Wet bescherming persoons-gegevens: continuïteit en verandering

Mr. P.J. Hustinx

De Wet bescherming persoonsgegevens is een logisch vervolg op de Wet persoonsregistraties. Juridisch-technisch is het belangrijkst bij deze opvolging de overgang van 'persoonsregistratie' naar 'verwerking van persoonsgegevens'.

Inleiding

Op 1 september 2001 is de Wet bescherming persoonsgegevens in werking getreden. Op die datum verviel de Wet persoonsregistraties die sinds 1989 in werking is geweest. Met deze overgang sluit Nederland zich met enkele jaren vertraging aan bij de EU-lidstaten die uitvoering hebben gegeven aan de EG Richtlijn 95/46, die ook wel bekend staat als de 'privacy-richtlijn'. In alle landen om ons heen is de afgelopen jaren een stelsel van wettelijke regels ontwikkeld voor de verwerking van persoonsgegevens in computersystemen en conventionele bestanden. In onze samenleving neemt die verwerking een steeds belangrijker plaats in. Daarom moet ervoor worden gezorgd dat de grondrechten van de burger ook in deze omgeving gewaarborgd blijven. Bij de bescherming van persoonsgegevens gaat het overigens niet alleen om privacy, maar om behoorlijke en zorgvuldige verwerking van persoonsgegevens in het algemeen. De bedoelde richtlijn geeft aan hoe die bescherming in alle EU-lidstaten op hoofdlijnen moet zijn ingericht. Daarbij ging het tevens om het scheppen van een vrije ruimte waarin het verkeer van persoonsgegevens zich volgens dezelfde regels kan voltrekken. Het bevorderen van een evenwichtige ontwikkeling van diensten en producten in de informatiesamenleving stond daarbij mede voorop.

Van Wpr naar Wbp

De invoering van een nieuwe wet is in de regel geen sinecure en dat is nu niet anders. Maar toch is het goed om duidelijk voor ogen te houden dat er inhoudelijk sprake is van een grote continuïteit tussen Wpr en Wbp. Beide stammen immers uit hetzelfde gedachtegoed, dat teruggaat tot het Dataprotectieverdrag van de Raad van Europa, waarbij inmiddels meer dan twintig landen binnen en buiten de EU partij zijn. Ook de EG-richtlijn sluit daarbij aan. Dat neemt niet weg dat er ook belangrijke veranderingen zijn, zowel juridisch-technisch als meer inhoudelijk. Deze laatste leiden deels tot vermindering van administratieve lasten, deels tot aanscherping van rechten en verplichtingen en de handhaving daarvan. Er is dus aanleiding om attent te zijn op de consequenties van dit geheel voor organisaties.

Juridisch-technisch veruit het belangrijkst is de overgang van 'persoonsregistratie' naar 'verwerking van persoonsgegevens'. Dit past bij de dynamiek van de informatiesamenleving, maar heeft als consequentie dat de wettelijke regeling nu ook veel dieper binnendringt in de processen van die samenleving. Voorbeelden van inhoudelijke aanscherpingen zijn de nadruk op informatieverstrekking aan betrokkenen ('transparantie'), de invoering van een recht van bezwaar ('verzet') en de uitbreiding van bevoegdheden voor de toezichthouder, voortaan het College bescherming persoonsgegevens (CBP) geheten, die in bepaalde gevallen boetes zal kunnen opleggen of bestuursdwang zal kunnen toepassen. Daar staat tegenover dat de verplichtingen tot aanmelding bij de toezichthouder zijn beperkt en dat er ook in de nieuwe wet grote nadruk wordt gelegd op zelfregulering en kwaliteitszorg met inachtneming van de wettelijke kaders. Kortom, de overgang van Wpr naar Wbp geeft een beeld te zien van veel continuïteit, maar ook van enkele opvallende veranderingen.

Reikwijdte en begrippen

Het begrip persoonsgegeven ondergaat inhoudelijk geen wijziging. De omschrijving wordt wel duidelijker: 'elk gegeven over een identificeerbare natuurlijke persoon'. De vorm van dat gegeven doet niet terzake, ook videobeelden kunnen bijvoorbeeld persoonsgegevens bevatten. De identificeerbaarheid is in de meeste gevallen geen probleem, al kan deze in grensgevallen tot een lastige beoordeling leiden. Inhoudelijk is van belang dat alle gegevens die informatie verschaffen over een individu, of die medebepalend zijn voor de wijze waarop die persoon in het maatschappelijk verkeer wordt beoordeeld of behandeld, kunnen worden aangemerkt als 'persoonsgegevens' in de zin van de wet.

