Het portret[1] – Privacyiconen – Peter Hustinx

“Je moet af en toe even flink op tafel slaan”

Jeroen Terstegge en Koen Versmissen

In januari verliep de tweede zittingstermijn van Peter Hustinx als European Data Protection Supervisor (EDPS). Inmiddels is bekend dat hij nog tot 16 oktober dit jaar in functie zal blijven, zodat de Commissie voldoende tijd heeft om een opvolger te zoeken. Met zijn aanstaande pensionering in zicht voor ons een goed moment om terug te blikken op Peter’s imposante carrière op het gebied van bescherming van persoonsgegevens.

Hoe ben je in het privacyvakgebied beland?

Dat is een lang verhaal, maar je kan het in twee delen opsplitsen. Er was een periode van bijna twintig jaar waar het een onderwerp was dat op mijn bord lag, en daarna de periode van de Registratiekamer, het CBP en de EDPS waarin ik er fulltime mee bezig was. Aanvankelijk was het een toevallig uitvloeisel van mijn studie in de Verenigde Staten, waar ik onder meer in aanraking was gekomen met het hele vroege denken over privacy. Alan Westin had in 1967 al een boek geschreven (*Privacy and Freedom, red.).* Maar tussen 1970 en 1971 studeerde ik bij Arthur Miller, de rechtsgeleerde die een boek had geschreven *The Assault on Privacy* (1971) en daar een workshop over hield. En dat vond ik interessant. Toen ik vervolgens in 1971 op het Ministerie van Justitie kwam waren er net twee aardbevingen geweest op dit terrein: de ene was de volkstelling (1971, *red.*) en de andere was het gedoe rond het CPA-nummer (de Centrale Personen Administratie, *red.)*. Het toenmalige kabinet Biesheuvel had daarom in zijn regeerakkoord opgenomen dat ze iets aan privacy gingen doen en stelde daarvoor de Commissie Koopmans in, waar ik vervolgens adjunct-secretaris van werd. Daardoor snuffelde ik niet alleen in een vroeg stadium aan de eerste contouren van privacywetgeving, maar deed parallel daaraan ook mee aan hetgeen in de Raad van Europa op dit terrein gebeurde (Verdrag 108, *red.*).

Toen eind jaren ’80 het dossier van de Wet Persoonsregistraties gesloten was, ging ik me op het ministerie vooral met straf- en strafprocesrecht en bestuursrecht bezighouden. Maar toen twee jaar later de eerste voorzitter van de Registratiekamer, Klaas de Vries, ontslag nam, werd ik naar voren geschoven. Ik heb me toen afgevraagd of ik dat na twintig jaar wel wilde, maar inmiddels was het me wel duidelijk geworden dat dit onderwerp verregaande consequenties en potentie had en dat het spannend was om daar een rol in te spelen. Daar kwam nog bij dat het in het begin niet alleen ging om de beginselen, zeg maar de inhoud van het recht, maar al heel gauw ook om de vraag welke middelen moesten worden ingezet om het te laten werken. Moest dat via het privaatrecht, het strafrecht of het bestuursrecht? En welke instellingen heb je daar voor nodig? Binnen de Staatscommissie Koopmans werd geopperd om een soort Informatiekamer in te stellen. Door de dereguleringsgolf in die jaren vond ik het boeiend om na te denken

[1] Dit interview is verschenen in "Privacy & Compliance", Tijdschrift voor de praktijk, 01/2014, blz. 4-13.

over een Kamer die niet alleen effectief was, maar ook niet te veel mocht kosten. Daarnaast trok het brede werkterrein: niet alleen justitie, maar ook de gezondheidszorg, telecommunicatie, verkeer, de sociale zekerheid en de bevolkingsboekhouding.

Op 1 juli 1991 ben ik voorzitter geworden van de Registratiekamer. Dat viel samen met het Nederlandse voorzitterschap van de Raad, en toen lag in Brussel het ontwerp van Richtlijn 95/46 op tafel. De Europese Commissie had een Richtlijn voorgesteld met een heel Duits stempel, met een duidelijk onderscheid tussen de private en de publieke sector. Onder het Nederlandse voorzitterschap is toen besloten om het te integreren tot één regeling. Ik was bij die discussie heel nauw betrokken en rolde vervolgens vrij natuurlijk in de rol van de voorzitter van de Artikel 29 Werkgroep. Daarna volgde het voorzitterschap van het CBP en de benoeming tot EDPS.

