verwerker van de persoonsgegevens moeten toetsen of het evenredigheidsbeginsel in het geding is. Aan de hand van de omstandigheden van het concrete geval zal de verwerker van de persoonsgegevens deze afweging moeten maken.

Noodzakelijkheidscriterium
(Subsidiariteit: Belang kan niet op andere minder belastende wijze worden gerealiseerd)
Het doel waarvoor de persoonsgegevens worden verwerkt dient in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze te kunnen worden verwerkelijkt. Het noodzakelijkheidscriterium houdt in dat van de verwerking van persoonsgegevens moet worden afgezien als hetzelfde doel ook langs andere weg en met minder ingrijpende middelen kan worden gerealiseerd, bijvoorbeeld door de vergaring van anonieme gegevens. Wordt desondanks tot gegevensverwerking overgegaan, dan is van belang dat degene die gegevens wil verwerken in redelijkheid alle eventuele bestaande mogelijkheden benut om de inbreuk op de persoonlijke levenssfeer van betrokkenen te beperken.

Gelijkheidsbeginsel
Het gelijkheidsbeginsel wordt verwoord in artikel 1 van de Grondwet en is nader uitgewerkt in de Algemene wet gelijke behandeling (AWGB). Deze wet verbiedt het maken van onderscheid tussen personen op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat bij verschillende vormen van economisch en maatschappelijk verkeer, tenzij de wet het maken van onderscheid toestaat of het om indirect onderscheid gaat dat objectief gerechtvaardigd is. De meeste van de genoemde gronden worden ook vermeld in een aantal bepalingen in de Wet bescherming persoonsgegevens over de verwerking van bijzondere gegevens. Deze bepalingen – (de artikelen 16, 17, 18 en 19) – bieden extra waarborgen bij het verwerken van persoonsgegevens betreffende onder meer iemands godsdienst of levensovertuiging, ras, politieke gezindheid en seksuele leven. Het gelijkheidsbeginsel werkt dus ook door in deze wet. Een verwerking met de bedoeling om een ongerechtvaardigd onderscheid te maken, is onrechtmatig in de zin van artikel 6 van de WBP.

Enkele belangrijke begrippen in de Wet bescherming persoonsgegevens:

In hoofdstuk 1 van de Wbp wordt een aantal begrippen gedefinieerd.

Betrokkene:
dat is degene op wie de gegevens betrekking hebben: dit is altijd een natuurlijk persoon, individu, ofwel het data subject
Verantwoordelijke:
heeft zeggenschap over doel en wijze van verwerking. Natuurlijk persoon of rechtspersoon, of bestuursorgaan. (controller)Dit is formeel, juridisch en feitelijk (functioneel) degene die het doel van en de

middelen voor de verwerking van persoonsgegevens vaststelt.Degene die zeggenschap heeft over doel en middelen van verwerking. Degene die beslist over bewaartermijnen, verstrekking inzageverzoeken etc. Binnen de overheid zijn als verantwoordelijke te kwalificeren: de afzonderlijke ministers op rijksniveau, college van GS, CdK, college van B&W en binnen waterschappen het CDH.
Bewerker:
Dit is degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen. (dus extern. Is nooit intern) (processor) De bewerker: verwerkt persoonsgegevens ten behoeve van en onder verantwoordelijkheid van de verantwoordelijke. Dat wil zeggen overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. Het bepalen van de doeleinden van de verwerking en de zeggenschap daarover zijn doorslaggevend. Of en in hoeverre een bewerker de details van verwerkingswijze van persoonsgegevens kan bepalen hangt in grote mate af van de overeenkomst met de verantwoordelijke. (artt. 12, 14 en 49 van de Wbp: de bewerker is zelden verantwoordelijk, tenzij het gaat om beveiliging). De bewerker 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.
CBP: College bescherming persoonsgegevens (data protection authority). Toezichthouder
FG: Functionaris gegevensbescherming (de privacy officer)

Verplichtingen in de Wet bescherming persoonsgegevens liggen primair bij de verantwoordelijke. Daaronder valt het actief toezicht houden op de bewerker. In de overeenkomst met de bewerker van persoonsgegevens moeten afspraken gemaakt worden over geheimhouding en beveiliging.

Wat zijn persoonsgegevens?

Persoonsgegevens zijn gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. De vraag die daarbij gesteld moet worden is of het een onevenredige inspanning kost om aan de hand van het gegeven de desbetreffende natuurlijke persoon te identificeren. Als dat niet het geval is dan is er sprake van een persoonsgegeven.