De Wbp heeft betrekking op alle verwerkingen van persoonsgegevens die geheel of ten dele langs geautomatiseerde weg plaatsvinden, maar ook op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De term bestand slaat hier op elk gestructureerd geheel van persoonsgegevens, dus eigenlijk een handmatig gevoerde persoonsregistratie onder de Wpr. De reikwijdte van de wet blijft in zoverre dus gelijk. De term verwerking omvat echter wel alle handelingen en elk geheel van handelingen, die men met betrekking tot persoonsgegevens kan verrichten. In feite alles tussen het verzamelen en het vernietigen van die gegevens. Zoals gezegd leidt dat ertoe dat de wet eerder ingrijpt – namelijk reeds bij en zelfs voorafgaand aan het verzamelen van persoonsgegevens – en alle mogelijke verwerkingsprocessen op de voet volgt. Ook het genereren van informatie over identificeerbare personen als onderdeel van een proces wordt aldus aangemerkt als het verzamelen van persoonsgegevens.

De Wbp richt zich primair tot de 'verantwoordelijke': degene die bevoegd is om te bepalen voor welk doel en met welke middelen persoonsgegevens worden verwerkt. In de praktijk zal dat vaak een rechtspersoon zijn – zoals een BV of een stichting – en bij de overheid meestal een bestuursorgaan. De personen die optreden, doen dat dan namens de verantwoordelijke. De handelingen van werknemers worden hierbij dus toegerekend aan hun werkgever. De Wbp kent daarnaast ook de bewerker: degene die ten behoeve van de verantwoordelijke verwerkt, maar niet aan zijn rechtstreeks gezag is onderworpen. Dit zal zich vaak voordoen bij allerlei vormen van uitbesteding. Deze bewerkers zijn extern aansprakelijk voor hun eigen aandeel in de verwerking van persoonsgegevens, maar moeten zich overigens geheel gedragen volgens de aanwijzingen van de verantwoordelijke.

Verdere verwerking van persoonsgegevens moet verenigbaar zijn met het doel waarvoor deze gegevens zijn verkregen.

De Wbp geldt evenals de Wpr voor bijna alle maatschappelijke gebieden. Voor bepaalde terreinen zijn echter bijzondere wetten vastgesteld, zoals de Wet GBA voor de gemeentelijke bevolkingsadministratie. Vaak zal de Wbp echter in samenhang moeten worden gezien met andere wetten, zoals de Algemene bijstandswet voor de gemeentelijke sociale diensten en de gezondheidswetgeving in de medische sector. Die samenhang is bewust bedoeld: men moet er dus op bedacht zijn dat veel open begrippen van de Wbp hun invulling krijgen vanuit die ruimere context. Ook onderliggende contracten kunnen zo van belang zijn, met name in de sfeer van de arbeidsverhoudingen of de commerciële dienstverlening. Adviseurs en auditors kunnen hierdoor soms verzeild raken in een complexe wereld!

Algemene normen

De Wbp stelt aan de hiervoor bedoelde verwerkingen een aantal eisen en randvoorwaarden. Voorop staat het principe dat persoonsgegevens alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze mogen worden verwerkt. Dat lijkt vanzelf te spreken, maar dit principe vormt zowel het vangnet voor ongewenste gedragingen die elders in de wet niet expliciet zijn benoemd, als de springplank voor nieuwe ontwikkelingen. In de praktijk zal het vaak gaan om een gebrek aan openheid rond de verwerking van persoonsgegevens. De wet bevat op dit onderdeel trouwens een expliciete verwijzing naar het algemene principe.

Meer in het bijzonder is van belang dat persoonsgegevens alleen voor duidelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld. Of doeleinden gerechtvaardigd zijn, wordt afgemeten aan de uitputtende reeks van gronden voor *rechtmatige* verwerking die de wet noemt, bijvoorbeeld noodzaak voor de uitvoering van een overeenkomst, voor de nakoming van een wettelijke verplichting, of voor de behartiging van een rechtmatig bedrijfsbelang, met dien verstande dat in dit laatste geval de belangen van de betrokkenen daaraan niet in de weg mogen staan. Ook de ondubbelzinnige toestemming van de betrokkene kan de verzameling van persoonsgegevens gerechtvaardigd maken. Na de verzameling van persoonsgegevens moet ook de verdere verwerking daarvan steeds op één of meer van die grondslagen kunnen steunen. Daarnaast geldt echter de beperking dat deze verdere verwerking ook *verenigbaar* moet zijn met het doel waarvoor de persoonsgegevens zijn verkregen. De wet geeft een aantal criteria waarmee die verenigbaarheid kan worden beoordeeld, zoals de verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens verkregen zijn, de aard van de gegevens en de wijze waarop deze verkregen zijn, de gevolgen voor de betrokkene en de waarborgen waarmee de beoogde verwerking omgeven is. Een verdere verwerking moet in elk geval achterwege blijven, als een geheimhoudingsplicht daaraan in de weg staat.

