

## **WATERSCHAPPEN EN DE INVOERING VAN DE WET BESCHERMING PERSOONSgegevens**

*Privacy en privacybescherming is in ons land een groot goed. Een 'goed' waar we als het nodig is voor willen vechten en dat regelmatig naar aanleiding van ontwikkelingen of incidenten hoog op de agenda staat van de politiek, bestuur en uitvoering.*

*Toch is er weinig belangstelling te merken voor de nieuwe Wet Bescherming Persoonsgegevens (WBP). De WBP is op 6 juli 2000 in het Staatsblad verschenen en is op 1 september 2001 in werking getreden. Het 'going concern' vergt meer energie om je bezig te houden met iets als de WBP. Toch is er sprake van een groot afbreukrisico zeker met de toenemende ICT-ontwikkelingen.*

*De geringe belangstelling is niet terecht. De WBP biedt bij uitstek het handvat om de zo belangrijke privacy en privacybescherming in ons land te waarborgen. Om organisaties te helpen bij de invoering van de WBP heeft de Registratiekamer (tegenwoordig College Bescherming Persoonsgegevens geheten) samen met diverse organisaties een aantal instrumenten ontwikkeld.*

### **Algemene inleiding**

Op 6 juli 2000 verscheen de Wet Bescherming Persoonsgegevens (WBP) in het Staatsblad (nr. 302). De WBP vervangt de Wet op de Persoonsregistraties (WPR) en is op 1 september 2001 in werking getreden.

Privacy en de regelgeving daaromtrent is voor organisaties altijd een lastig onderwerp geweest. 'Iets voor juristen' en 'we hebben het te druk met ons dagelijks werk' zijn dan de opmerkingen die worden geuit als iemand aandacht vraagt voor dit probleem.

Terecht? Nee natuurlijk niet want als het om onze eigen gegevens gaat zijn we een stuk kritischer. Alhoewel: bij menig supermarkt geven we graag onze persoonsgegevens prijs om in aanmerking te komen voor extra kortingen. Met de ontwikkelingen van de huidige Informatie-Communicatie-Technologie is het echter steeds meer mogelijk om persoonsgegevens vanuit verschillende bronnen met elkaar te combineren.

Deze ontwikkelingen kennen een prijs te weten onze privacy en de bescherming van onze persoonlijke levensvrijheid. En het is zaak hier aandacht te hebben voor een juiste bescherming van deze inperking van onze privacy.

Voor overheidsorganisaties waar de persoonsgegevens van alle Nederlanders worden verwerkt geldt dit des te meer. Zeker met gegevens over inkomsten, de WOZ waarde, belasting gegevens, etc moet extra goed worden omgegaan. Maar ook bij overheidsorganisaties is het moeilijk het onderwerp privacy goed op de agenda te krijgen. De Wet op de Persoonsregistraties werd mede door de reglementplicht vooral gezien als iets van en voor juristen. De Wet Bescherming Persoonsgegevens vraagt echter iets anders van organisaties. Niet meer het reglement maar de verwerking staat centraal oftewel wat doet u als waterschap met de persoonsgegevens.

In dit artikel gaan wij allereerst in op de Wet Bescherming Persoonsgegevens zelf. Kort wordt aangestipt waar de belangrijkste wijzigingen in zijn terug te vinden en waarom de WPR (toch niet erg oud) moest worden vervangen. Vervolgens gaat wij in op de wijze waarop het College Bescherming Persoonsgegevens de invoering van de WBP extra wil stimuleren.

*De WBP kent zeker een overlap ten opzichte van de huidige Wet Persoonsregistraties doch ook een aantal nieuwe zaken. Van belang is meer de gewijzigde benadering. Niet de 'registratie' maar de 'verwerking' van gegevens is het uitgangspunt. Maak dit transparant en hou de rechten van betrokkenen goed in de gaten. Bescherm de gegevens goed. Dit is de centrale boodschap van de WBP.*

### **De Wet Bescherming Persoonsgegevens**

De WBP is het gevolg van Europese regelgeving waarbij regels rond privacybescherming binnen de EU op elkaar worden afgestemd. De meeste veranderingen vallen op zich ook wel mee en betreffen met name een verandering in terminologie.

Wat wel een fundamentele wijziging in de wet is geweest is de benadering van persoonsregistraties. Onder de WPR was de registratie van belang en het (althans voor overheidsinstellingen) hebben van een privacyreglement. Deze verplichting komt te vervallen. Hiervoor in de plaats komt echter een meldingsplicht voor in beginsel iedere geautomatiseerde verwerking van persoonsgegevens.