Wanneer is sprake van een persoonsgegeven?
Aspecten die daarbij aan de orde komen zijn de volgende:
1. identiteit (individualiseren (single out: onderscheiden van anderen) is niet genoeg. Bijv. een ip-adres wisselt, hoeft niet altijd naar één persoon te herleiden te zijn.
2. redelijkheid: is identificeren redelijkerwijs mogelijk? Kost het een onevenredige inspanning om de identiteit te achterhalen?
3. relativiteit: Wat voor de ene organisatie een persoonsgegeven is, hoeft dat voor de andere organisatie niet te zijn. HET HANGT ER VANAF!!

Wel of geen persoonsgegeven?
1. verwerking van persoonsgegevens op naam (hoeft niet altijd sprake te zijn van een persoonsgegeven);
2. identiteit van betrokkene kan met beschikbare middelen (telefoonboek, kentekenregister enz.) alsnog worden achterhaald. VB: combinatie van beroep, woonplaats en leeftijd, of postcode, huisnr. Met abonneebestand enz.
3. Identificatie kan slechts met disproportionele aanwending van geld, mankracht enz. (identificatie door de computer kost vele dagen) In dat geval zal niet snel sprake zijn van een persoonsgegeven.

Persoonsgegevens in arbeidsrelaties zijn bijv.: adres van de werknemer, foto van werknemer, rapport met statistische gegevens over het bedrijf (waaronder gemiddelde salaris per functie), klantnummer werknemer bij bijv. pensioenfonds.

Bijzondere persoonsgegevens:
Hiervoor geldt een extra streng regime: godsdienst, politieke gezindheid enz.

- Het enkele gegeven dat iemand ziek is, is al een persoonsgegeven. Voor werkgevers geldt een uitzondering op dit verbod, maar uitsluitend voor zover de gegevens noodzakelijk zijn voor uitvoering van wet, pensioen, cao's, re-integratie of begeleiding in verband met ziekte of arbeidsongeschiktheid. Verwerking van deze gegevens mag alleen door personeel dat een geheimhoudingsplicht heeft. Schending van de geheimhoudingsplicht is een misdrijf!

In het eerste lid van artikel 2 van de Wbp wordt bepaald dat de wet van toepassing is op het geheel of gedeeltelijk automatisch verwerken van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Verwerking van persoonsgegevens:

Elke handeling m.b.t. persoonsgegevens: o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken d.m.v. doorzending, verspreiding of enige andere vorm van ter beschikking stelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwisselen of vernietigen van gegevens (enz.). Dit zijn slechts voorbeelden; elke handeling met betrekking tot persoonsgegevens (al dan niet geautomatiseerd) is een verwerking van persoonsgegevens.
Het gaat er om of er enige feitelijke macht of invloed, al dan niet via een computersysteem, over de gegevens uitgeoefend kan worden. Kan er een handeling met de gegevens worden verricht? De Wbp noemt een aantal handelingen die als verwerking worden aangeduid:
Op grond van de Wbp mogen persoonsgegevens alleen verzameld worden als daarvoor een doel bestaat. Dit doel moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn. Ook moet steeds worden nagegaan of het verwerken van persoonsgegevens noodzakelijk is voor het doel. Voor de uitvoering van diverse wetten zal in de betreffende wet dikwijls zijn aangegeven welke persoonsgegevens nodig zijn en dus verwerkt mogen worden. Daar waar over verwerking van persoonsgegevens in bijzondere wetgeving niets is geregeld, geldt dus het strikte regime van de Wbp.

(Proces van gegevensverwerking)
Persoonsgegevens moeten in overeenstemming met de wet op een behoorlijke en zorgvuldige wijze worden verwerkt (artikel 6 Wbp). Het begrip zorgvuldig sluit aan bij de zorgvuldigheidsnorm in het Burgerlijk Wetboek en het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur. Dit basisbegrip wordt verder uitgewerkt in diverse bepalingen van de Wbp.
Voor de verwerking van persoonsgegevens gelden op hoofdlijnen de volgende regels:
•

Bij het proces van gegevensverwerking moeten een aantal stappen worden onderscheiden. In hoofdstuk 2 van de Wbp worden voorwaarden gesteld voor de rechtmatigheid van de verwerking van persoonsgegevens. Hieronder een toelichting op de artikelen in dit hoofdstuk.