Je bent ook nauw betrokken geweest bij de Europese beleidsvorming.

In Europees verband speelde vooral de Raad van Europa een belangrijke rol, die dit onderwerp aanvloog vanuit een mensenrechtenagenda. Het ging hun vooral om de rechtsvorming, niet om de economie of de techniek. Men stelde zich wel de vraag hoe technologie zou inwerken op mensenrechten. Men dacht toen al dat technologie een heel vergaande invloed zou hebben. Men vermoedde dat het vraagstuk van bescherming van persoonsgegevens ergens tussen privacy en informatievrijheid in zou liggen. Maar daar stond niets over op papier. Men wilde daarom weten wat nou eigenlijk de beginselen van behoorlijk gebruik van computers zijn. En dat leidde nog voorafgaand aan het Verdrag 108 tot een tweetal aanbevelingen. De eerste ging over de private sector. Daar kwam eigenlijk vrij natuurlijk op papier wat die beginselen zouden moeten zijn. Vervolgens kwam er ook een aanbeveling voor de publieke sector, maar met wat speciale regelingen vanwege de bijzondere positie van de overheid, zoals de politie. Die twee aanbevelingen stonden aan de basis van Verdrag 108. Dat verdrag verplichtte de lidstaten om het verdrag in nationaal recht om te zetten. De Europese Commissie maakte zich toen zorgen vanwege de diversiteit die daaruit voortkwam. De eerste twee jaar van de onderhandelingen over het Verdrag hebben we besteed om de hoofdstructuur van het Verdrag te maken. De rest van de tijd is besteed aan de regeling voor doorgifte van persoonsgegevens (artikel 12), toepasselijk recht en nationale jurisdictie. Die laatste twee hebben het Verdrag overigens niet gehaald, omdat ze op dat moment nog veel te ingewikkeld waren. En dat zijn ze overigens nog steeds.

Toen het Verdrag klaar was, kwam de vraag naar voren wat die algemene beginselen nu precies betekenen op concrete gebieden. Er zijn daarom ook een paar correcties op het verdrag gekomen, zoals het begrip ‘persoonsgegevens’. Aanvankelijk stond daar “makkelijk herleidbaar”, maar dat is geherformuleerd naar een meer neutrale definitie. Het beginsel van de doelbinding was er al heel vroeg. Dat was ook een logisch gevolg van het denken in het Europees Verdrag voor de Rechten van de Mens. Iedere inbreuk op een fundamenteel recht is gebonden aan een doel, maat en wettelijke grondslag. De stap die het databeschermingsrecht maakte, was dat er altijd een wettelijke grondslag moest zijn voor de verwerking van persoonsgegevens, ongeacht de vraag of er sprake is van een inbreuk op een

fundamenteel recht. Daarom vind ik ook dat privacy en dataprotectie wezenlijk twee heel verschillende dingen zijn, hoewel ze elkaar wel overlappen. Het curieuze is dat de consequentie dat dat niet alleen gevolg heeft voor het verzamelen en het bewaren, maar ook op het gebruik – de onverenigbaarheidsgedachte – pas heel laat naar voren kwam. Maar toen kwam meteen ook de twijfel: alleen hetzelfde doel, is dat niet een beetje te strikt? Die term 'onverenigbaar' zat al een beetje in de mensenrechtenjurisprudentie, en ook de Aanwijzingen voor de Rijksdienst, die een vorm van zelfregulering waren voorafgaand aan de WPR, kenden al het beginsel van onverenigbaarheid. De ontwikkeling van de beginselen van dataprotectie kan je daarom het beste vergelijken met een Wiki-proces; in heel Europa waren mensen met elkaar bezig om via een iteratief proces tot formuleringen te komen.

De OESO-principes hebben de tand des tijds redelijk doorstaan. Maar ze worden onder invloed van ontwikkelingen zoals Big Data wel steeds meer ter discussie gesteld.