Overigens: een persoonsgegeven is ieder op een individu herleidbaar gegeven (dus ook bijv. foto's en videobanden van beveiligingscamera's waar individuen op staan).

De WBP benadert de registraties vanuit het begrip 'verwerking'. De wet spreekt over begrippen als verantwoordelijke, bewerker, gebruiker, etc. Ook moeten verwerkingen van persoonsgegevens worden gemeld bij de Registratiekamer te Den Haag (straks College Bescherming Persoonsgegevens) of een apart te benoemen privacyfunctionaris voordat zij in gebruik worden genomen. Wel komt er nog een vrijstellingsbesluit waarin een aantal registraties word vrijgesteld van melding.

De WBP laat gegevensverwerkingen alleen toe voor een 6-tal limitatief in de wet genoemde situaties. Wanneer minimaal één van onderstaande situaties van toepassing is, is geautomatiseerde gegevensverwerking toegestaan:

- ondubbelzinnige toestemming van de betrokkene
- noodzakelijk voor de uitvoering van een overeenkomst
- noodzakelijk om een wettelijke verplichting na te komen
- ter vrijwaring van een vitaal belang van betrokkene
- voor de goede vervulling van een publiekrechtelijke taak
- voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke tenzij de rechten en vrijheden van de betrokkene (in het bijzonder recht op bescherming van de persoonlijke levenssfeer) prevaleert.

Verder zijn verschillende rechten zoals het recht van verzet aangescherpt en gelden voor gegevens ook bewaartermijnen.

Explicieeter dan in de WPR wordt aandacht besteed aan de beveiliging van de persoonsgegevens.

*De komst van de WBP is een goed moment om stil te staan bij de aandacht voor privacy binnen organisaties. Maar hoe doe je dit? Hiervoor heeft het College Bescherming Persoonsgegevens in samenwerking met tal van organisaties een 'audit aanpak' ontwikkeld met een drietal producten te weten de Quick Scan, de Zelfevaluatie en de Privacy Audit. Hieronder een uiteenzetting.*

### **Meer aandacht voor privacy**

Om het privacyvraagstuk en de nieuwe regelgeving meer onder de aandacht te krijgen heeft het College Bescherming Persoonsgegevens de zogenaamde 'audit aanpak' opgepakt.

Vanaf januari 2000 is in een samenwerkingsverband onder regie van de Registratiekamer gewerkt aan de ontwikkeling van een 'audit aanpak' voor de invoering van de WBP.

Bureaus met diverse achtergronden (EDP, Juridisch, Organisatieadvies, RA, etc.) hebben aan een drietal producten die voor organisaties in Nederland behulpzaam moeten zijn bij de invoering van de WBP gewerkt. Binnen deze audit-aanpak zijn de volgende producten samengesteld:

#### Quick-scan

Als u vindt dat personeelsleden, belastingplichtigen, ingelanden, debiteuren, bezoekers en andere relaties vertrouwen moeten hebben in uw organisatie dan moet uw waterschap dat vertrouwen verdienen en vervolgens waarmaken. Een zorgvuldige verwerking van persoonsgegevens draagt bij aan dit vertrouwen. Het is daarom belangrijk vast te stellen hoe uw waterschap persoonsgegevens verwerkt. Een eerste stap hierbij is het creëren van voldoende bewustzijn over het belang van de zorgvuldige omgang met persoonsgegevens binnen uw waterschap.

Om het proces van bewustzijn te stimuleren, is een korte privacyvragenlijst opgesteld. De uitkomsten van deze vragenlijst geven een globale indruk hoe het met de privacybescherming binnen uw waterschap is gesteld.

De Quick-scan bevat een 13-tal vragen, is beknopt en gaat niet in op alle aspecten van de bescherming van persoonsgegevens, zoals die in de WBP zijn gesteld.

De QS kan breed verspreid worden en is eenvoudig in te vullen; ook door leken. De vragen die aan de orde komen betreffen de volgende onderwerpen:

- privacybewustzijn in de waterschap (voorlichting over de WBP, uitspraken directie of leiding, aandacht voor privacybescherming binnen de waterschap)
- uitvoering wettelijke bepalingen (doelbinding, rechtmatige grondslag, regels over de verwerking van persoonsgegevens, hoe wordt omgegaan met bijzondere persoonsgegevens, controle op juistheid en volledigheid)
- beveiliging (autorisaties, verlies en onrechtmatige verwerking)
- controle (op naleving maatregelen privacybescherming)

#### Zelfevaluatie

Met een scheef oog kijkend naar het INK-model is een Zelfevaluatie-instrument ontwikkeld waarbij aan de hand van een 14-tal hoofdvragen (en een veelvoud aan subvragen) de WBP wordt doorgenomen en waarin d.m.v. een soort score in 5 fasen in beeld wordt gebracht waar een waterschap zich bevindt ten aanzien van privacybescherming en welke verbeteracties te plegen zijn.

