Accountant logische uitvoerder privacyaudits

College Bescherming Persoonsgegevens stuurt aan op certificering

Interview bij het afscheid van prof. A.W. Neisingh RE RA – partner KPMG IRM

Niet in alle gevallen, maar wel vaak en vooral bij organisaties die georiënteerd zijn op consumenten (B2C) is er sprake van een vanzelfsprekende relatie tussen financiële en persoonsgebonden gegevens. Dat kwalificeert de accountant als een logische uitvoerder van privacyaudits. Al is dat geen vanzelfsprekendheid. De voorzitter van het College Bescherming Persoonsgegevens mr. P.J. Hustinx wijst op de noodzaak van bijscholing in de complexe materie van de Wet bescherming persoonsgegevens. Bovendien kan de beroepsgroep concurrentie van buiten de accountancy verwachten als het gaat om privacycertificering.

Het afscheid van Dries Neisingh is geplaatst onder het thema 'Nieuwe tijden voor accountants', de titel van het seminar op 12 november aan de Rijksuniversiteit Groningen, waar hij zijn afscheidscollege zal houden. Nu zijn nieuwe tijden van alle tijden, maar toch zijn de huidige tijden wel buitengewoon roerig. Daarom is het thema goed gekozen. Dat vinden ook vier vooraanstaande denkers en publicisten, die zich allen bezighouden met de belangrijkste elementen uit het levenswerk van Dries Neisingh. Zij geven op het genoemde afscheidsseminar acte de présence en stemden bovendien toe in een interview met Compact. De volgende onderwerpen komen daarbij aan bod:

1. Welke wettelijke kaders staan de opdrachtgever en de accountant bij de verlening van assurancediensten ter beschikking? Spreker: prof. mr. H. Franken, hoogleraar Universiteit Leiden.
2. De accountant als logische uitvoerder van privacyaudits, welke aanvullende deskundigheid is vereist? Spreker: mr. P.J. Hustinx, voorzitter College Bescherming Persoonsgegevens.
3. Welke IT-kennis mag de afnemer van assurancediensten bij de accountant verwachten? Spreker: dr. R.G.A. Fijneman RE RA, universitair hoofddocent Universiteit van Tilburg, partner KPMG IRM.
4. Hoe heeft het denken over toezicht en toezichthouders zich ontwikkeld? Spreker: prof. dr. A. Schilder RA, directeur Nederlandsche Bank, bestuurslid Pensioen- en Verzekeringskamer en hoogleraar UvA.

Mr. P.J. Hustinx, voorzitter van het College Bescherming Persoonsgegevens: 'Er zijn natuurlijk vooral in de business-to-business gerichte ondernemingen hele domeinen waarin de vraagstelling niet speelt, maar het is inderdaad zo dat scheiding van controle op financiële informatie en bezig zijn met persoonsgebonden gegevensverwerking in steeds meer situaties niet goed mogelijk is. Daarbij denk ik aan informatie over geleverde diensten aan individuen of aan situaties waarbij de kredietwaardigheid van personen in het geding is bij de beoordeling van de waarde van uitstaande vorderingen. Financiële accountants stuiten op persoonsgegevens bij instellingen als banken en verzekeraars, ziekenhuizen, overheden, nutsbedrijven of meer in het algemeen gezegd de grote dienstverleners. Overigens is de combinatie van financiële en persoonsgebonden informatie niet onontwarbaar. Maar je moet wel beginnen met vast te stellen waar we over spreken, namelijk over het feit dat bij de stroom van persoonsgegevens binnen organisaties zowel maatschappelijke als persoonlijke belangen aan de orde zijn. Die persoonlijke belangen benoemen we nu als het privacyvraagstuk, maar het gaat in wezen om een aantal zeer fundamentele belangen van mensen. Word ik eerlijk behandeld? Zijn mijn gegevens wel juist, want ik word erop beoordeeld? Vindt er geen discriminatie plaats? Zijn zoveel gegevens over mij wel nodig voor deze taak? Privacybescherming vertaalt zich dus in een hele reeks van criteria en grensafbakeningen die terug moeten komen in werkprocessen, organisatorische procedures en technische voorzieningen.'