De randvoorwaarden van de rechtmatige grondslag én de verenigbaarheid met het doel van de verkrijging vormen – naast het beginsel van de transparantie waarover later meer – het kader dat bij de verwerking van persoonsgegevens steeds in het oog moet worden gehouden. De wet stelt echter ook eisen aan de kwaliteit van de gegevens – zoals juistheid en relevantie – zodat een systeem van kwaliteitsbewaking nodig is om aan die eisen te voldoen. Daarnaast legt de Wbp bijzondere nadruk op de beveiliging van persoonsgegevens. De verantwoordelijke moet passende maatregelen treffen om persoonsgegevens te beveiligen tegen verlies of tegen elke vorm van onrechtmatige verwerking. Dit laatste is nieuw en heeft grote consequenties voor de inrichting van de beveiliging. De wet zegt daarvan slechts dat het moet gaan om technische of organisatorische maatregelen die een passend beveiligingsniveau bieden – rekening houdend met de stand van de techniek en de kosten van uitvoering – gelet op de risico's die verbonden zijn aan de verwerking en de aard van de gegevens. In de Tweede Kamer is hieraan toegevoegd dat de maatregelen er ook op gericht moeten zijn onnodige verwerking van persoonsgegevens te voorkomen. Dit vormt de expliciete grondslag van de toepassing van Privacy Enhancing Technologies (PET), zoals de Registratiekamer die heeft uitgedragen.

Bijzondere gegevens

Voor bepaalde soorten gegevens gelden nadere beperkingen, die zijn bedoeld als een extra beschermingslaag. Het gaat daarbij om vrijwel dezelfde typen die onder de Wpr als gevoelig zijn aangeduid, zoals gegevens over godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid en strafrechtelijke gegevens. Op Europese schaal is ook het lidmaatschap van een vakvereniging als bijzonder aangemerkt. Het uitgangspunt voor deze gegevens is dat verwerking daarvan verboden is tenzij deze expliciet is toegestaan. Het verdient dus aanbeveling om altijd eerst na te gaan of er een bijzondere verwerkingsgrond voorhanden is voor deze typen gegevens. Zo ja, dan komen de algemene normen als nadere voorwaarden aan de orde. Zo niet, dan is de verwerking niet

toegestaan. In bepaalde gevallen zal het CBP een ontheffing kunnen verlenen op gewichtige gronden van algemeen belang. In de praktijk zal het meestal gaan om gegevens over gezondheid of strafrechtelijk verleden. Ook persoonsnummers, zoals sofi-nummers, worden in de Wbp overigens als bijzondere gegevens aangemerkt.

Rechten van betrokkenen

De rechten van betrokkenen veronderstellen dat zij ten minste op de hoogte zijn van het feit dat gegevens over hen worden verwerkt. Dit principe van openheid of transparantie is in de Wbp uitgewerkt als een zelfstandige voorwaarde voor rechtmatigheid. De verantwoordelijke is verplicht om uit eigen beweging bepaalde informatie te verstrekken, tenzij de betrokkene daarvan reeds op de hoogte is. Als persoonsgegevens worden verzameld bij de betrokkene zelf, moet de verantwoordelijke vooraf ten minste duidelijk aangeven wie hij is en waarvoor de gegevens bestemd zijn. In bepaalde gevallen moet nadere informatie worden verstrekt, als dat nodig is om onjuiste indrukken te vermijden. Anders gezegd: het is onbehoorlijk om de betrokkene 'op het verkeerde been' te zetten of te houden. Als persoonsgegevens op een andere wijze worden verzameld, moet soortgelijke informatie worden verstrekt, maar dan in de regel pas als de gegevens worden vastgelegd. Het is zinnig om de nakoming van deze verplichtingen onder te brengen in een bredere voorlichtingsstrategie, waarbij de benodigde informatie in een eerder stadium wordt verstrekt, zodat betrokkenen reeds op de hoogte zijn en de uitzondering van toepassing wordt. Voorwaarde is wel dat de informatie voldoende duidelijk is: transparantie is immers de norm!

