Auditor en privacy

De rol van de auditor bij de implementatie van de Wbp

Drs. H.G.Th. van Gils RE RA en J.P.M.J. Leerentveld RA

Op 1 september 2001 is de Wet bescherming persoonsgegevens (Wbp) van kracht geworden. Deze wet vervangt de Wet persoonsregistraties (Wpr) en stelt eisen aan de wijze waarop organisaties persoonsgegevens verwerken. De eisen in de Wbp zijn veranderd en uitgebreid ten opzichte van de Wpr. De wijzigingen weerspiegelen de sterk gegroeide en nog steeds groeiende mogelijkheden van informatie- en communicatietechnologie. Een organisatie die momenteel voldoet aan de bepalingen van de Wpr, voldoet daarmee niet automatisch aan de eisen die de Wbp stelt. Het College Bescherming Persoonsgegevens (CBP, opvolger van de Registratiekamer) heeft als toezichthoudende instantie in samenwerking met beroepsorganisaties van auditors en marktpartijen een aantal assuranceproducten ontwikkeld, waarmee onder meer de overgang van Wpr naar Wbp wordt vergemakkelijkt. In dit artikel zullen wij een overzicht geven van deze assuranceproducten. Daarnaast verwijst dit artikel naar meer informatie over zowel de Wbp als de gevolgen van de Wbp voor organisaties.

Introductie

Eerst geven wij een korte introductie van de Wbp en de belangrijkste verschillen met de Wpr. De gevolgen van de Wbp voor de organisatie worden benoemd, waarbij de bescherming van persoonsgegevens als een belangrijke managementverantwoordelijkheid wordt gezien. Daarna zullen wij de assuranceproducten introduceren, waarbij doelstelling, opzet en werkwijze van de producten uiteengezet worden. Het betreft een Quickscan, Wbp Zelfevaluatie en Raamwerk Privacy Audit. De toegevoegde waarde voor organisaties van deze producten als beoordelings- en toetsingsinstrument zal blijken, evenals de rol van de auditor bij de implementatie van de Wbp in het algemeen en de toepassing van deze assuranceproducten in het bijzonder. Tot slot zullen wij kort ingaan op de gevolgen van de Wbp voor de reguliere jaarrekeningcontrole en de eisen formuleren waaraan een auditor moet voldoen als hij betrokken is bij de toepassing van de assuranceproducten.

Waarom een nieuwe wet?

Met de inwerkingtreding van de Wbp voldoet Nederland aan de Europese Richtlijn (95/46/EG) van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Daarmee is invulling gegeven aan de wens om de regelgeving in Europa te harmoniseren. De eerbiediging van de persoonlijke levenssfeer is één van de grondbeginselen van het internationale rechtsbestel[1]. De hedendaagse ontwikkelingen in met name de informatie- en communicatietechnologie (ICT) geven duidelijk de maatschappelijke noodzaak aan voor een adequate privacybescherming. De eenvoudige wijze van verzamelen, registreren, verwerken en aanwenden van omvangrijke hoeveelheden persoonsgegevens voor verschillende doeleinden, alsmede de mogelijkheden tot koppeling van geautomatiseerde gegevensbestanden, brengen grote risico's van inbreuken op de persoonlijke levenssfeer met zich mee. Onrechtmatige verwerking van persoonsgegevens is ook moeilijk(er) vast te stellen, doordat herkomst en gebruik van persoonsgegevens lastig zijn te traceren.

De Wbp[2] kent een belangrijke uitbreiding van het object; niet alleen de registratie van persoonsgegevens, zoals onder de Wpr, is aan voorwaarden gebonden, maar de gehele verwerkingsketen, van het verzamelen, vastleggen, ordenen en bewaren tot aan het verstrekken en vernietigen van persoonsgegevens, valt onder de reikwijdte van de nieuwe wet.