1. Algemeen: gegevensverwerking in overeenstemming met de wet en behoorlijk en zorgvuldig (artikel 6).

Artikel 6 keert zich tegen die vormen van gegevensverwerking die als unfair of oneerlijk worden beschouwd. Voorwaarde voor een eerlijke verwerking van gegevens is dat de betrokkenen van het bestaan van de verwerking kennis kunnen hebben en wanneer van hen gegevens worden verkregen, daadwerkelijk en volledig worden ingelicht over de omstandigheden waaronder deze worden verkregen. Het is dus verboden om onopgemerkt gegevens van personen te verzamelen en te verwerken. In het Strafrecht zijn tegen dit soort praktijken strafbepalingen opgenomen. Bijv. tegen het illegaal afluisteren van telefoongesprekken, het illegaal maken van afbeeldingen van personen met heimelijk opgestelde camera's in niet voor het publiek toegankelijke ruimten.

2. Verzameling voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7).

In dit artikel is geregeld dat er sprake moet zijn van een welbepaald doel, dat bovendien gerechtvaardigd moet zijn (het belang van de verantwoordelijke moet aanleiding geven tot de verwerking van gegevens en mag niet in strijd zijn met de wet, de openbare orde of de goede zeden. In het eerste lid van artikel 9 wordt in aansluiting hierop bepaald dat de gegevens (vervolgens) niet mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. (p. 78MvT) Niet alleen moet het doel bepaald zijn, het doel moet ook gerechtvaardigd zijn. Van gerechtvaardigde doeleinden kan alleen sprake zijn als deze met inachtneming van de in artikel 8 genoemde gronden kunnen worden verwerkt. Het doel mag nooit in strijd met regels van geschreven of ongeschreven recht zijn. Het vergaren van gegevens met het doel daarmee illegale activiteiten te verrichten is dus in strijd met art. 8 en dus ook in strijd met art. 7 van de Wbp.

In artikel 9 wordt vervolgens bepaald dat gegevens niet mogen worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Gegevens mogen dus wel worden gebruikt voor andere doelen dan waarvoor zij zijn verzameld. Maar dit andere doel moet verenigbaar zijn met het oorspronkelijke doel.

De omschrijving van het doel blijkt uit de melding van de verwerking bij het College bescherming persoonsgegevens (CBP) of bij de functionaris voor de gegevensbescherming (artikel 28 WBP) of uit de doelstelling van één van de verwerkingen van persoonsgegevens genoemd in het Vrijstellingsbesluit (artikel 29 WBP);

3. Grondslag rechtmatigheid gegevensverwerking (artikel 8: is uitwerking van «gerechtvaardigde doeleinden» als bedoeld in artikel 7).

Artikel 8 bevat een limitatieve opsomming van de gronden die een gegevensverwerking rechtvaardigen. Elke verwerking moet voldoen aan het proportionaliteitsbeginsel (evenredigheid) en het subsidiariteitsbeginsel (noodzakelijkheid) (zie hierboven).
De verantwoordelijke moet een gerechtvaardigd belang hebben bij de verwerking van persoonsgegevens. Hierbij moet in alle stadia van de verwerking altijd minimaal één van de volgende voorwaarden van toepassing zijn (artikel 8 WBP):
Persoonsgegevens mogen slechts worden verwerkt indien: (limitatieve opsomming)

a. De betrokkene zijn toestemming heeft gegeven (deze grond is niet exclusief, ook op andere gronden kunnen gegevens worden verwerkt, de wet kan zelfs toestemming van betrokkene als rechtvaardigingsgrond uitsluiten bijv. in geval van ongelijke machtsverhoudingen tussen verantwoordelijke en betrokkene).
b. Gegevensverwerking is toelaatbaar als deze noodzakelijk is om contractuele verplichtingen na te komen. Daarbij geldt als voorwaarde dat betrokkene partij is bij de betreffende overeenkomst.
c. Gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke is onderworpen.
d. Hier gelden 2 criteria: gegevensverwerking moet noodzakelijk zijn ter uitvoering van een wettelijke plicht en verantwoordelijke moet belast zijn met de uitvoering van die wettelijke verplichting.
e. Gegevensverwerking is gerechtvaardigd als deze noodzakelijk is ter bestrijding van ernstig gevaar voor de gezondheid van de betrokkene.
f. Gegevensverwerking is mogelijk voorzover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak.
g. Een gegevensverwerking ter vervulling van een publiekrechtelijke taak kan eveneens geschieden zonder dat daaraan een wettelijke verplichting ten grondslag ligt.
h. Een betrokkene heeft wel het recht zich tegen gegevensverwerking te verzetten als deze verwerking noodzakelijk is ter vervulling van een publiekrechtelijke taak, maar niet in geval van een wettelijke verplichting tot gegevensverwerking door de verantwoordelijke.
i. Gegevensverwerking is geoorloofd indien deze noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, doorslaggevend zijn. (noodzakelijkheidscriterium).