De betrokkenen hebben ook het recht zelf om informatie te vragen over de persoonsgegevens die over hen worden verwerkt, het doel en de herkomst daarvan. Ook hebben zij het recht op verbetering, aanvulling, verwijdering of afscherming van hun gegevens, indien deze onjuist, onvolledig of niet terzake dienend zijn, of onrechtmatig worden verwerkt. De Wbp heeft daar een recht op verzet aan toegevoegd. Dat recht is absoluut – en de verantwoordelijke moet de verwerking dan meteen staken – als betrokkenen bijvoorbeeld bezwaar hebben tegen de verwerking van hun gegevens voor direct marketing. In andere gevallen moet een nadere afweging volgen tussen de belangen van de verantwoordelijke en de bijzondere belangen van de betrokkene. In al deze gevallen kan de betrokkene een geschil voorleggen aan de rechter. Ook kan hij de bemiddeling vragen van het CBP of gebruikmaken van een geschillenregeling binnen een branche als die er is.

Daarnaast hebben betrokkenen altijd de mogelijkheid om verantwoordelijken of bewerkers aansprakelijk te stellen voor de schade die zij als gevolg van hun onrechtmatige gedragingen hebben geleden, met inbegrip van immateriële schade of nadeel. De Wbp helpt hen daarbij door een omgekeerde bewijslast voor de tegenpartij: deze moet bewijzen dat zij alles gedaan heeft wat van haar kon worden gevergd. Ten slotte kan de rechter worden gevraagd om een verbod op te leggen of andere maatregelen te treffen waardoor de belangen van betrokkenen worden beschermd.

Toezicht en handhaving

De Wbp voorziet in een eigen toezichthouder: het College Bescherming Persoonsgegevens, dat net als de Registratiekamer een onafhankelijke positie heeft. Het CBP neemt de taken van de Registratiekamer over, maar krijgt ook een aantal nieuwe taken en bevoegdheden, zowel in het stadium voordat een verwerking aanvangt als later, waarbij ook de mogelijkheid bestaat om sancties op te leggen of andere maatregelen te nemen. Het CBP houdt daarnaast alle onderzoeksbevoegdheden die de Registratiekamer ook had.

Er is overigens alle reden om aan te nemen dat het CBP de beleidsoptiek zal overnemen die de Registratiekamer heeft ontwikkeld en die bekendstaat als het 'viersporenbeleid'. Daarmee wordt gedoeld op bewustwording, normontwikkeling en privacytechnologie als drie sporen die een goede omgang met persoonsgegevens kunnen bevorderen, zodat de aandacht voor het vierde spoor van de handhaving kan worden gericht op die gevallen waar dat nodig is. Ook binnen dit laatste spoor zijn verschillende fasen te onderscheiden, waarbij enerzijds ruimte is voor zelfregulering en anderzijds voor ingrijpende interventies.

Vóór in het proces staat in de Wbp de verplichting tot aanmelding van de verwerking bij het CBP, tenzij het gaat om een verwerking die valt onder één van de veertig vrijstellingen van het Vrijstellingsbesluit. Om na te gaan of dit het geval is kan gebruik worden gemaakt van de elektronische hulpmiddelen die daarvoor worden ontwikkeld en die zowel op diskette als op de website van het CBP (www.cbpweb.nl) beschikbaar zullen zijn. Daarmee kan zo nodig ook een melding worden aangemaakt, terwijl op termijn ook een melding langs elektronische weg mogelijk zal zijn. Het niet voldoen aan de wettelijke meldingsplicht kan aanleiding geven tot strafsancties of administratieve boeten. Deze plicht kan in bepaalde gevallen eveneens worden nagekomen door aanmelding bij een privacyfunctionaris binnen de betrokken organisatie of branche, die verderop nog aan de orde komt. Deze mogelijkheid bestaat niet als het om een in de wet omschreven situatie met bijzondere risico's gaat waarin het CBP een voorafgaand onderzoek moet instellen. Een niet-geautomatiseerde verwerking behoeft nooit te worden aangemeld, tenzij voorafgaand onderzoek nodig is.