De eisen die de wet stelt aan de verwerking zijn te classificeren in een aantal kernbegrippen: transparantie, doelbinding, rechtmatige grondslag, kwaliteit en beveiliging. Hieruit vloeien voor organisaties die persoonsgegevens verwerken (verantwoordelijken) de belangrijkste plichten voort. Zo mogen zij persoonsgegevens slechts verwerken voorzover zij daarvoor een rechtmatige grondslag hebben, zoals in de Wbp limitatief omschreven. Belangrijk is dat de verwerking van persoonsgegevens slechts plaatsvindt voor het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, dan wel voor een doel dat daarmee verenigbaar is. Aan de verwerking van bijzondere persoonsgegevens (o.a. godsdienst, ras, gezondheid, seksleven, strafrechtelijke gegevens) zijn stringentere eisen gesteld. Voorzover persoonsgegevens worden verwerkt dient dit, voor de betrokkenen, transparant te gebeuren en moet de kwaliteit van de persoonsgegevens en de beveiliging van de verwerking gewaarborgd zijn. De informatieplicht naar betrokkenen van wie persoonsgegevens worden verwerkt, is uitgebreid. Daarnaast biedt de Wbp burgers meer rechten, waaronder het recht op inzage, wijziging en verwijdering van persoonsgegevens en het recht op verzet tegen het verwerken van persoonsgegevens[3].

Onder de nieuwe wet is het CBP als opvolger van de Registratiekamer belast met het toezicht op de naleving van de wet. Het CBP kan onderzoeken, waaronder privacyaudits, uitvoeren om de naleving van de wettelijke bepalingen te controleren.

Een evenwichtig verwerkingsbeleid voor persoonsgegevens zal een belangrijke plaats in de managementcyclus moeten innemen.

Het CBP heeft onder de Wbp ruimere handhavings- en sanctiebevoegdheden. Onder de Wpr had de Registratiekamer alleen de mogelijkheid overtredingen publiekelijk bekend te maken. Onder de Wbp heeft het CBP de mogelijkheid tot het opleggen van boetes en het afdwingen van de naleving van de wet. Bij het niet naleven van de meldingsplicht kan het CBP een boete opleggen van maximaal *f* 5.000 per melding. Voor het afdwingen van het naleven van de overige bepalingen heeft het de mogelijkheid tot het opleggen van een last onder dwangsom en het toepassen van bestuursdwang. Het CBP is zich ervan bewust dat het als organisatie niet alleen in staat is de bescherming van persoonsgegevens in Nederland te realiseren. Organisaties zijn hier primair zelf verantwoordelijk voor. De ontwikkeling van assuranceproducten in samenwerking met de auditprofessie is dan ook een uitstekend initiatief om zelfregulering door organisaties te bevorderen.

Privacy als managementvraagstuk

De eisen die de Wbp stelt aan de verwerking van persoonsgegevens hebben gevolgen voor de procedures en maatregelen die een organisatie moet nemen om haar gegevensverwerking te beveiligen en te beheersen. Het management ziet zich voor de taak gesteld deze eisen te vertalen naar toereikende procedures en maatregelen en deze op een doeltreffende manier te verankeren in haar bestaande interne en administratieve organisatie. Vanzelfsprekend zal het stelsel van procedures en maatregelen voor de privacybescherming nauw aansluiten bij het reguliere beheersingskader dat voor de realisering van de bedrijfsdoelstellingen is ingericht. Voor een belangrijk deel zal er sprake zijn van overlap met bestaande procedures en maatregelen. De procedures en maatregelen die specifiek voor de privacybescherming moeten worden getroffen, liggen voor een deel in de gebruikersomgeving (voldoen aan specifieke plichten en waarborgen van rechten van betrokkenen) en voor een deel in de geautomatiseerde omgeving, waarbij de nadruk ligt op de maatregelen die de integriteit, exclusiviteit, beheersbaarheid en controleerbaarheid van de gehele verwerking moeten waarborgen.

Het privacyvraagstuk is voor veel bedrijven tegenwoordig van strategisch belang[4] en wordt door bepaalde bedrijven zelfs als ‘unique selling point’ gezien. NCR, IBM en Microsoft zijn bezig om in hun producten Privacy Enhancing Technologies[5] toe te passen die het de gebruiker mogelijk maken om privacy via technische voorzieningen te realiseren c.q. af te dwingen. Een evenwichtig verwerkingsbeleid voor persoonsgegevens en een adequate implementatie en beheersing daarvan zullen derhalve een belangrijke plaats in de managementcyclus moeten innemen.

