Privacy audit **blijft winkeldochter**

Nu er een controlerichtlijn is voor privacy-certificering, kunnen registeraccountants en register EDP-auditors een goedkeurende verklaring verstrekken aan organisaties die bij de verwerking van persoonsgegevens voldoen aan de privacyregels. Maar is er wel vraag naar dit - dure - product?

LEX VAN ALMELO

"Toen ik in 1988 nog assistent-accountant was bij BDO, was dit kantoor er ook al mee bezig. Het komt niet echt van de grond." Aldus Harold Kinds - nu beleidsmedewerker IT bij de vereniging van kleinere accountantskantoren SRA - over de privacy audit. Bij een privacy audit laat een organisatie controleren of zij voldoet aan de regels voor de bescherming van persoonsgegevens.
Sinds 1988 is er het nodige gebeurd om dit product in de markt te zetten. Maar tot nog toe zonder al te veel succes. In oktober 2001 schreef *'de Accountant'* onder de kop 'Afwachtende markt voor privacy audit' dat er enkele assurance-producten zijn ontwikkeld: 'Maar het loopt nog niet storm.' Vijf jaar later kunnen wij deze diagnose letterlijk herhalen. Er zijn weliswaar nieuwe initiatieven ontplooid en nieuwe instrumenten ontwikkeld, maar storm, nee, dat loopt het nog niet.

Richtlijn schept helderheid

Wat is er sinds 2001 veranderd? In 2003 heeft een universitaire onderzoeker de markt verkend en vorig jaar verscheen de handleiding voor privacy compliance die NIVRA en NOREA (de beroepsorganisatie van register EDP-auditors) hebben geschreven in samenwerking met het College Bescherming Persoonsgegevens (CBP). Sinds juni 2006 is er bovendien een 'richtlijn assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' *(zie kader)*.
"Nu we een verklaring kunnen afgeven, hebben wij eindelijk iets concreets aan te bieden aan organisaties die gevoelige persoonsgegevens verwerken", zegt Herman van Gils van KPMG.
Jan Matto van Mazars is "blij dat er eindelijk een richtlijn is. De richtlijn geeft helderheid

Vijf privacyproducten

Er zijn de afgelopen jaren verschillende producten ontwikkeld om vast te stellen of organisaties voldoen aan de eisen die gelden voor de bescherming van persoonsgegevens.

- **Quickscan:** Een lijst met dertien vragen waarmee elke medewerker in een organisatie zich een beeld kan vormen van hoe het is gesteld met de bescherming van de persoonsgegevens die de organisatie verwerkt.
- **Wbp-zelfevaluatie:** Met dit instrument kunnen privacy- en/of IT-functionarissen in een organisatie nagegaan of zij voldoen aan de vereisten van de Wet bescherming persoonsgegevens.
- **Raamwerk privacy audit:** In dit toetsingskader zijn de wettelijke normen voor de bescherming van persoonsgegevens toegesneden op de uitvoering van een audit.
- **Handreiking bij het raamwerk:** De handreiking 'Contouren voor Compliance' is gemaakt om het lijvige toetsingskader uit bovengenoemd raamwerk toegankelijker te maken voor zowel privacy auditors als privacyfunctionarissen binnen een organisatie. Het is een hulpmiddel voor compliance en controle.
- **Richtlijn privacy audits:** In deze richtlijn staan de eisen waaraan een privacy audit en privacy auditors moeten voldoen, opdat zij een systeem kunnen certificeren *(zie kader 'Richtlijn privacy audits')*.

FOTO: CORBIS

over de waarde van de verklaring. Maar wat ons betreft had het wel wat eerder gemogen."

Adri de Bruijn van PricewaterhouseCoopers erkent dat de richtlijn "een lange voorgeschiedenis" heeft. Maar het duurt nu eenmaal even voordat twee beroepsgroepen het eens zijn over deskundigheidseisen, terwijl bovendien duidelijkheid moest ontstaan over de rol die het CBP gaat spelen. De richtlijn geeft volgens hem vooral een helder normenkader voor externe auditors, maar is ook bruikbaar voor interne toetsing. "Het voordeel van externe toetsing is dat je als organisatie met een privacycertificaat kunt laten zien dat je je zaken op orde hebt en zorgvuldig omgaat met persoonsgegevens."