De hoofdthema's betreffen:

- de melding
- transparantie van gegevens
- doelbinding
- rechtmatige grondslag
- kwaliteit
- rechten van betrokkenen
- beveiliging:
  - bewustzijn
  - IT-voorzieningen
  - toegangsbeveiliging
  - netwerken
  - bewaren en vernietiging
  - calamiteitenplan
- bewerker (bijvoorbeeld het nutsbedrijf waarmee u meelift)
- niet EU-landen (indien van toepassing)

Door de uitvoering van een Zelfevaluatie op te pakken binnen een waterschap kan niet alleen een goed beeld worden verkregen van de stand van zaken maar wordt tevens een 'bewustwordingsslag' binnen het waterschap gemaakt. Uit testen met het instrument kwam ook naar voren dat het uitvoeren van een zelfevaluatie ook een leuke manier is om kennis over te dragen.

#### Privacy-audit

De Privacy-audit is een instrument waarbij een bedrijf of instelling zich kan laten certificeren. Het voldoen aan de eisen van de privacy audit betekent dat een waterschap voldoet aan de richtlijnen van de WBP.

De inhoudelijke beoordeling bij een PA sluit aan bij die van de Zelfevaluatie. Dezelfde onderwerpen komen bij de bepaling van de verwerkingseisen voor persoonsgegevens terug. De diepgang is echter verder en ook wordt nadrukkelijk gekeken naar de zgn. managementcyclus in dit geheel (met dus een relatie naar bedrijfsdoelstellingen, organisatie van verwerking, de verwerking zelf en de evaluatie van de verwerking). Verder wordt bij de PA ook gekeken naar de risicoanalyse.

Op dit moment is het instrument van de audit nog niet zover doorontwikkeld dat certificering mogelijk is.

In de instrumenten Zelfevaluatie en Privacy-audit wordt veel aandacht besteed aan de beveiliging van persoonsgegevens. De richtlijnen hiervoor komen rechtstreeks uit de Code voor Informatiebeveiliging (een internationale standaard voor IT-beveiliging).

De drie genoemde producten zijn gereed voor gebruik en zijn ook getest. De Zelfevaluatie is b.v. getest bij een ministerie, een direct marketingbedrijf, een arbo-dienst, een psychiatrisch ziekenhuis maar ook bij de Staatsloterij en de Stichting Toezicht Effectenverkeer.

Exemplaren van deze instrumenten zijn vrij toegankelijk via de website van het College Bescherming Persoonsgegevens([www.cbppwep.nl](http://www.cbppwep.nl)). Een aanrader voor een ieder die meer wil weten over deze instrumenten en de werken ervan.

#### **De Wbp en Waterschappen**

Waterschappen beschikken over veel persoonsgegevens. Gezamenlijk in ieder geval van alle Nederlandse huishoudens.

De gegevens ontvangen zij van gemeenten (als afnemer GBA en vanuit de WOZ-administratie) met daarbij tevens gegevens als het zgn. A-nummer en het soft-nummer en vanuit het kadaster.

De verwerking van deze gegevens geschiedt op grond van de publiekrechtelijke taak die Waterschappen hebben en is gestoeld op de Waterschapswet.

De Wbp brengt echter met zich mee dat Waterschappen een aantal zaken moeten regelen. Hieronder een overzicht van de meest essentiële zaken:

- Meldingen

Nagegaan moet worden welke verwerkingen onder de meldingsplicht (artikel 27 Wbp) vallen en welke hiervan zijn vrijgesteld. Overigens, op grond van artikel 30 lid 3 Wbp dient ook voor de vrijgestelde meldingen een overzicht te worden opgesteld.

Vervolgens dienen verwerkingen die gemeld moeten worden ook daadwerkelijk gemeld te worden. Hiervoor geldt voor huidige verwerkingen een overgangstermijn tot 1 september 2002.

- Rechten van betrokkenen

De rechten van betrokkenen zijn gewijzigd. Er is niet alleen een recht van inzage maar ook een recht op correctie en een recht op verzet (absoluut en relatief). Een en ander uiteraard met uitzonderingen en bijzonderheden.

Het is goed hier kennis van te nemen en procedures aan te passen dan wel vast te stellen.

Nieuw ten opzichte van de Wet Persoonsregistraties is bijvoorbeeld dat een besluit inzake het al dan niet inwilligen van een verzoek van een burger een voor bezwaar en beroep vatbare beslissing is inzake de Algemene Wet Bestuursrecht.