Zelfregulering

Het beleid van het CBP richt zich mede op het bevorderen van de bescherming van persoonsgegevens door zelfregulering. Degenen die verantwoordelijk zijn voor het verwerken van persoonsgegevens, dienen deze bescherming als vanzelfsprekend te ervaren en in hun dagelijkse werkzaamheden te verankeren. Het viersporenbeleid (bewustwording, normontwikkeling, technologie en handhaving) dat het CBP sinds enige jaren hanteert, stimuleert zelfregulering. Via voorlichting draagt het CBP bij aan bewustwording bij verantwoordelijken. De assuranceproducten dragen eveneens bij aan het creëren van een adequaat niveau van bewustwording. Via allerlei publicaties, waaronder het Raamwerk Privacy Audit en de onlangs uitgebrachte studie ‘Beveiliging van persoonsgegevens’, schept het CBP een normatief kader dat als referentie dient voor de feitelijke invulling van de privacybescherming. Inzicht in de risico’s bij verwerking van persoonsgegevens door middel van informatietechnologie en de mogelijkheden hiervan (Privacy Enhancing Technologies) dragen bij tot een goed niveau van bescherming van persoonsgegevens. In de assuranceproducten neemt technologie een vooraanstaande plaats in. Daar waar het CBP zijn handhavingsbevoegdheden uitoefent, zal het ook gebruikmaken van de ontwikkelde assuranceproducten, in het bijzonder het Raamwerk Privacy Audit.

Assuranceproducten

Begin 2000 is gestart met de ontwikkeling van de assuranceproducten in een projectvorm (Audit Aanpak Privacy) geïnitieerd door toen nog de Registratiekamer, waarbij alle beroepsorganisaties van auditors (NIVRA, NOvAA, NOREA en ISACA) en verschillende accountants- en adviesorganisaties zijn betrokken. De ontwikkeling is door een klankbordgroep met daarin vertegenwoordigers van Consumentenbond, VNO-NCW, FNV en de ministeries van Justitie en Binnenlandse Zaken en Koninkrijksrelaties kritisch gevolgd.

Belangrijke uitgangspunten van het project waren: een breed draagvlak, een brede verspreidingskring van de te ontwikkelen producten, een duidelijke toegevoegde waarde voor de kwaliteit van gegevensverwerkende processen bij toepassing van de producten en aansluiting bij algemene auditprincipes.

Dit heeft geleid tot een aantal samenhangende producten in een gelaagde opbouw. De drie assuranceproducten hebben een verschillende diepgang en sluiten zodoende logisch op elkaar aan. De Quickscan is een korte vragenlijst die de belangrijkste kernbepalingen van de Wbp omvat met als doel het creëren van bewustwording. De Wbp Zelfevaluatie is een instrument voor het management om zelfstandig, in betrekkelijk korte tijd, de kwaliteit van de privacybescherming te beoordelen. Hierop is een review mogelijk van een deskundige auditor die het resultaat van de zelfevaluatie objectiveert. De bevindingen van de Wbp Zelfevaluatie kunnen de start vormen van een verbetertraject in de organisatie voor de bescherming van persoonsgegevens. Het Raamwerk Privacy Audit vormt de basis voor het uitvoeren van een privacyaudit door een deskundige auditor. De uitkomsten van een privacyaudit geven de leiding van een organisatie, door middel van een oordeel met een hoge mate van zekerheid, inzicht in de mate van naleving van de wettelijke bepalingen.

De indeling van de producten is gebaseerd op een negental aandachtsgebieden die uit de Wbp zijn afgeleid. In de Quickscan komen de belangrijkste aandachtsgebieden op globale wijze aan bod. In de Wbp Zelfevaluatie en het Raamwerk Privacy Audit zijn alle negen aandachtsgebieden[6] verankerd, met een toenemende diepgang.

De verwachting is dat, net als bij de implementatie van de Wpr, de accountant ook nu een belangrijke rol zal spelen bij het adviseren en begeleiden van zijn cliënten bij de implementatie van de Wbp. De assuranceproducten zijn prima instrumenten voor het management om deze implementatie te realiseren. De accountant kan zijn cliënten stimuleren tot het gebruik van deze producten en kan bij de Wbp Zelfevaluatie een reviewende rol hebben en desgevraagd belast worden met de uitvoering van een privacyaudit.