Verenigde Staten

Bij gebrek aan een erkende verklaring en een keurmerk waarmee je als organisatie goede sier kunt maken, is de toeloop op de privacy auditors beperkt gebleven. Ook het aantal accountantskantoren dat zich op dit terrein begeeft, is tot nu toe gering: BDO, KPMG, Mazars en PricewaterhouseCoopers.

KPMG heeft volgens Ronald Koorn van dat kantoor een aantal advies- en auditopdrachten uitgevoerd en daarbij onder meer een structuur voor de verwerking en bescherming van persoonsgegevens doorgelicht. "In de internationale praktijk hebben wij onderzoek gedaan naar enkele Amerikaanse multinationals die hier medewerkers of klanten hebben van wie de persoonsgegevens worden verwerkt in de Verenigde Staten. Als dergelijke gegevens vanuit EU-landen naar de VS - waar de privacywetgeving niet voldoet aan de EU-eisen - worden doorgegeven, moet de verwerking voldoen aan de zogenoemde *Safe Harbor Principles*. Wij hebben onderzocht of dat het geval is."

Adri de Bruijn (PwC): 'Als organisatie met een privacycertificaat kun je laten zien dat je je zaken op orde hebt en zorgvuldig omgaat met persoonsgegevens.'

Bureau Kredietregistratie

BDO controleert volgens Jur de Vries en Edwin Schrijver al meer dan tien jaar de manier waarop het Bureau Kredietregistratie (BKR) in Tiel de gegevens verwerkt van miljoenen Nederlanders die een hypotheek, lening of andere schulden hebben uitstaan. "Het BKR heeft jaren geleden al zijn eigen verantwoordelijkheid genomen en de bescherming van persoonsgegevens opgenomen in haar kwaliteitssysteem."

Schrijver: "Wij doen een uitgebreide privacy audit, waarbij we controleren of de juiste informatie over de juiste personen wordt verwerkt. Je kunt hierbij eigenlijk geen fouten tolereren."

Mazars heeft volgens Jan Matto "diverse opdrachten" uitgevoerd voor banken, verzekeraars en overheidsinstanties die willen weten of zij *compliant* zijn. Nu er "een paar schapen over de dam zijn" volgen er hopelijk meer.

Harold Kinds (SRA): 'Ik vraag mij af of de behoefte leeft in het midden- en kleinbedrijf. Ik word er in ieder geval nooit over gebeld.'

Internationale outsourcing

De privacy audit moet nog op gang komen, dat is wel duidelijk. "Financiële instellingen klopten hiervoor in het verleden niet bij ons aan, maar wij zijn nu wel met hen in gesprek. Tot nu toe konden wij nog geen officieel certificaat verstrekken. Met de richtlijn kan het wel", zegt KPMG'er Ronald Koorn. PwC'er Adri de Bruijn: "Volgens ons is er wel een markt, maar nog geen overweldigende belangstelling."

Jan Matto (Mazars): "Wij hebben er redelijk op ingezet en zien mogelijkheden in bepaalde sectoren, zoals de financiële en de zorgsector. Handelsinformatiebureaus hebben al belangstelling getoond."

De klandizie zal moeten komen van organisaties die veel en/of gevoelige persoonsgegevens verwerken. Afgezien van financiële instellingen denken de auditors daarbij vooral aan non-profit-organisaties in de zorg en het onderwijs. Van het bedrijfsleven lijken zij niet al te veel te verwachten. Toch vindt Adri de Bruijn dat grote concerns door internationale outsourcing steeds vaker moeten nadenken over de bescherming van persoonsgegevens die de grens overgaan. Bovendien koppelen ondernemingen en non-profit-organisaties steeds meer verschillende bestanden en dat is lang niet altijd toegestaan.