Natuurlijk herken ik die uitdagingen, maar mij frappeert toch ook de grote continuïteit. Niets is in steen gehouwen, dat zou ook onverantwoord zijn. Maar er is sinds 1980 ongeveer iedere tien jaar een assessment geweest, waaruit bleek dat de beginselen nog steeds zinvol waren. Verder zijn de OESO-principes naar hun inhoud gelijk aan die van de Raad van Europa. Toen de Europese Unie begon met zijn review, hebben ook de OESO en de Raad van Europa besloten om hun richtlijnen c.q. verdrag te herzien. De review van de OESO is in juni 2013 gereed gekomen. Maar als je die nader beschouwt, is het eigenlijk een bevestiging van de oude richtlijnen. Alleen is accountability veel meer benadrukt en wordt er meer gesproken over internationale samenwerking. Die conclusies berusten dus kennelijk op een gemeenschappelijk inzicht. Als je bijvoorbeeld kijkt naar wat president Obama zegt over privacy in de private sector, dan komt hij in essentie op dezelfde uitgangspunten. De Amerikanen noemen dat *reinvigorated FIPS* (Fair Information Principles, *red.*), maar in wezen gaat het om hetzelfde. Maar ik denk dat je de OESO beginselen altijd in een context moet zien en die context is de laatste paar jaar enorm veranderd. Toestemming is bijvoorbeeld in sommige culturen, zoals Duitsland en Oostenrijk, overgeaccentueerd. Aan de andere kant zijn er ook landen die toestemming wel belangrijk vinden, maar waar de uitwerking ervan in de praktijk heel goedkoop is. Daarmee haal je het systeem onderuit.

Het Europese Hof heeft bijvoorbeeld een paar jaar geleden Spanje op de vingers getikt voor het onredelijk beperken van het gerechtvaardigd belang inzake marketing. De keerzijde van de Spaanse benadering was dat je op het internet heel veel gemakkelijke toestemming, of zelfs misbruik van toestemming ziet. Men neemt graag toestemming als rechtvaardigingsgrond, maar wil liever niet nadenken over het geval dat de toestemming wordt geweigerd of ingetrokken. Mijn advies is: als het te belastend is om toestemming te vragen, doe dat dan ook niet. Denk na over de uitvoering van een contract, de nakoming van wettelijke verplichtingen of het gerechtvaardigd belang. In dat laatste geval moet je ook veel meer nadenken over de vraag waarom je denkt dat wat je doet gerechtvaardigd is. De vraag is dan: is mijn default positie die ik aan de betrokkene voorleg wel zo'n goed aanbod? Er is dus iets voor te zeggen om de grond van het gerechtvaardigd belang te versterken met een externe verantwoordingsverplichting.

In het kader van Richtlijn 95/46 is het heel duidelijk dat toestemming slechts *een* rechtvaardigingsgrond is, dus naast de andere rechtvaardigingsgronden die allemaal op hun eigen manier werken. Een evenwichtig systeem moet de ruimte laten voor het gerechtvaardigd belang. In de Opinie over doelbinding (WP 203 van de Artikel 29 Werkgroep, *red.*) zie je die evenwichten werken. In dat rapport gaat het ook over Big Data en Open Data. Ik zal de laatste zijn die zegt dat de toepassing van de privacyprincipes op die ontwikkelingen onproblematisch is, maar ik ben het niet eens met mensen die zeggen dat de principes niet meer passen. Het draagt niet bij aan de helderheid als je zegt dat vanwege de grote hoeveelheid gegevens het alleen nog maar gaat om het gebruik ervan. Het gebruik is de test en daar moet de bescherming dus helemaal sterk zijn, maar ik denk dat je altijd moet beginnen met het perspectief van de verkrijging van de gegevens. Goed data management begint nou eenmaal met het nadenken over het verzamelen van gegevens. Als je dat niet doet, krijg je nooit de goede oplossingen. De beginselen zijn wat mij betreft nog steeds geldig. Met een paar kleine nuances kan je ze gewoon handhaven. Maar je moet bedacht zijn op de evenwichten die erin zitten. In dat perspectief is de verdeling van verantwoordelijkheden rond de toepassing van de beginselen de kernvraag van de discussie. Ik zie de herziening van het Europese privacyrecht dus als een verheldering van de beginselen, vooral ook om te verzekeren dat daar praktische invulling aan wordt gegeven in de betreffende context.