In geval een betrokkene rechtsgeldig toestemming heeft verleend, maar later besluit zijn toestemming in te trekken dan is dat mogelijk. Betrokkene heeft te allen tijde het recht zijn toestemming in te trekken. De rechtsgrondslag komt dan aan de gegevensverwerking te ontvallen. Het is in dat geval aan de verantwoordelijke niet toegestaan om alsnog op grond van art. 8 sub b tot verwerking van persoonsgegevens over te gaan. Dit sluit aan op de norm van artikel 6: verwerking zou dan onbehoorlijk en onzorgvuldig zijn ten opzichte van de betrokkene.

Bij de toepassing van artikel 8 geldt steeds in aanvulling op artikel 8 voor gevoelige gegevens op grond van paragraaf 2 van hoofdstuk 2 een verscherpt regime!

4. Verdere verwerking niet onverenigbaar met doeleinden van verkrijging (artikel 9).
Zie onder 2. Het doel waarvoor de verantwoordelijke de gegevens wil gebruiken, moet worden afgewogen tegen het doel waarvoor de gegevens zijn verkregen. Van belang is bovendien de aard van de betreffende gegevens. Gegevens kunnen bijvoorbeeld gevoelig zijn door de context waarin zij worden gebruikt (bv. Gegevens omtrent iemands kredietwaardigheid of welstand). Hoe gevoeliger het gegeven, hoe minder snel mag worden aangenomen dat sprake is van verenigbaar gebruik indien bij enige verwerking wordt afgeweken van het oorspronkelijke doel.

(vb: de gemeentelijke basisadministratie bevat persoonsgegevens voor veel verschillende doeleinden. Het gaat echter om gegevens die personen identificeren en hun adres vastleggen. Omdat de gegevens weinig informatie bevatten, is het gebruik voor uiteenlopende doeleinden gerechtvaardigd. In beginsel zijn de gegevens bestemd voor de overheid. Wanneer daarentegen een ziekenfonds op basis van de gegevens van de declaraties van een specialist een selectie maakt van patiënten die aan een bepaalde kwaal lijden en deze lijst ter beschikking stelt aan een fabrikant van hulpmiddelen die het leven met deze kwaal vergemakkelijkt, is er sprake van onverenigbaar gebruik. MvT p. 92).

Het doorgeven van een verjaardag aan bijvoorbeeld een afdeling communicatie voor het maken van een verjaardagskalender op intranet mag (tenzij hier uitdrukkelijk bezwaar tegen gemaakt wordt. Maar het doorgeven van gegevens aan een verzekeraar voor het doen van een aanbieding aan werknemers mag niet!)

5. Kwaliteit gegevens: toereikend, relevant, niet bovenmatig, nauwkeurig (artikel 11).
Persoonsgegevens moeten juist en nauwkeurig zijn, ter zake dienend en niet bovenmatig.
Degene die de gegevens verwerkt heeft een continue verplichting tot toetsing van de gegevens.

6. Beveiliging (artikelen 12, 13 en 14)

Uitgangspunt is dat de verantwoordelijke verantwoordelijk en aansprakelijk is voor de gegevensverwerking. In het tweede lid van artikel 12 wordt een geheimhoudingsplicht opgelegd aan de bewerker, alsmede degenen die onder het gezag van de verantwoordelijke of de bewerker werkzaam zijn. In beginsel kan slechts een uitdrukkelijke wettelijke verplichting op de geheimhoudingsplicht een inbreuk maken.