Quickscan

De Quickscan is een beknopte vragenlijst (dertien vragen) waarmee elke medewerker in een organisatie snel inzicht kan verkrijgen in de mate waarin de organisatie zich bewust is van de bescherming van persoonsgegevens. De vragen zijn geclusterd in vier categorieën: privacybewustzijn in de organisatie, uitvoering wettelijke bepalingen, beveiliging en controle. Op de vragen is alleen 'ja' of 'nee' als antwoord mogelijk. De uitkomsten van de Quickscan geven een globale indruk hoe het met de privacybescherming in de organisatie is gesteld. Het instrument kan het begin zijn van een verbetertraject en als opmaat dienen voor het uitvoeren van een zelfevaluatie.
De Quickscan bevat een duidelijke toelichting op het gebruik. Kennis van de Wbp is niet vereist om de Quickscan in te vullen. De uitkomsten zijn nuttig voor de leiding en de ondernemingsraad en, indien benoemd, de functionaris voor de gegevensbescherming[7]. Voor interpretatie van de antwoorden van de Quickscan is op de website van het CBP (www.cbpweb.nl) een uitgebreide toelichting beschikbaar. Aan de hand van deze toelichting kunnen ook de vervolgstappen worden bepaald.

Vraag 3 uit 'Privacybewustzijn in de organisatie'
De directie of leiding van een organisatie kan op verschillende manieren de privacy bij haar medewerkers onder de aandacht brengen. Daarbij kan gedacht worden aan: informatiesessies over privacy, een privacyrichtlijn voor medewerkers, specifieke acties en maatregelen ter bescherming van de privacy.

Wordt er op uitvoerend niveau binnen uw organisatie aandacht besteed aan privacybescherming? [Ja/Nee]

Vraag 9 uit 'Uitvoering wettelijke bepalingen'
De Wbp legt organisaties die persoonsgegevens verwerken een informatieplicht op. Daardoor weten de personen (betrokkenen) van wie persoonsgegevens worden verwerkt hoe de organisatie met hun persoonsgegevens omgaat.

Leeft uw organisatie de informatieplicht naar betrokkenen na? [Ja/Nee]

Kader 1. Twee vragen uit de Quickscan als voorbeeld.

Wbp Zelfevaluatie

De Wbp Zelfevaluatie is een uitgebreider product dat door functionarissen die bij de privacybescherming betrokken zijn, kan worden gebruikt. De Wbp Zelfevaluatie is een methode om zelfstandig de kwaliteit van de privacybescherming in een organisatie te beoordelen. De uitkomsten van de Wbp Zelfevaluatie geven een duidelijk beeld van de huidige situatie en de noodzakelijke verbeterpunten.

Zoals eerder is aangegeven, is de Wbp Zelfevaluatie opgebouwd rond negen aandachtspunten, die direct aan de Wbp zijn te relateren. De aandachtspunten zijn als vragen geformuleerd (zie tabel 2). De functionaris (of zoals de handreiking in de Wbp Zelfevaluatie zelf aangeeft: het team) dient de vragen op een schaal van vijf te beantwoorden, waarbij steeds het volgende model geldt:

Niveau	Betekenis van de score
1.	Niets vastgelegd en niets bekend
2.	Niets vastgelegd, maar wel bekend
3.	Vastgelegd en bekend
4.	Vastgelegd, bekend en nageleefd
5.	Vastgelegd, bekend, nageleefd en gecontroleerd

Tabel 1.

Door de zelfevaluatie als team uit te voeren en eerst de antwoorden individueel te geven, kan een goede basis voor overleg en bewustwording ontstaan. Dit geldt des te meer als niet alleen de scores worden ingevuld maar ook het bijbehorende ambitieniveau (zelfde scoresysteem, waarbij het ambitieniveau mede zal afhangen van de ontwikkelingsfase waarin de organisatie zich bevindt) en vooral alle reviewvragen worden doorgenomen. Ieder

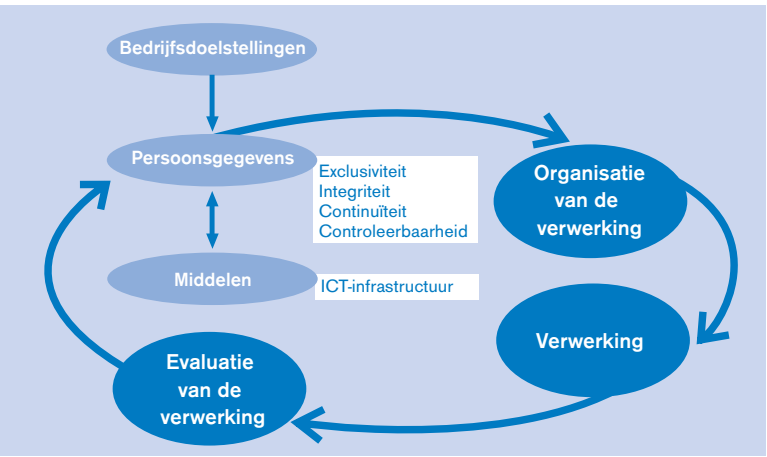
Tabel 2. De negen uit de Wbp afgeleide aandachtsgebieden.