Hoe kijk je terug op je periode als EDPS?

Het was een hele ervaring om van niets iets te maken. Toen ik kwam was er helemaal niets, zelfs geen begroting. Ik vind het de grootste verdienste dat de EDPS er als instelling nu is en allerlei dingen doet. De Verordening waarmee de EDPS wordt ingesteld (45/2001, *red.*), is een soort Europese WBP. Daarin zagen we drie strategische lijnen: 1) het toezicht, 2) de wetgevings- en beleidsadvisering, en 3) het samenwerken met collega-toezichthouders. De eerste hoofdtaak is om ervoor te zorgen dat de Verordening wordt nageleefd door de Europese instellingen. In het begin zag je daar dezelfde weerstand die je ook op nationaal niveau zag (geen prioriteit, geen mensen, etc.). We hebben accountability gebruikt als een mechanisme om ruimte te geven aan de verantwoordelijken, maar wel af te rekenen. We gebruiken ook benchmarking om te laten zien hoe instellingen het ten opzichte van elkaar doen. En je ziet dat ze echt stappen vooruit hebben gemaakt.

Verbetering is natuurlijk altijd mogelijk, maar over het algemeen scoren de meeste heel goed. We gebruiken de benchmark-resultaten ook om *underperforming* zichtbaar te maken. Die instellingen worden door ons met naam en toenaam genoemd. Dat vinden ze natuurlijk niet leuk. Die *underperformers* krijgen van ons speciale aandacht. Ze krijgen van ons bezoek en er wordt een *roadmap* gemaakt voor verbetering, met maandelijkse rapportages. Die toezichtstaak loopt wat mij betreft heel goed.

Je hebt je ook flink tegen de wetgeving in Europa aanbemoeid.

De wetgevings- en beleidsadvisering vond ik strategisch heel belangrijk en die heb ik dus stevig aangezet. Ik vond niet dat ik moest afwachten, maar actief mee moest doen met de dingen die hier in Brussel gebeuren. Dat had ook te maken met mijn

achtergrond. Dat is daarmee onze tweede hoofdtaak geworden. We hebben daarvoor een methodologie. We analyseren ieder jaar de agenda van de Commissie. Die scoren we op relevantie en we zeggen wat wij daar ongeveer van verwachten. En zolang de Commissie nog over zo'n onderwerp nadenkt, zijn wij bereid om daarover te adviseren als de Commissie daarom vraagt. Maar als het voorstel wordt aangenomen, moeten ze het aan ons voorleggen en komt er een openbaar advies. We begonnen met deze methodiek in een periode waarin 9/11 nog niet zo lang geleden was en zeker in de derde pijler (politie- en justitiesamenwerking, *red.)* was privacy toen geen geliefd onderwerp. We hebben desondanks die methodiek over de hele breedte van de beleidsvorming in de aanbieding gezet. En tot mijn grote genoegen hebben de Commissie, het Parlement en de Raad daar al die jaren actief aan meegewerkt. Dat had best anders kunnen zijn.

Je bent soms ook best wel kritisch geweest op bepaalde dossiers.

Je moet ook af en toe even flink op tafel slaan. Niet te vaak, anders denken ze "daar heb je hen weer". Maar dat hebben we in de afgelopen jaren zo'n dozijn keer heel stevig gedaan en dat heeft goed gewerkt. De verordening geeft mij daarnaast ook de mogelijkheid om te interveniëren bij geschillen voor het Hof van Justitie. Volgens juristen was dat een kwestieuze bepaling. Eigenlijk mogen alleen de klassieke instellingen dat doen. Maar toen de zaak van de passagiersgegevens (PNR) voor het Hof kwam, vond ik dat een historische gelegenheid om te interveniëren. En het Hof stond dat toen toe. Volgens het Hof was de EDPS er voor om de naleving te bevorderen over de volle breedte van de wet. En dat heb ik natuurlijk ingelijst. Sindsdien is de advisering in een andere dynamiek komen te staan. Onze adviezen werden serieuzer genomen, juist omdat wij er bij het Hof op terug konden komen. Dat is een ongelofelijke samenloop van omstandigheden geweest.

En de derde taak?