- **Transparantie**

Meer dan voorheen hebben Waterschappen de plicht om de ingelanden te laten weten welke gegevens waarom worden verwerkt en aan wie ze worden doorgegeven. Dit betekent aanpassing van foldermateriaal of aanpassing van bijlagen bij bijvoorbeeld aanslagbiljetten, brieven e.d.

- **Bewaartermijnen**

De Wbp schrijft voor dat bepaald moet zijn hoelang persoonsgegevens bewaard mogen worden. Dit moet geregeld zijn.

- **Beveiliging**

Artikel 13 van de Wbp gaat in op de beveiliging van persoonsgegevens. De verantwoordelijke heeft de verplichting om passende technische en organisatorische maatregelen ten uitvoer te leggen 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 gegevens te voorkomen.

Om dit te concretiseren en te vertalen naar de eigen situatie toe zijn er diverse hulpmiddelen. De eerder genoemde Zelfevaluatie gaat op een groot aantal onderdelen van de beveiliging in maar zeker ook een aanrader is een uitgave van (toen nog) de Registratiekamer. Het betreft hier nr. 23 van de Achtergrondstudies en Verkenningen dat specifiek ingaat op het onderwerp 'Beveiliging van persoonsgegevens'. Aan de hand van eenvoudige criteria kan per gegevensverwerking de relevantie risicoklasse worden bepaald en de bijbehorende aanbevolen beveiligingsmaatregelen.

Ook dit document kunt u eenvoudig raadplegen in downloaden via internet ([www.cbpwep.nl](http://www.cbpwep.nl)).

### **Bewerker**

Een apart onderdeel waar we hier op in willen gaan is de positie van de bewerker. Een bewerker is volgens de Wbp degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen (artikel 1 onder e).

De begripsinhoud is losgekoppeld van de middelen waarmee de verwerking wordt gevoerd.

De bewerker verwerkt gegevens voor de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder dienst (uitdrukkelijke) verantwoordelijkheid. Bepalend voor de afbakening van het begrip is de relatie met de verantwoordelijke voor de gegevensverwerking en de mate van zeggenschap waarmee de verwerking van persoonsgegevens gepaard gaat. De bewerker is allereerst een buiten de organisatie van de verantwoordelijke staande persoon of instelling.

De verantwoordelijke die gegevens buiten zijn rechtstreeks gezag verwerkt wil hebben is op grond van artikel 14, tweede lid, verplicht een overeenkomst met de bewerker aan te gaan.

Daarnaast beperkt de bewerker zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van de persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens et cetera. Zou hij immers deze zeggenschap wel verwerven dan dient hij als verantwoordelijke te worden opgemerkt.

Veel Waterschappen maken voor de invordering van hun heffingen gebruik van bewerkers. Veel waterschappen liften immers mee via nutsbedrijven (Waterleidingsbedrijven en/of Elektriciteitsbedrijven). Op zich is hier niets mis mee. Echter hier dienen dus deugdelijke overeenkomsten aan ten grondslag te liggen. Artikel 14 van de Wbp zegt hierover:

Lid 1:

“Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.”

Lid 2:

“De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.”

In lid 3 van dit artikel wordt nog eens extra ingegaan op onder andere de verplichting om zorg te dragen voor de zgn. geheimhoudingsplicht van artikel 12.

Waterschappen zullen met name met deze artikelen rond de bewerker te maken krijgen van eventuele herziening van de huidige contracten. Zij zullen moeten nagaan hoe door de bewerker gewaarborgd wordt dat de persoonsgegevens die zij beschikbaar stellen niet voor andere doeleinden worden gebruikt, hoe wordt omgegaan met de beveiligingsaspecten, het toezien hierop en hoe de geheimhoudingsplicht bij de bewerker wordt gewaarborgd. Een en ander laat onverlet dat waterschappen voor wat betreft hun eigen gegevensverwerkingen eveneens sterk wordt aangeraden z.s.m. met name een zelfevaluatie uit te voeren. De tijd begint immers te dringen.

*De auteurs:*

*Auteurs van dit artikel zijn de heren drs. W. de Vries en drs. M.B.H. Ijpelaar CISA. Beiden zijn senioradviseur bij Bestuur & Management Consultants te Leusden.*

*Dhr. De Vries is direct betrokken geweest bij de ontwikkeling van het instrument Zelfevaluatie en bij de implementatie van de Wbp bij diverse organisaties. Dhr. Ijpelaar is als beveiligingsdeskundige betrokken bij diverse projecten bij de lokale overheid.*