In artikel 13 is een beveiligingsverplichting vastgelegd: De verantwoordelijke moet passende technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

In artikel 14 is geregeld dat de verantwoordelijkheid voor beveiligingsmaatregelen ligt bij de verantwoordelijke. Ook wanneer de verwerking van persoonsgegevens door een bewerker geschiedt. (zorgplicht verantwoordelijke)

7. Bewaring: niet langer dan noodzakelijk voor verwerkingsdoeleinden (artikel 10).
Gegevens mogen niet te lang worden bewaard. Er moet worden toegezien op de juistheid van de verwerkte gegevens. Bij bewerking van gegevens door een derde is een overeenkomst vereist. Melding bij CBP, tenzij vrijgesteld. (Vrijstellingsbesluit)

In artikel 16 is geregeld dat de verwerking van persoonsgegevens betreffende iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging is verboden behoudens het bepaalde in deze paragraaf (2). Hetzelfde geldt voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

Samengevat:
de **basisprincipes** voor verwerking van persoonsgegevens:
- Zorgvuldigheid;
- Doelbinding;
- Grondslagvereiste;
- Gegevenskwaliteit;
- Beveiliging en bewaring;
- Transparantie;
- Verscherpt regime voor bijzondere persoonsgegevens;
- Procedurevoorschriften;
- Melding bij CBP;
- Exportvergunning bij justitie.

Doel:
Bescherming van de persoonlijke levenssfeer. Uitgangspunt daarbij is:
Persoonsgegevens moeten herleidbaar zijn tot een natuurlijk persoon:
Verwerking van persoonsgegevens mag, mits:
- Er sprake is van een duidelijk omschreven en bepaald doel;
- Dat doel moet kenbaar en gerechtvaardigd zijn;
- Gerechtvaardigde verwerking vereist grondslag: ondubbelzinnige toestemming van de betrokkene, uitvoering van een overeenkomst of wettelijke verplichting; of noodzakelijk voor het gerechtvaardigd belang van de verwerker (bijv. historisch overzicht van het personeel)

Informatieverplichting: De verantwoordelijke is verplicht om vooraf te informeren over identiteit en over het doel van de verwerking van gegevens.
Andere gegevens: afhankelijk van de aard van gegevens, omstandigheden verkrijging en gebruik van gegevens.
Praktijk: Privacy reglementering kenbaar maken, bijvoorbeeld via uitleg op intranet.

Rechten betrokkene:
Inzage (binnen 4 weken een volledig overzicht);
Correctie: verbetering, aanvulling, verwijdering, afscherming (binnen 4 weken beslissen op verzoek).
Derden aan wie gegevens zijn doorgegeven informeren.
Een betrokkene kan zich verzetten, grondslag voor verzet moet zijn: ‘gerechtvaardigd belang’ tegen commercieel gebruik.

Sancties Wbp:

Boete € 4.500,-- op schending meldingsplicht. Dwangsommen, bestuursdwang. Betrokkene neemt individueel of collectief actie: Hij kan bijv. reputatieschade claimen. CBP zoekt publiciteit bij handhaving..

Transparantie vooraf is van groot belang.

Medezeggenschapsrecht:
De ondernemingsraad heeft instemmingsrecht op het (vast te stellen) privacy beleid. Het privacy beleid zou een regeling moeten omvatten over het verwerken van, alsmede de bescherming van persoonsgegevens van de in de onderneming (of rechtspersoon) werkende personen. (art. 27 lid 1 WOR)
Volg/controle/registratiesysteem 'een regeling inzake voorzieningen die gericht zijn op, of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen'.

Wet openbaarheid van bestuur (Wob) in relatie tot de Wet bescherming persoonsgegevens;
De Wob kent als hoofdregel dat overheidsinformatie openbaar is. In artikel 8, lid 1 Wob is het beginsel van actieve openbaarmaking neergelegd. Dat wil zeggen het uit eigen beweging verstrekken van informatie door het bestuursorgaan. De plicht tot het verstrekken van informatie ontstaat zodra dit in het belang is van een goede en democratische bestuursvoering. Soms geeft ook een bijzondere wet aan, dat informatie openbaar gemaakt moet worden. Er moet altijd een belangenafweging plaats vinden. De overheid moet er voor zorgen dat ook bij actieve openbaarmaking een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer wordt vermeden of zo beperkt mogelijk wordt gehouden. De Wob geeft immers als weigeringsgrond voor openbaarmaking de bescherming van de persoonlijke levenssfeer. Het is geen absolute weigeringsgrond, maar er moet een belangenafweging plaatsvinden (belang openbaarheid versus belang bescherming persoonlijke levenssfeer).
Indien privacygevoelige gegevens actief openbaar worden gemaakt, geldt dat toestemming van de betrokkene nodig is, of dat er een aantoonbare noodzaak is voor de openbaarmaking, zoals nakoming van een wettelijke verplichting.