Een dergelijk onderzoek moet tegelijk met de aanmelding worden aangevraagd en brengt voor de verzoeker de verplichting mee om het resultaat daarvan af te wachten, tenzij blijkt dat van nader onderzoek door het CBP wordt afgezien, bijvoorbeeld omdat het gaat om een 'standaardgeval' waarbij aan alle eerder geformuleerde eisen is voldaan. Een voorafgaand onderzoek leidt tot een oordeel over de rechtmatigheid van de verwerking, waartegen de belanghebbende desgewenst in beroep kan gaan bij de bestuursrechter. Een aanmelding leidt anders niet tot een instemmend of afkeurend oordeel, tenzij het CBP uit eigen beweging zou besluiten tot een onderzoek omdat de inhoud van de melding daartoe aanleiding geeft. Zoals gezegd, zal het oordeel van het CBP soms nodig zijn, omdat de verwerking van bijzondere gegevens niet kan steunen op een wettelijke grondslag, ter-

wijl het algemeen belang de verwerking toch lijkt te vereisen. Ook in dat geval kunnen belanghebbenden dat oordeel aanvechten bij de rechter.

Verderop in het proces kan het CBP op verzoek van belanghebbenden of uit eigen beweging besluiten tot een onderzoek naar de verwerking, zelfs als deze eerder het voorwerp is geweest van een voorafgaand onderzoek. Bij een dergelijk onderzoek kunnen alle bevoegdheden van het CBP worden ingezet, met inbegrip van een uitgebreid onderzoek ter plaatse met steun van deskundigen of de sterke arm. Een dergelijk onderzoek zal in de regel leiden tot een rapport van bevindingen, dat eerst om commentaar wordt voorgelegd aan de betrokken organisatie en dat vervolgens ook aanleiding kan zijn tot het doen van aanbevelingen. Afhankelijk van het vervolg kan een en ander leiden tot een gebruik van de nieuwe handhavingsbevoegdheden: de mogelijkheid om aanwijzingen te geven onder oplegging van een dwangsom, en zo nodig de toepassing van bestuursdwang, waarbij op kosten van de overtreder via direct ingrijpen kan worden rechtgezet wat deze ten onrechte heeft gedaan of nagelaten. Daarbij kan het dus gaan om het afbreken van systemen of het aanbrengen van een bepaalde beveiliging. Ook in deze gevallen kan de verantwoordelijke daartegen in beroep gaan bij de bestuursrechter.

Zelfregulering en kwaliteitszorg

De wetgever heeft er geen twijfel over laten bestaan dat de open normen van de Wbp ook kunnen worden gezien als een uitnodiging aan verantwoordelijken om invulling te geven aan hun verantwoordelijkheid voor een behoorlijke en zorgvuldige gegevensverwerking. Op het niveau van de sector of branche is de ontwikkeling van een gedragscode daarvoor een middel. De wet bevat de mogelijkheid om gedragscodes ter beoordeling voor te leggen aan het CBP en het oordeel van het CBP weer ter toetsing voor te leggen aan de rechter. Het CBP kan van zijn kant aangeven dat zelfregulering in een bepaalde sector ten onrechte achterwege blijft en aansturen op het opleggen van een dwingende regeling. Deze mogelijkheid is overgenomen uit de Wpr, maar is daar tot dusver niet gebruikt.

> Het beschikken over een privacyfunctionaris kan een concurrentiewapen worden op het terrein van de privacygevoelige dienstverlening.

Een tweede mogelijkheid is dat een privacyfunctionaris wordt aangesteld voor een bepaalde organisatie of sector, die binnen deze kring optreedt als interne toezichthouder en ook kan fungeren als aanspreekpunt voor betrokkenen. De wet stelt hieraan bepaalde eisen, maar laat de verantwoordelijken overigens vrij om hier een passende voorziening te treffen. Als deze functionaris – in de Wbp ‘functionaris voor de gegevensbescherming’ genoemd – aan de eisen van de wet voldoet en bij het CBP is aangemeld, kan de aanmelding van verwerkingen bij het CBP achterwege blijven. De betrokken functionaris kan uitgroeien tot de motor van kwaliteitszorg op dit gebied. Het is denkbaar dat ‘privacy’ aldus ook een rol gaat spelen in de concurrentie op het terrein van de privacygevoelige dienstverlening.

In dit perspectief valt ook de auditaanpak te zien, die in het afgelopen jaar is ontwikkeld door een samenwerkingsverband van Registratiekamer, enige marktpartijen en koepelorganisaties op het terrein van de EDP-auditing. Deze aanpak voorziet expliciet in een gelaagd model van Quickscan, Zelfevaluatie en Privacy Audit, waarbij de eerste inzet op bewustwording en de volgende in opklimmende mate zekerheid bieden over de kwaliteit die binnen een organisatie aanwezig is bij de verwerking én bescherming van persoonsgegevens. Het ligt in de rede dat het CBP zich terughoudend zal opstellen tegenover bedrijven en instellingen die aldus werken aan een structurele verbetering van de gegevensbescherming.