1. Melding	In hoeverre zijn maatregelen en procedures getroffen met stappen vanaf het voornemen om persoonsgegevens te gaan verwerken tot en met het melden van de verwerking en het verstrekken van inlichtingen?
2. Transparantie	Wordt ervoor gezorgd dat de verwerking van de persoonsgegevens voor de betrokkenen transparant is en wordt aan de betreffende informatieverplichting voldaan?
3. Doelbinding	Worden de persoonsgegevens voor een specifiek doel verzameld en verder verwerkt op een manier die verenigbaar is met het doel waarvoor de persoonsgegevens zijn verkregen?
4. Rechtmatige grondslag	Worden de bijzondere persoonsgegevens voor een specifiek doel verwerkt op grond van de in de Wbp genoemde grondslagen?
5. Kwaliteit	Is voorzien in procedures waarin de kwaliteit van de verwerking van persoonsgegevens wordt gewaarborgd?
6. Rechten	In hoeverre worden de rechten van betrokkenen gegarandeerd?
7. Beveiliging en bewustzijn	Bevordert uw organisatie actief het beveiligingsbewustzijn bij de medewerkers? Zijn er afspraken gemaakt over het beheer van de informatietechnologie? Zijn maatregelen en procedures getroffen om te voorkomen dat onbevoegden toegang krijgen tot locaties, informatiesystemen en gegevensbestanden? Zijn maatregelen getroffen om te voorkomen dat onbevoegden toegang krijgen tot persoonsgegevens bij datacommunicatie? Zijn er procedures voor het bewaren en vernietigen van gegevens? Welke voorzorgen zijn getroffen in het geval zich calamiteiten voordoen?
8. Bewerker	Is de gegevensverwerking geheel of gedeeltelijk uitbesteed en zijn in het contract (SLA) afspraken vastgelegd over informatiebeveiliging en de toetsing daarvan?
9. Niet EU-landen	Wordt gerealiseerd dat het verwerken van persoonsgegevens in een land buiten de EU aan aanvullende en bijzondere regels is gebonden en worden die regels nagekomen?

aandachtspunt is namelijk rijkelijk voorzien van reviewvragen (te beantwoorden met ja/nee), waardoor de invuller als het ware wordt geleid naar de van toepassing zijnde score. De overzichtelijkheid van de clustering van vragen in aandachtsgebieden en de mate van detaillering van de vragen vergroot de bewustwording van de functionaris.

Eventuele verschillen tussen de feitelijke score en het aangegeven ambitieniveau kunnen voor het management een goed hulpmiddel zijn om verbeteracties te definiëren. Ook een lage absolute score of lage ambitie kan de vraag oproepen of men zich het belang van de bescherming van persoonsgegevens in voldoende mate realiseert. Desgewenst kan een organisatie de intern uitgevoerde zelfevaluatie laten reviewen door een externe auditor, die daarbij tevens een vergelijkingsmaatstaf kan aanleggen ten opzichte van andere organisaties.

Figuur 1. De managementcyclus met betrekking tot verwerking van persoonsgegevens.



Raamwerk Privacy Audit

Het Raamwerk Privacy Audit vormt het sluitstuk van de productenset en in die hoedanigheid de basis voor het uitvoeren van privacyaudits. De privacyaudit dient door een onafhankelijke auditor te worden uitgevoerd. Het is een fullscope-audit naar de wijze waarop en de mate waarin de organisatie voldoet aan de eisen die de wet heeft gesteld aan de bescherming van persoonsgegevens. Daarom is uitgegaan van de gehele managementcyclus. Natuurlijk gaat het hier ook weer om de negen aandachtsgebieden, die in figuur 1 binnen het element *Verwerking* vallen. Maar deze verwerking moet in een deugdelijke organisatie zijn ingebed en er dient een evaluatie plaats te vinden van de mate waarin de verwerkingsprocessen worden beheerst.