Dat is de samenwerking met collega-toezichthouders. Die is geleidelijk aan gegroeid. Binnen de Artikel 29 Werkgroep ben ik natuurlijk veruit het langstzittende lid. Als je dan met selectiviteit je punten inbrengt, krijg je veel gedaan. Op de meest strategische onderwerpen hebben we onze standpunten ingebracht. Denk bijvoorbeeld aan de privacybeginselen en de BCRs. Ik denk dat dat er mede toe geleid heeft dat de Commissie heeft voorgesteld om de diensten van de EDPS te betrekken bij het werk van de European Data Protection Board (EDPB).

Ben je tevreden over wat je hebt bereikt?

Ja, ik ben redelijk tevreden met wat we als EDPS bereikt hebben. Er zijn natuurlijk ook zaken geweest waar ik minder blij mee was. Neem bijvoorbeeld dataretentie. Daar heb ik negatief over geadviseerd, maar dat is uiteindelijk toch doorgegaan. Maar het is dan wel bevredigend dat het Hof bij de Iers/Oostenrijkse verwijzing, waar ik niet mag interveniëren, ons gevraagd heeft om te komen pleiten. Het is nu even afwachten wat het Hof met ons advies doet. Een ander hoogtepunt vond ik dat de Commissie, nadat ik ze had geadviseerd dat wijziging van Richtlijn 95/46 onvermijdelijk was, met zuchten en steunen dat toch is gaan doen, en ik heb daarna niet nagelaten om aan die herziening een bijdrage te leveren.

Wat is de grootste uitdaging voor je opvolger?

Een aantal dingen zijn nog niet af. Dat geldt uiteraard voor de herziening van het Europese privacykader. Maar er zijn ook risico's. De kritiek neemt ook toe naarmate je jezelf meer in de kijker speelt. Wij zijn geen politieke instelling, maar er wordt soms stevig opgetreden. En dan moet je niet op de verkeerde momenten op de verkeerde plaats zijn. Dat kan je lelijk opbreken. Dat vereist stuurmanskunst.

Het lijkt er bijna op dat jouw succes als EDPS het lastig maakt om een goede opvolger te vinden.

Daar kan ik onmogelijk blij over zijn. Het probleem ligt momenteel op het bord van de Raad en het Parlement. Die beslissen of de procedure doorgaat of dat die afgesloten wordt. Maar uiteindelijk zullen ze wel iemand vinden die het stokje kan overnemen.

Elke Europese instelling moet ten minste één DPO hebben. Werken jullie samen met die DPO?

Ja, we werken veel samen met de DPO's. Drie keer per jaar is er een bijeenkomst met alle DPO's. Daarnaast werken we maandelijks, wekelijks of zelfs dagelijks samen met DPO's, onder andere via e-mails en telefoontjes. Bij alle zaken wordt de DPO in cc gezet. We hebben in een vroeg stadium de DPO's ook gepositioneerd als strategische partner voor de verantwoordelijke. Zo stellen we de DPO ruim van tevoren in kennis van onze activiteiten. Op die manier organiseren we de betrokkenheid van de DPO bij de zaken die hem aangaan. Overigens zie je bijvoorbeeld bij de Commissie dat er twee DPO's zijn, maar daarnaast zijn er ook een stuk of vijfendertig dataprotectie-coördinatoren, in elk DG een. Die 30-40 mensen, waarvan een aantal parttime, zijn de backbone van de accountability-praktijk. We hebben de DPO's voldoende op afstand gehouden om ze naar eigen inzicht te laten functioneren, en voldoende dichtbij om ze te steunen waar het nodig is.

De Verordening vereist allerlei maatregelen die organisaties moeten nemen, zoals het aanstellen van een DPO. Voor andere compliance-onderwerpen gelden vaak niet dat soort specifieke eisen, en dat roept soms weerstand op in organisaties. Hoe zorgt een DPO ervoor dat hij of zij serieus genomen wordt?