Zowel het recht op 'openbaarheid' als het recht op 'eerbiediging van de persoonlijke levenssfeer' zijn grondrechten. Er treedt een spanning op als gevraagd wordt om openbaarmaking van gegevens die de persoonlijke levenssfeer betreffen. De vraag rijst: welk recht gaat voor?
Beide rechten zijn nevenschikkend. 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 openbaarmaking aan de andere kant het belang van de persoonlijke levenssfeer van de betrokkene.

Factoren die behulpzaam kunnen zijn bij de afweging van belangen zijn de volgende. Het stramien van artikel 8 EVRM kan worden gevolgd:
1. Is sprake van een persoonsgegeven?
2. Is sprake van een inbreuk op een persoonsgegeven?
3. Is deze inbreuk bij wet voorzien?
4. Is deze inbreuk te rechtvaardigen vanuit een legitiem doel?
5. Is deze inbreuk noodzakelijk in een democratische samenleving? Daarbij kan worden gelet op de volgende factoren (niet limitatief):

a. de aard van de gegevens waarvan openbaarmaking wordt gevraagd;
b. b.de gevolgen van de beoogde verwerking voor de betrokkene wiens gegevens openbaar gemaakt zouden moeten worden;
c. de wijze waarop de gegevens van de betrokkene zijn verkregen

De Wob bepaalt het recht van een ieder (burgers, bedrijfsleven) 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 over persoonlijke levenssfeer.
De ene is een absolute weigeringsgrond. Het bestuursorgaan is gehouden geen gegevens openbaar te maken die betreffen 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. Dat betreft het afwegen van twee belangen: Het belang van 16,7 miljoen Nederlanders om iets te weten over één persoon versus het belang van de betrokkene om met rust te worden gelaten
Het gaat om een afweging van belangen. Het bestuursorgaan weegt die belangen af. Daarbij heeft het een grote vrijheid.

In artikel 10, tweede lid, aanhef en onder e, komt een zgn. relatieve weigeringsgrond voor. Dat artikellid luidt:
2. 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;
Het verschil tussen een absolute weigeringsgrond en een relatieve weigeringsgrond is:
- 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. 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 bestuursvoering (dat wordt voorondersteld aanwezig te zijn) en aan de andere kant het privacybelang van de betrokkene. In zo'n geval moet dus een motivering volgen. Dat vereist een kwaliteitstoets.

Er is dus geen belangenafweging bij absolute weigeringsgrond, wel bij een relatieve weigeringsgrond.

Het is aan het bestuursorgaan om die belangenafweging te maken en aan de rechter om haar te toetsen, met inachtneming van het uitgangspunt van de Wob dat openbaarheid regel is.

Wetsvoorstel 33 662: Meldplicht datalekken

1. Strekking van het wetsvoorstel In dit wetsvoorstel wordt een meldplicht geïntroduceerd in de Wet bescherming persoonsgegevens (hierna: Wbp) voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. De verantwoordelijke moet op grond van het voorgestelde artikel 34a van de Wbp bij een inbreuk waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens een melding doen bij de toezichthouder, het College bescherming persoonsgegevens (hierna: Cbp). Daarnaast dient in de meeste gevallen een melding aan de betrokkene te geschieden indien de inbreuk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. De meldplicht rust op alle verantwoordelijken voor de verwerking, zowel in de private als publieke sector. Het nalaten aan deze verplichtingen te voldoen kan worden gesanctioneerd met een bestuurlijke boete, op te leggen door het Cbp. Het doel van de meldplicht is het voorkomen van datalekken ten gevolge van doorbreking van beveiligingsmaatregelen en als deze zich toch voordoen, de gevolgen ervan voor de betrokkenen zoveel mogelijk te beperken. Met de meldplicht wordt bijgedragen aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens.