Het Raamwerk Privacy Audit gaat in op de negen aandachtsgebieden van de *Verwerking*, waarbij per aandachtsgebied steeds een handreiking wordt gedaan voor de evaluatie van de relevante onderzoeksvragen. In de bijlagen vindt een nadere uitwerking plaats van de aandachtsgebieden voor de *Organisatie van de verwerking* (het zogenaamde O-deel) en de *Evaluatie van de verwerking* (E-deel). In die zin geeft het Raamwerk Privacy Audit een breder referentiekader dan de Wbp Zelfevaluatie. Echter, het Raamwerk bevat niet, zoals de Wbp Zelfevaluatie, kant-en-klare vragen en scoremogelijkheden, omdat het Raamwerk Privacy Audit uitgaat van de deskundigheid van de auditors om de soort en omvang van de controlewerkzaamheden op het intern getroffen stelsel van technische en organisatorische maatregelen

ter beveiliging van de verwerking van persoonsgegevens te bepalen.

In dat kader is een risicoanalyse op zijn plaats. Aan de hand van een eenvoudig schema (zie tabel 5) is een risicoklasse te bepalen. Deze risicoklassen zijn terug te vinden in het document 'Beveiliging van Persoonsgegevens'[8], dat in dit verband als een goed referentiekader voor te treffen beveiligingsmaatregelen en procedures geldt. Het document bevat overeenkomstig de Code voor Informatiebeveiliging veertien categorieën van maatregelen, die per risicoklasse nader zijn gespecificeerd. Daarnaast kan de auditor mogelijk gebruikmaken van reeds eerder uitgevoerde audits, bijvoorbeeld in het kader van de jaarrekeningcontrole of specifieke IT-audits (zoals systeemaudits en rekencentrumaudits).

Certificering

In het algemeen kan worden gesteld dat de behoefte aan bescherming van de persoonlijke levenssfeer toeneemt naarmate meer gegevens met een commerciële waarde worden verwerkt. Om aan belanghebbenden (medewerkers, klanten, enz.) duidelijk te kunnen maken dat op zorgvuldige wijze wordt omgegaan met de bescherming van persoonsgegevens, wordt op dit moment door het CBP en de beroepsorganisaties van auditors (NIVRA, NOvAA, NOREA, ISACA) een privacycertificaat ontwikkeld. Het CBP heeft aangegeven grote waarde te hechten aan een afgegeven privacycertificaat op basis van het Raamwerk Privacy Audit. Om de kwaliteit van het certificaat te waarborgen zullen in het op te stellen accreditatie- en certificatieschema hoge eisen worden gesteld aan de deskundigheid van de auditor, alsmede aan de kwaliteit van de uitvoering van het onderzoek.

Auditors

Aan het slot van dit artikel is het zinvol na te gaan op welke wijze de nieuwe Wbp de auditor raakt. Voorop staat dat ook de auditor bij de uitvoering van zijn werkzaamheden de bepalingen van de Wbp in acht moet nemen, hetgeen betekent dat ook hij/zij zorgvuldig zal moeten omgaan met eventuele persoonlijke gegevens die hem/haar ter kennis komen.

Voorts zullen kort de volgende mogelijke rollen van de auditor worden belicht:
- controleur van de jaarrekening;
- adviseur bij de implementatie van de Wbp;
- assurance provider bij specifieke privacyvraagstukken.

Tot slot wordt ingegaan op de vereiste deskundigheid.

Controleur van de jaarrekening

Richtlijn 250 'Het belang van wet- en regelgeving bij de controle van de jaarrekening' uit de Richtlijnen voor de Accountantscontrole bevat enkele relevante artikelen. Artikel 2 wijst er nadrukkelijk op dat de accountant er bij de planning en uitvoering van controlewerkzaamheden, bij de evaluatie van de controlebevindingen en bij de rapportage daarover zich dient te realiseren dat het niet naleven van wet- en regelgeving door de huishouding een materieel effect op de jaarrekening kan hebben. Hoewel de boetes in geval van niet melden voor de meeste organisaties niet materieel zullen zijn voor de jaarrekeningcontrole, kunnen de gevolgen van een dwangsom dan wel bestuursdwang wel materiële invloed op de jaarrekening hebben.