Ik vind dat heel herkenbaar. Wij hebben daarom een nota gemaakt over de positionering van DPO's met daarin onderwerpen als onafhankelijkheid van de DPO, DPO als parttime functie en de rapportagelijn van de DPO (hoe hoog in de organisatie?). Daarnaast hebben de DPO's een door mij ondersteunde gedragscode ontwikkeld, waarin staat wat een DPO moet doen als hij net benoemd is, wat zijn prioriteiten moeten zijn, enzovoorts. Een DPO moet *buy in* organiseren. Hij moet een programma maken en daar steun voor verwerven. Dat programma moet gerelateerd zijn aan de missie van de organisatie. De organisatie moet kunnen begrijpen hoe ze er beter van worden. Natuurlijk zijn sommige dingen verplicht, maar een goed privacybeleid kan ook kansen bieden. Een DPO moet dus niet op zijn handen blijven

zitten. Succesvolle DPO's zijn zij die die uitdaging aangaan. Ik denk overigens dat de stelling niet klopt dat er geen gedetailleerde voorschriften zijn bij andere onderwerpen. Kijk bijvoorbeeld naar de regels voor de boekhouding en de regels voor de accountancy die er van oudsher al zijn. Maar ook op nieuwere terreinen zie je vergelijkbare regels. Denk maar aan de boekhouding voor chemische stoffen en emissies. Ook op het terrein van arbeidsomstandigheden bestaan gedetailleerde voorschriften. In beginsel volgt de herziening van de Richtlijn diezelfde gedachte.

Het gaat erom dat compliance in de praktijk wordt vormgegeven. Verantwoordelijkheid is geen definitie maar een actie. En dan kom je uit bij accountability. De term zelf komt niet voor in de Verordening, maar het bedrijfsleven heeft in de afgelopen jaren alle elementen van accountability uitgediept en dan kom je tot dezelfde conclusies: het gaat om *data management*. Ik ben maar ten dele blij met de manier waarop dat in de Verordening is gezet. Sommige zaken heeft de Commissie te ouderwets ingekleurd, zoals bij de bewijsbepaling (de documentatieplicht van art. 28, *red.*). Natuurlijk is er behoefte aan bewijs, maar het is niet nodig dat organisaties op elk moment van de dag een accurate beschrijving hebben van hun verwerkingen. Dat hadden we bij de meldingsplicht. Ik heb geadviseerd om voor te schrijven dat er een methodiek is om de verwerkingen te beheren. Dat kan vervolgens worden gestandaardiseerd en per sector verder worden gespecificeerd. Er wordt nu gewerkt aan een *risk-based approach* om te zorgen dat dat soort verplichtingen wel kunnen werken.

Terecht worden in de Verordening ouderwetse handhavingsverplichtingen weggesneden. De meldingsplicht voor verwerkingen is daar een voorbeeld van. Daar worden nieuwe voor in de plaats gezet, hoewel daarbij niet altijd de juiste schaal wordt betracht. De Commissie had beter de kenmerkende elementen van verantwoordelijkheid kunnen beschrijven, zoals het nemen van maatregelen, de effectiviteit daarvan nagaan en bewijsmiddelen hebben om dit aan te tonen. En dan had kunnen worden omschreven welke maatregelen ten minste moeten worden genomen. De voorschriften zoals die nu in de Verordening staan kunnen verantwoord zijn in één cultuurkring, maar het is zeker dat de uitwerking daarvan in 28 verschillende landen helemaal verschillend zal zijn. Het is dus een uitdaging om eenvormige regels te maken, die vervolgens niet te knellend zijn, maar wel overal passend zijn. Ik geloof dat we op dat punt, met name in de Raad, dichter bij de uitkomst zijn dan doorgaans wordt aangenomen.

Overigens zijn de kosten van de maatregelen naar mijn mening schromelijk overdreven. Er wordt geen rekening gehouden met de baten noch met de frictiekosten. Ook wordt de huidige non-compliance genegeerd. De Commissie heeft de gemoederen wakker geschud door te dreigen met miljoenenboetes. Die zijn natuurlijk schaalbaar, maar vormen niettemin een buitengewoon effectief middel om aandacht te krijgen in de *boardroom*. En dan heb je toezichthouders nodig die daar op een verstandige manier mee omgaan. Dat betekent dat ze de goede praktijken moeten belonen en ook stevig moeten optreden als het fout is. Toezichthouders moeten daarom niet alleen de bevoegdheid hebben om boetes uit te delen, maar ook om een plan van aanpak te vragen en om voortgangsrapportages te vragen, gekoppeld aan sancties om organisaties aan te sporen. Dat kan je echter niet voor de hele economie doen. Een toezichthouder moet dus goed kunnen uitleggen waarom hij handhaaft in een concrete zaak.