Hoewel financiële controle, EDP-auditing en de beoordeling van de privacystrategie bij de opdrachtgever dicht bij elkaar kunnen liggen, is het volgens Hustinx niet zo dat de accountant het er maar even bij kan doen. Daarvoor is de materie van de Wet bescherming persoonsgegevens (Wbp) te complex. De wet is ingegaan op 1 september 2001. Op dat moment werd de Registratiekamer omgedoopt in het College Bescherming Persoonsgegevens, dat ten opzichte van de oude Registratiekamer er een heleboel nieuwe bevoegdheden bij kreeg. De Wbp wijkt dan ook op essentiële punten grondig af van de voorgaande Wet persoonsregistraties. 'De accountant moet daarom op studie en ik denk dat hij die nieuwe kennis ook moet bijhouden', aldus Hustinx. Hij denkt dat een actieve bijscholing van enkele dagen noodzakelijk is.

Gelaagde aanpak

Als de accountant inderdaad privacycontroles gaat doen, is het natuurlijk de vraag in welke rol hij komt ten opzichte van de toezichthouder. Hustinx: 'In de eerste en de laatste plaats werkt een accountant voor zijn opdrachtgever, de cliënt. De toegevoegde waarde van de accountant is het geven van zekerheid, het geven van een basis waar anderen op kunnen vertrouwen. Dat geldt ook voor de privacyaanpak. Een organisatie die volgens de richtlijnen van de wet verplicht is om privacy te waarborgen, wil de zekerheid dat zij het netjes gedaan heeft. In bijzondere omstandigheden wil het management bovendien weten hoe het beter kan. Het onderzoek van de accountant is dus in veel gevallen vooral bedoeld om de zekerheid en het vertrouwen van de opdrachtgever te steunen. Naarmate hij dat beter doet en ook nog naar buiten toe zichtbaar kan maken dat de privacybescherming goed gebeurt, zullen derden inclusief de toezichthouder CBP daar goede nota van nemen.'

Natuurlijk is de vraag volgens Hustinx gerechtvaardigd of er voldoende grond is om op de uitkomsten van de controle te vertrouwen. Daarom heeft de toezichthouder samen met de belangrijkste deskundigen uit het werkveld geprobeerd zo scherp mogelijk te omschrijven waarop men moet letten. Hustinx: 'We hebben een standaard-auditmethodiek ontwikkeld. Dat is vorig jaar afgerond met de grote accountantskantoren, met de beroepskoepels NOREA, NIVRA en NOvAA, maar ook met VNO/NCW, en met nog vele andere organisaties. Die audit is de laatste stap in een gelaagde aanpak. De eerste stap bestaat uit een door de organisatie zelf uit te voeren quick scan gevolgd door zelfevaluatie, zelfevaluatie met review en als hoogste trap dus die privacyaudit. Dries Neisingh was vanuit KPMG één van de sturende partners in de stuurgroep.'

Die betrokkenheid van Dries Neisingh kwam onder meer voort uit het feit dat hij al zes jaar geleden als buitengewoon lid van de Registratiekamer heeft geholpen bij het opzetten van proef-privacyaudits. Dat viel samen met het moment waarop de Registratiekamer zelf EDP-auditors in dienst nam. De ervaringen van die proefaudits hebben gediend als basis voor de ontwikkeling van de genoemde gelaagde aanpak, uitmondend in de privacyaudit. Hustinx wijst op de volgende logische stap waarin de standaard-auditmethodiek moet worden opgevolgd door een certificeringsprocedure. 'De uitkomst van dit proces is dat de accountant aan zijn cliënt een certificaat kan uitreiken dat de opdrachtgever garandeert dat hij de verwerking van persoonsgegevens heeft ingericht volgens de richtlijnen in de wet. Dat certificaat betekent voor ons, voor de toezichthouder, dat wij erop kunnen vertrouwen dat het goed zit bij zo'n organisatie. En wat ons betreft moeten ze dat certificaat dan ook maar goed zichtbaar maken in de jaarverslagen, zodat ook de samenleving daarop kan vertrouwen.'

Aangifte doen

Als straks dit certificaat is ingevoerd en wordt uitgereikt aan de eerste organisaties die voldoen aan de richtlijnen, kan de vraag opkomen of organisaties die niet zijn gecertificeerd de wet overtreden. En wat betekent dat voor de positie van de accountant of de EDP-auditor bij zijn cliënt? Hustinx: 'Op het terrein van de Wbp gaat het inderdaad vooral om de vraag of de verwerking van persoonsgegevens voldoet aan de eisen van de wet. De organisatie die de audit laat uitvoeren is hiervoor verantwoordelijk en zeker niet de accountant, die dus ook niet verplicht is om aangifte te doen.'