Internationale aspecten

De Wbp brengt ook in een ander opzicht enige nieuwe elementen. Ingevolge de EG-richtlijn is de wet bijvoorbeeld van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verantwoordelijke in Nederland. Dat brengt mee dat Nederlands recht ook van toepassing kan zijn op verwerkingen in het buitenland en dat omgekeerd het recht van andere EU-landen van toepassing kan zijn in ons land. Met name in de sfeer van de elektronische handel op afstand kan zich die situatie steeds meer voordoen. Als een verantwoordelijke buiten de EU is gevestigd, zal hij een vertegenwoordiger binnen de EU moeten aanwijzen. Deze vertegenwoordiger wordt voor de toepassing van de Wbp als verantwoordelijke aangemerkt, zodat de verdeling van rechtsmacht binnen de EU weer rond loopt. De nationale toezichthouders zijn, ieder binnen zijn eigen jurisdictie, ook belast met het toezicht op de naleving van het recht van de andere EU-lidstaten en leveren elkaar onderling hulp en bijstand.

Een ander nieuw element is dat het gegevensverkeer binnen de EU met inachtneming van de wettelijke grenzen weliswaar vrij is, maar het gegevensverkeer naar derde landen niet. Daarbij geldt het uitgangspunt dat alleen gegevensverkeer is toegestaan naar landen buiten de EU die een passend niveau van bescherming bieden. Is aan deze voorwaarde niet voldaan, dan gelden speciale voorwaarden en beperkingen die soms een ontheffing nodig maken van de minister van Justitie. Met de Verenigde Staten is een bijzondere regeling getroffen die bekend staat als ‘Safe Harbor’. Bedrijven die zich aan die regeling onderwerpen en zich daaraan houden, worden geacht een passend niveau van bescherming te bieden. Inmiddels zijn ook door de Europese Commissie goedgekeurde contracten beschikbaar die passende bescherming kunnen bieden. Bedrijven die in een internationale omgeving werkzaam zijn, doen er goed aan zich op deze problematiek te oriënteren.

Invoering en overgangsrecht

Om terug te grijpen op het begin van dit artikel: er is veel inhoudelijke continuïteit, maar er zijn ook de nodige nieuwe elementen. Daarbij komt dat de belangen in veel opzichten zijn toegenomen en dat de gevolgen van niet-naleving, mede door de nieuwe handhavingsopties, ook ernstiger kunnen zijn.

Het is dus gewenst dat organisaties zich terdege rekenschap geven van de vraag waar zij op dit gebied nu staan of willen staan. Hetzelfde geldt voor hun adviseurs en dienstverleners, want ook zij krijgen te maken met een nieuwe werkelijkheid. Mocht dit tot dusver niet zijn gebeurd, dan is het de hoogste tijd een inventarisatie te maken van 'verwerkingen' met 'privacy-impact' en te analyseren welke consequenties de Wbp daarvoor heeft. Daarbij is in elk geval kritische aandacht nodig voor doelomschrijvingen en het verruimde regime voor spontane informatieverstrekking aan de betrokkenen. Deze operatie kan ook een goede kans bieden om de 'privacy standing' van een organisatie aan de orde te stellen en waar nodig te verbeteren.

De kalender voor deze operatie ligt inmiddels vast. Op 1 september 2001 is de Wbp in werking getreden. Nieuwe gegevensverwerkingen moeten aan de nieuwe regels voldoen. Bestaande of lopende verwerkingen – dat wil zeggen verwerkingen die vóór die datum reeds plaatsvonden – moeten binnen één jaar zijn aangepast. Daarbinnen moeten zij ook voldoen aan de meldingsplicht, zo die er is. Bij voorafgaande onderzoeken behoeft niet een lopende verwerking te worden onderbroken. Deze overgangstermijn loopt op 1 september 2002 af. Alleen voor die gevallen waarin de nieuwe regels voor bijzondere gegevens strikter zijn dan de bestaande, is een aanpassingstermijn van drie jaar voorzien. Op 1 september 2004 loopt ook deze termijn af.

Mr. P.J. Hustinx
is voorzitter van het College Bescherming Persoonsgegevens (CBP).