De digitale economie is tegenwoordig heel internationaal. Hoe passen we onze Europese privacywaarden in het mondiale speelveld zonder onszelf buitenspel te zetten?

Er is een grote mate van eensgezindheid in de wereld over wat de principes zijn op dit terrein. Kijk naar de nieuwe principes van de OESO. Daar deden nu meer landen aan mee dan de vorige keer en de uitkomst is verrassend hetzelfde. Dat zie ik ook op internationale conferenties. Natuurlijk zijn er verschillen tussen APEC en de EU, maar er zijn ook overeenkomsten. En als het aankomt op uitvoering in de praktijk denk ik dat we een heel eind door dezelfde deur kunnen. Dat geldt ook voor Amerika, ook al is daar een grote terughoudendheid om een stap vooruit te maken. Maar onderschat niet de invloed die Europa op dit terrein heeft gehad en nog steeds heeft.

Dus als wij goed gebruik kunnen maken van het moment, leidt dat de facto tot een wereldnorm met een enorme invloed. Er zijn allerlei manieren om zo'n norm interoperabel te maken tussen de verschillende landen. Een manier is om er van uit te gaan dat bedrijven compliant willen zijn, maar het liefst maar één keer wereldwijd willen implementeren tegen zo laag mogelijke kosten. Die mogelijkheid is er nu. Daarnaast is er nog de formidabele marktmacht van Europa. Ook de Federal Trade Commission in Amerika is veel actiever geworden op het terrein van privacybescherming. In Amerika wordt het niet-naleven van privacybeleid, anders dan in Europa, gezien als een onredelijke handelspraktijk, maar daar komen ze een heel eind mee. De FTC heeft zich in een aantal zaken bereid getoond om iets wat in Europa beloofd is, maar niet geleverd, via de Amerikaanse band te voorzien van een sanctie. Dat hebben ze niet toevallig gedaan.

Er is dus een toenemende bereidheid om samen te werken met Europa. In het licht van de trans-Atlantische markt is dat een formidabele bijdrage aan de interoperabiliteit. Ik heb bij gelegenheid het Europese systeem van *adequacy* neergezet als een bijdrage aan de interoperabiliteit. We staan aan de vooravond van een aantal stevige ontwikkelingen. Kijk bijvoorbeeld naar Google, dat nu in verschillende landen voorwerp is van onderzoek. Dat leidt waarschijnlijk ook tot jurisprudentie en dat is ook noodzakelijk omdat onze wereld steeds meer geïntegreerd raakt.

Hoe moet een compliance officer met die wereldwijde verschillen omgaan?

De DPO kan ervoor zorgen dat hij in de context van zijn organisatie een agenda ontwikkelt waarin dit soort dingen systematisch worden benoemd. De DPO moet de (wereldwijde) eisen dus zien te vertalen naar de producten en diensten van zijn bedrijf. Waar nodig zullen uiteraard kleine verschillen te zien zijn tussen landen en markten, maar het moet wel een geïntegreerde benadering zijn. Als je in een organisatie werkt waarvoor het belangrijk is dat er netjes met persoonsgegevens wordt omgegaan en die niet het risico wil lopen op negatieve publiciteit door een datalek of een handhavingsactie, dan moet je daar dus in investeren. Als de handhavingsactiviteiten toenemen, dan wordt die geïntegreerde benadering alleen maar belangrijker en dat zou een gezonde ontwikkeling zijn.

En hoe moet een toezichthouder met die complexiteit omgaan?

Het is de taak van de verantwoordelijke om de regels na te leven. En het is de taak van de betrokkenen om hun rechten uit te oefenen. Voor de toezichthouder is het dus belangrijk dat het systeem door de bank genomen goed werkt. Als het systeem ergens hapert, moet je daar als toezichthouder wat mee doen. Dat geldt ook als partijen zich structureel misdragen. De toezichthouder moet zich dus niet al te veel met klein grut bezighouden, maar klein grut moet wel bediend worden. Daar moet dus wel een loket voor zijn, eventueel ergens anders.