Volgens artikel 13 van de betreffende richtlijn dient de accountant de controle op te zetten en uit te voeren met een professioneel-kritische instelling voor omstandigheden en gebeurtenissen die twijfel oproepen omtrent de vraag of de huishouding zich houdt aan wet- en regelgeving.

Titel 9 BW2 geeft aan dat de accountant melding doet van de kwaliteit van de (geautomatiseerde) informatieverzorging en het maatschappelijk verkeer gaat ervan uit dat de accountant het management op de hoogte brengt van risico's die zich voordoen met betrekking tot de management control van de bedrijfsprocessen. Risico's inzake de vertrouwelijkheid van gegevens, inclusief persoonsgegevens, passen daar zeker in deze tijd goed bij. In de praktijk blijkt ook in menige management letter dat de accountant deze rol invult en het management op de risico's wijst.

O 01	Planning en organisatie van de verwerking van persoonsgegevens
O 02	Definieer ICT-infrastructuur
O 03	Bepaal het technologiebeleid
O 04	Definieer de verwerkingsorganisatie en haar relaties
O 05	Management van kwaliteitbevorderende verwerkingsinvesteringen
O 06	Communiceren privacydoelstellingen en privacybeleid
O 07	Personeelsmanagement
O 08	Waarborgen dat aan aanvullende eisen wordt voldaan
O 09	Beoordeling van afhankelijkheid en kwetsbaarheid van de verwerking
O 10	Projectmanagement
O 11	Kwaliteitsmanagement voor de gegevensverwerking
O 12	Service level beheer
O 13	Beheren van diensten van derden
O 14	Beschikbaarheidsbeheer
O 15	Waarborgen van continuïteit
O 16	Waarborgen van logische toegangsbeveiliging
O 17	Opleiden en trainen van gebruikers
O 18	Ondersteunen en adviseren van gebruikers (helpdesk)
O 19	Configuratiebeheer
O 20	Probleembeheer en incidentenbeheer
O 21	Gegevensbeheer
O 22	Faciliteitenbeheer
O 23	Operationeel beheer

Tabel 3. Aandachtspunten Organisatie van de verwerking (O-deel).

E 01	Beheersen van de processen
E 02	Verkrijgen van een deskundig oordeel

Tabel 4. Aandachtspunten Evaluatie van de verwerking (E-deel).

Hoeveelheid persoonsgegevens	Complexiteit verwerking	Aard van de persoonsgegevens		
		Algemeen	Bijzonder (art. 16 Wpb)	Financieel/economisch
Weinig	Laag	Risicoklasse 0	Risicoklasse 2	Risicoklasse 2
Veel	Hoog	Risicoklasse 1	Risicoklasse 3	

Tabel 5. Schema voor het bepalen van de risicoklasse.

Drs. H.G.Th. van Gils RE RA is werkzaam als senior medewerker bij KPMG Information Risk Management en was als taskforcelid en werkgroeplid betrokken bij het project Auditaanpak.

J.P.M.J. Leerentveld RA is werkzaam als privacy-auditor bij het College Bescherming Persoonsgegevens en is projectleider Audit Aanpak Privacy.

De auteurs danken J. Pasmooij RE RA RO voor zijn kritische bijdrage aan dit artikel.

Adviseur bij de implementatie van de Wbp

Gezien de deskundigheid van de accountant en IT-auditor mag verwacht worden dat zij voor hun klanten een actieve bijdrage kunnen leveren aan de overgang van de Wpr naar de Wbp. Een goed voorbeeld daarvan is het begeleiden van een organisatie bij het uitvoeren van de Wbp Zelfevaluatie.

Assurance provider bij specifieke privacyvraagstukken

Voor het laten uitvoeren van een privacyaudit kan een organisatie verschillende motieven hebben. Globaal kunnen twee belangrijke motieven worden onderkend, namelijk het belang om eventuele sancties en negatieve berichtgeving die kunnen voortvloeien uit het niet naleven van de wet te voorkomen en het zich op positieve wijze profileren naar afnemers, leveranciers, werknemers, publiek, enz. door middel van een privacycertificaat.

Afhankelijk van de behoefte van organisaties aan assurance kan hierin worden voorzien door ofwel een onafhankelijke review op een intern uitgevoerde zelfevaluatie, ofwel het uitvoeren van een privacyaudit op basis van het Raamwerk.