De accountant is bovendien doorgaans vrijgesteld van de meldingsverplichting die in principe voor iedereen geldt die bezig is met de verwerking van persoonsgegevens. Dit is geregeld in artikel 15 van het Vrijstellingsbesluit Wbp voor juridische dienstverleners en accountants. Er is echter een duidelijk spanningsveld tussen de bescherming van persoonsgegevens aan de ene kant en een forensisch onderzoek door accountants aan de andere kant. Daar zitten dermate grote haken en ogen aan dat Hustinx besluit in het kader van dit interview er niet dieper op in te gaan. 'Dat bewaar ik voor het symposium op 12 november.' Hij wil nog wel kwijt dat accountants bij een forensisch onderzoek dat niet krachtens de wet in opdracht van opsporingsbevoegde autoriteiten plaatsvindt mogelijk wél verplicht kunnen zijn de verwerking van persoonsgegevens te melden bij het College, dat dan vervolgens op zijn beurt verplicht is dit in het Openbaar Register op te nemen. En dat doet het vertrouwelijke karakter van forensische accounting natuurlijk geen goed.

Paradigmashift

Privacyaudits zijn ook zonder certificering al zeer waardevol. Dat is bijvoorbeeld duidelijk gebleken bij de eerste proefaudits, waaraan organisaties die vrijwillig meededen een zeker ontnuchterende ervaring overhielden. Want men dacht redelijk ver te zijn in de processen en systemen die privacy moesten waarborgen, maar dat viel tegen. Zo'n uitkomst is echter in de eerste plaats een opportunity. En zo hebben de deelnemers van toen dat volgens Hustinx ook opgevat. 'Een groot psychiatrisch ziekenhuis is bijvoorbeeld volop aan de slag gegaan met de ontwikkeling van wat nu heet Privacy Enhancing Technology (PET), een techniek die zeer veelbelovend is en recent nog het onderwerp was van een belangrijk seminar dat we als CBP in de Ridderzaal hebben gehouden. De techniek van PET valt buiten de scope van dit artikel, maar ik noem het vooral als effect van het doen van privacyaudits. Momenteel zijn er al tien andere ziekenhuizen die door de inzet van PET niet-geautoriseerde gebruikers van geautomatiseerde systemen afschermen van persoonsgegevens in patiëntendossiers.'

Een dergelijke afscherming lijkt in strijd met het principe van transparantie dat door IT'ers juist zo wordt gehuldigd. Hustinx wijst in dit verband op een mogelijke begripsverwarring.'IT'ers bedoelen met de transparantie van systemen dat bedrijfsapplicaties liefst met open standaarden tot in het oneindige geïntegreerd en gekoppeld zijn. Maar vanuit de privacybescherming bedoelen we met transparantie iets anders, namelijk de wijze waarop organisaties zichtbaar kunnen maken hoe zij omgaan met de verplichtingen in de Wet bescherming persoonsgegevens. Díe transparantie geldt het publiek én de toezichthouder, maar zeker ook de betrokken personen zelf, en is een belangrijk onderwerp bij het auditen. Want wat zichtbaar moet zijn is de wijze waarop met persoonsgegevens wordt omgegaan (bijvoorbeeld welke gegevens worden voor welk doel gebruikt?), en de mate waarin de continuïteit, de integriteit en de exclusiviteit van de systemen geregeld zijn. De laatste component is vanuit het oogpunt van bescherming van persoonsgegevens uiteraard de belangrijkste. Het rapport 'Beveiliging van persoonsgegevens' dat recent nog onder auspiciën van het CBP is gepubliceerd, gaat uitgebreid in op de details van deze exclusiviteitseisen. Dries Neisingh zat trouwens in de commissie van deskundigen en is dus direct betrokken geweest bij het opstellen van dit rapport.'

Een belangrijke conclusie in dit rapport is dat het afschermen of beveiligen van persoonsgebonden materiaal in een gegevensverzameling op basis van zowel technische als organisatorische richtlijnen tot de meest elementaire voorzieningen in de bescherming van per-

soonsgegevens behoort. Zonder het belang van organisatorische richtlijnen te bagatelliseren, geeft Hustinx daarbij volop de voorkeur aan zo robuust mogelijke technische voorzieningen die binnen de geautomatiseerde systemen privacybeschermend werken. En dat vraagt volgens hem in de IT een paradigmashift omdat dit uitgangspunt haaks staat op de zo stevig nagestreefde transparante, open bedrijfsapplicaties die men graag op internettechniek gebaseerd voor iedereen toegankelijk wil maken. Hustinx: 'Ik zou het liefst de Chinese muren van bijvoorbeeld functiescheiding en autorisaties die in de financiële huishouding al jaren gemeengoed zijn, willen overhevelen naar de toepassing van persoonsgebonden gegevensverwerking. Noem het voor mijn part Japanse muren. Als ze er maar komen. Daarom ben ik zo enthousiast over Privacy Enhancing Technology, zoals die in de gezondheidszorg al tot stand is gekomen en waarin dergelijke robuuste technische scheidingen tussen autorisatie en toepassing zijn aangebracht zonder verlies van de functionaliteit van het informatiesysteem. En dat laatste is natuurlijk ook essentieel.'