Sancties:
- Huidige boete omhoog naar 4e categorie art. 23 Sr (€ 20.250)
- Nieuwe boete voor meeste andere belangrijke Wbp verplichtingen:
- 6e categorie art. 23 Sr (€ 810.000)
- Flexibilisering: boete kan worden verhoogd naar 10 % omzet
- Eerst bindende aanwijzing (behalve bij opzet)
- die vatbaar is voor bezwaar en beroep
- Nieuwe hoge boetes gelden niet bij CBP-toezicht Wet politiegegevens, Wet justitiële en strafvorderlijke gegevens of Wet basisregistratie personen

Awb (H 5) Privacy en handhaving:
Het college bescherming persoonsgegevens houdt toezicht op naleving van de Wbp.
Mogelijke overtredingen van de Wbp:
(Bijlage 1.1)• Bij verwerking ex art. 8 (a): toestemming voldoet niet;
• Overmatige gegevensverwerking, opslag;
• Gegevens die te lang worden bewaard;
• Verwerking van gevoelige gegevens;
• Ontoereikende beveiliging/geen bewerkerscontracten;
• Doorgifte naar een land buiten de EU/EEA zonder modelcontract of uitdrukkelijke toestemming.

(Voornaamste kritiek: Normen zijn te algemeen om daar boetes op los te laten.)
Toezichtsbevoegdheden volgen uit H. 5 van de Awb:
Denk aan: vorderen van inlichtingen (5:16 Awb , 18:7 Tw)
Betreden van plaatsen (5:15 Awb)
Vorderen van inzage van zakelijke gegevens en bescheiden en kopieën.
Medewerkingsplicht(5:20 Awb)

Sancties CBP: bestuursdwang (op basis van art. 65 Wbp), Last onder dwangsom (5:32 Awb).
Bestuursrechtelijke boete:
€ 4.500 bij: niet (tijdige) melding, niet actualiseren van een melding, export naar (verboden) land.

N.B.: Wetsvoorstel meldplicht datalekken voorziet in hogere boetes en de Europese verordening in nog hogere boetes.

De nieuwe Privacy Verordening.
De nieuwe Privacy verordening gaat de thans geldende Richtlijn 95/46/EG en de Richtlijn verwerking Justitiële en Politiegegevens vervangen. De nieuwe verordening zal directe werking gaan krijgen. De nieuwe verordening lijkt te zijn ingegeven door internet en social media vraagstukken.

In de nieuwe verordening zal "Accountability", ofwel verantwoording en transparantie overgaan van impliciete voorwaarde naar een expliciete eis!
Nieuw is vooral dat de Europese verordening torenhoge sancties kent ook voor milde vergrijpen.
Daarnaast worden aan de toezichthouder en de Commissie zwaardere bevoegdheden toegekend.

Accountability
- Documentatie bijhouden (artikel 28)
- Passende veiligheidsmaatregelen treffen (artikel 30)
- Data protection impact assessment (artikel 33) PIA Privacy impact assessment wordt verplicht.
- Data protection officer aanstellen (artikel 35) (Niet alleen een functie in naam. Dit gaat voor alle overheden gelden!): moet gaan om een externe privacy officer.

Overige (governance) eisen
- Meldplicht datalekken (artikel 31 & 32)
- Privacy by design & by default (artikel 23)

Risico's inschatten met PIA (beveiliging, authorisatie en business practices.)
Privacy compiance check: welke gegevens, doelen en hoe die te verklaeinen.

Rechten van betrokkenen
- Informatieverstrekking in duidelijke taal (artikel 11)
- Recht om 'vergeten' te worden (artikel 17)
- Recht op dataportabiliteit (artikel 18)

Aansprakelijkheid & sancties
- Artikel 73: Actiegroepen worden indirect 'belanghebbende'
- Artikel 77: Recht op schadevergoeding
- Artikel 79: Administratieve boetes

Artikel 79 (boetes):
Algemene eisen gegevensverwerking
Rechten betrokkene
accountability eisen
- Niet hebben van een duidelijk privacybeleid = tot 1M of 2% van de jaaromzet
- Niet hebben van afspraken bij samenwerking = tot 500K of 1% van de jaaromzet
- Geen beveiligingsbeleid = tot 1M of 2% van de jaaromzet
- Geen beleid voor privacy by design & privacy by default = tot 1M of 2% van de jaaromzet
- Niet doen van Privacy Impact Assessments = tot 1M of 2% van de jaaromzet
- Niet melden van datalekken = tot 500k of 1% van de jaaromzet

De verordening gaat een grote impact hebben op de verwerking van persoonsgegevens;
Politiek zeer omstreden en nog steeds onzeker dossier
Wetgevend proces kan nog lang duren. (mogelijk iwt in 2018)
Maar bewustzijn en voorbereiding is noodzakelijk