Deskundigheid

De vraag is of de accountant en IT-auditor voldoende kennis hebben om in de rollen zoals hiervoor beschreven, te kunnen opereren.
De vereiste deskundigheid voor de eerdergenoemde rollen beslaat de volgende deelgebieden:
* (administratieve) organisatie;
* informatietechnologie;
* auditing;
* privacyrecht (Wbp en overige sectorale en horizontale wetgeving).

De basis daarvoor is in de beroepsopleidingen voor accountants en IT-auditors gelegd in de vorm van de vakken (administratieve) organisatie, automatisering en controleleer respectievelijk IT-auditing.
Voor de accountant in zijn rol als controleur van de jaarrekening mag worden verondersteld dat de opleiding de eerstgenoemde drie deelgebieden in voldoende mate afdekt, met de kanttekening dat voor complexe IT-omgevingen de inzet van een IT-auditor noodzakelijk is.

Om te kunnen voorzien in de basiskennis omtrent de privacyproblematiek volstaat het dat de auditor kennisneemt van de relevante artikelen over wet- en regelgeving op het gebied van privacy zoals die in de vak- en branchebladen worden gepubliceerd.

In de rol van adviseur c.q. assurance provider is aanvullende opleiding vereist op het gebied van de privacywetgeving en het kunnen toepassen daarvan in de praktijk. Hiertoe wordt door de beroepsorganisaties op dit moment een applicatiecursus Wbp ontwikkeld.

Conclusie

De bescherming van gegevens over personen raakt vrijwel alle organisaties. De invoering van de Wbp per 1 september 2001 betekent dat organisaties zich moeten herbezinnen op de maatregelen en procedures ter bescherming van persoonsgegevens. De mate waarin voorzieningen moeten worden getroffen om die persoonsgegevens te beschermen tegen misbruik of oneigenlijk gebruik, verschilt door onder meer de inhoud van de gegevens, de hoeveelheid gegevens, de doelstelling van het gebruik, de wijze van verwerking en de verwerkingsomgeving.

De complexiteit van de Wbp noodzaakt voor veel facetten tot interpretatie en vertaling naar de praktijk van alledag. Om die vertaling zo goed mogelijk op de praktijk af te stemmen zijn de in dit artikel behandelde producten ontwikkeld en beschikbaar gesteld. Zie in dit verband de website van het CBP, www.cbpweb.nl.
Uit dit artikel blijkt dat de accountant en IT-auditor verschillende rollen kunnen vervullen bij het vraagstuk van de privacybescherming. Daarvoor zijn accountant en IT-auditor voldoende toegerust, behalve op het gebied van de privacywetgeving zelf. Hierin wordt echter voorzien door een applicatiecursus Wbp. Dit artikel levert een bescheiden bijdrage aan het verhogen van de privacykennis van de auditor, nodigt uit tot verdere verdieping op dit terrein en stimuleert het gebruik van de drie assuranceproducten.

Noten

1) Onder andere art. 12, Universele Verklaring van de Rechten van de Mens, Verenigde Naties, 1948 en art. 8 Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden, 1950 en art. 10 Grondwet, Koninkrijk der Nederlanden.
2) Meer informatie over de Wbp is te vinden op www.cbpweb.nl, waaronder de teksten van de wet en uitvoeringsbesluiten.
3) Zie de 'Handleiding voor verwerkers van persoonsgegevens' uitgegeven door het Ministerie van Justitie voor meer informatie over de gevolgen van de Wbp voor organisaties (www.minjust.nl).
4) 'E-privacy: het dichten van de kloof tussen Business en Consumers', PricewaterhouseCoopers, 2001.
5) Privacy Enhancing Technologies zijn een samenhangend geheel van ICT-maatregelen dat de persoonlijke levenssfeer beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem. Meer informatie in Achtergrondstudies en Verkenningen nr. 11 'Privacy Enhancing Technologies, the path to anonymity', revised edition, Registratiekamer, 1998.
6) Zie tabel 2 waarin de negen aandachtsgebieden zijn opgenomen.
7) De functionaris voor de gegevensbescherming houdt onafhankelijk toezicht op de toepassing en naleving van de Wbp (art. 64 Wbp).
8) 'Beveiliging van persoonsgegevens', Achtergrondstudies en Verkenningen nr. 23, Registratiekamer, 2001.