Bonus

Hoewel privacyaudits zonder certificering dus al hun nut hebben bewezen, is er desondanks een belangrijke reden om toch te streven naar met name de borging van de kwaliteit van de audit en niet in de laatste plaats ook de kwaliteit van de auditor. Hustinx: 'Je moet het effect van certificering als de volgende stap na een privacyaudit onder meer zien in de richting van de concurrentie. Het biedt een onderscheidend vermogen als een organisatie kan zeggen dat zij heeft geïnvesteerd in de bescherming van persoonsgegevens en dat goed heeft geregeld, volgens de wet en met een onafhankelijk certificaat bekrachtigd. Dat is ook een krachtig signaal naar de andere stakeholders van de organisatie en niet in de laatste plaats is dat een belangrijk signaal richting de toezichthouder. Ik denk dat de bonus van onze kant is dat we bij een gecertificeerde organisatie niet als eerste gaan kijken. Al is het nou ook weer geen vrijbrief. Want de kwaliteit van de certificering dient uiteraard op haar beurt ook weer geborgd te zijn en dat is wat we als CBP zullen doen door regelmatige steekproeven. Onze EDP-auditors waren nauw betrokken bij het opzetten van de standaardmethodiek voor de privacyaudit, ze zijn nu intensief bezig met de ontwikkeling van de certificeringssystematiek en gaan straks uiteraard het vervolgtraject van onder meer borging en opleiding mede voor hun rekening nemen.'

Concurrentie

'Overigens is het doen van privacyaudits niet exclusief voorbehouden aan de beroepsgroep van de accountancy, ook al ligt het voor de hand om die koppeling te maken gezien de integratie van persoons- en financiële gegevens in geautomatiseerde systemen. Maar het is heel goed denkbaar dat er een in privacyaudits gespecialiseerde dienstverlener opstaat die naast de accountants deze certificering voor zijn rekening neemt. Er is absoluut geen sprake van een closed shop. Dat was ook één van de voorwaarden van VNO/NCW en MKB Nederland, die willen voorkomen dat deze certificering kostenverhogend zou zijn. In het midden- en kleinbedrijf is men niet gewend aan tarieven van RE's en RA's. Bovendien zijn de grote accountantskantoren evenmin gewend aan de specifieke situatie van het MKB. Daarom spelen AA-accountants een rol in de discussie bij de totstandkoming van de certificering en daarom is het eveneens denkbaar dat de al bestaande, bekende certificeringsorganisaties in dit veld gaan optreden. Als toezichthouder vinden we het belangrijk dat de deskundigheid van de auditors is gewaarborgd, dat de privacyaudit toegevoegde waarde heeft, transparant is en maatschappelijk controleerbaar plaatsvindt. Wij zullen vervolgens toezicht houden op het certificeringstraject, klachten behandelen, steekproefsgewijze controles houden en niet in de laatste plaats onze handhavingsbevoegdheden inzetten als dat nodig is', aldus een niet alleen in het streven naar kwaliteitsborging op het gebied van privacybescherming visionaire maar ook strijdbare voorzitter van het College Bescherming Persoonsgegevens.

Relatie met Dries Neisingh

Peter Hustinx: 'Ik ken Dries al uit de tijd waarin wij beiden optraden op privacycongressen in de tachtiger jaren. Het was hem al vroeg duidelijk dat accountants en EDP-auditors een taak hadden op dit gebied. Vanuit die visie heeft hij ook mede vorm gegeven aan het vakgebied en de ontwikkeling van de privacywetgeving. Daarnaast is Dries vele jaren als buitengewoon lid verbonden geweest aan de Registratiekamer. In die rol heeft hij ook aan de wieg gestaan van het huidige beleid op het terrein van beveiliging en audits. In al deze contacten gaf Dries blijk van een grote inzet en een prettige duidelijkheid, ook als het aankwam op de details van een nieuwe publicatie.'