Geen behoefte

Veel ondernemingen en organisaties houden zich volgens de auditors niet helemaal aan de regels, zeggen Koorn en Schrijver. Dat schept een vraag, zou je zeggen. Maar vooral naar advies en minder naar controle. Want waarom zou je voor betrekkelijk veel geld een auditor over de vloer halen als je weet dat de kans op een negatief oordeel groot is?
Uit de marktverkenning die onderzoeker O. Kuyper van de Erasmus Universiteit in 2003 uitvoerde blijkt dat potentiële opdrachtgevers tegen de hoge kosten aan hikken. Veel van de ondervraagde privacyfunctionarissen (van wie een derde werkzaam was in het bedrijfsleven en tweederde in de non-profit-sector)

Richtlijn privacy audits

Het NIVRA en de NOREA (de Nederlandse Orde van Register EDP Auditors) hebben in juni 2006 een richtlijn voor privacy audits gepubliceerd. Volgens Richtlijn 3600 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' kunnen registeraccountants en register-EDP-auditors een opdrachtgever met een privacy audit zekerheid verschaffen over de mate waarin diens op de bescherming van persoonsgegevens gerichte maatregelen en -procedures voldoen aan de relevante wet- en regelgeving.
De privacy auditor moet volgens de richtlijn beschikken over voldoende kennis en ervaring op het terrein van ICT-controls en over voldoende juridische en praktische kennis van de Wet bescherming persoonsgegevens en overige relevante wet- en regelgeving. Voor zover de kennis en deskundigheid van de privacy auditor tekortschiet kan hij die tot op zekere hoogte inhuren.
De richtlijn bevat een verwijzing naar de normen die de privacy auditor bij zijn beoordeling respectievelijk de aanpak en uitvoering van zijn werkzaamheden moet hanteren, zoals het Raamwerk privacy audit *(zie kader 'Vijf privacyproducten')*. Verder staat in de richtlijn onder meer hoe de privacy auditor moet rapporteren en zijn oordeel moet formuleren.

Martin Noordzij (VNO-NCW): *'Van onze leden heb ik tot nu toe niet gehoord dat zij er behoefte aan hebben.'*

Jan Matto (CBP): *'Het zou een trigger zijn als het CBP een flinke boete oplegt.*

Ronald Koorn (KPMG): *'Als auditors zich in de markt willen prijzen, zullen zij de privacy audit moeten verkopen als onderdeel van een bredere controle.'*

verwachten een hoge mate van zekerheid over de compliance, maar deinzen terug voor de hoge kosten die dit met zich meebrengt.
"Ik vraag mij af of de behoefte leeft in het midden- en kleinbedrijf", zegt Harold Kinds van SRA. "Ik word er in ieder geval nooit over gebeld."
Ook grotere ondernemingen lijken goed te kunnen leven zonder privacy audits. Martin Noordzij van VNO-NCW: "Van onze leden heb ik tot nu toe niet gehoord dat zij er behoefte aan hebben."

Vliegwiel

"Informatiebeveiliging staat wel hoog op de agenda, maar zelfstandige privacy audits zijn nu nog een stap te ver", zegt Ronald Koorn van KPMG. Als accountants of EDP-auditors zich in de markt willen prijzen, zullen zij de privacy audit moeten verkopen als onderdeel van een bredere controle.
Volgens Jan Pasmooij van het NIVRA kan voor grotere ondernemingen van de Sarbanes Oxley-act en de code Tabaksblat een prikkel uitgaan om zeker te willen weten dat zij ook op het terrein van de privacynormen *compliant* zijn.

Jur de Vries van BDO hoopt dat van de groeiende aandrang om maatschappelijk verantwoord te ondernemen "een vliegwieleffect" uitgaat.
Maar van het College Bescherming Persoonsgegevens lijken de privacy auditors nog het meest te verwachten. Deze toezichthouder kan de vraag naar privacycertificering niet alleen stimuleren door het certificaat te erkennen, maar ook door zijn tanden te laten zien.
"Organisaties hebben een speciale aanleiding nodig, een incident", zegt Jan Matto. "Er doen zich weinig grote incidenten voor. Dat is op zichzelf prettig. Bij regelgeving hoort handhaving, het zou dus een *trigger* zijn als het CBP een flinke boete oplegt."
Dat kan woordvoerder Gert Onne van de Klashorst niet beloven. De zelfregulering moet "van onderop" komen en privacybescherming zou een onderdeel moeten worden van het kwaliteitsbeleid. De toezichthouder blijft namelijk graag "op afstand". Dat organisaties met een privacycertificaat minder streng worden gecontroleerd, kan het CBP niet zeggen. "Dat zou een benadeling zijn van kleinere bedrijven die een privacy audit niet kunnen betalen." ■