De uitdaging voor de toezichthouder is om zich te blijven richten op het grote plaatje en dan op tijd in te grijpen. Je moet je als toezichthouder niet in een tunnel laten vangen, omdat je het zo druk hebt met de dagelijkse zaken zoals klachten, meldingen enzovoorts. Je moet je als toezichthouder steeds blijven afvragen of je wel met de goede dingen bezig bent, of je je schaarse middelen wel effectief inzet.

De toezichthouders pleiten voor meer accountability, maar leggen in de praktijk wel nog vaak zout op slakken en geven geen credit voor hetgeen al gebeurt in organisaties op het gebied van privacy management. Gaat het de toezichthouders lukken om die omslag te maken?

Ik hoop het. Een aantal doen dat al. Daar gaat zo'n European Data Protection Board ook bij helpen. Uiteindelijk zal het steeds consistenter worden, maar het is een groeiproces. Als EDPS werken we al op die manier. We kijken waar de grote risico's zitten bij de verantwoordelijke, zoals inhoud van de informatie en het gebruik ervan. Waar is het door de bank genomen goed genoeg, en waar moeten we bovenop zitten omdat de risico's te groot zijn?

Momenteel zijn de one-stop shop gedachte en het proximity-beginsel een groot obstakel voor de voortgang van de Verordening. Maar het is niet onbelangrijk dat daar een goede oplossing voorkomt, ook niet vanuit het perspectief van de DPO die de organisatie moet adviseren over de regels en de risico's. Hoe kijk je daar tegen aan?

De one-stop-shop-gedachte en het proximity-beginsel staan inderdaad op gespannen voet met elkaar. Dit is het onderwerp waar momenteel omheen wordt gedraaid en waarop het slagen of falen van het herzieningsproject in dit stadium hangt. In oktober waren we denk ik dichterbij de oplossing dan in december. De onderwerpen moeten niet los van elkaar worden gezien. De one-stop-shop is een prima concept, maar je moet inzien dat er een one-stop-shop voor bedrijven is én een one-stop-shop voor betrokkenen. En aangezien die in grensoverschrijdende situaties verschillend zijn, moet je accepteren dat er nooit één loket is. De Lead Authority is niet exclusief bevoegd. Je moet het dus zien als een vorm van taakverdeling. Als de Lead Authority wordt gezien als de leider van een team, ben je veel dichter bij de oplossing. En dat geldt omgekeerd ook. Het probleem is wat mij betreft dus zeker oplosbaar.

Maar gaat het uiteindelijk niet gewoon om geld? Je wil niet dat

ieder land afzonderlijk een boete kan opleggen, maar je krijgt scheve ogen als de hele boete naar één land gaat.

Zelfs daar zou je nog wat aan kunnen doen. Als je het idee van samenwerking consequent doorvoert, dan zou je zelfs nog kunnen regelen dat zo'n boete van 100 miljoen tussen de betrokken landen verdeeld wordt. Dat staat nu niet in de Verordening, maar als je dit probleem moet oplossen, is dat de methode. Maar belangrijker is dat we ons afvragen wat de one-stop-shop nou eigenlijk is. Enerzijds heeft een toezichthouder onder de one-stop-shop een taak; anderzijds heeft hij bepaalde bevoegdheden die daar niet op aansluiten. De Franse toezichthouder kan nou eenmaal geen onderzoek ter plaatse doen in Duitsland. In dat geval moet de Franse toezichthouder zijn Duitse collega om medewerking vragen. En dan heb je al een samenwerking op het terrein van onderzoek. Ook bij het afdwingen van verplichtingen kan worden samengewerkt. In de Verordening wordt onder de one-stop-shop dus eigenlijk een vorm van samenwerking opgetuigd. En dat is ook de oplossing voor proximiteit. Daar speelt ook vertrouwen een rol tussen rechters onderling en toezichthouders onderling. De verantwoordelijke hoeft niet altijd lang te wachten op een beslissing.

In de EDPB kunnen we proberen om een zaak te versnellen. Zo zou de EDPB kunnen proberen om binnen een half jaar tot een standpunt te komen waar iedereen zich aan houdt. Ik begrijp dat in het internettijdperk een half jaar een eeuwigheid is, maar het gaat dan om zulke belangrijke zaken dat zo'n termijn wel gerechtvaardigd is. Het mooie van het voorstel was dat het de procedurele *triggers* had om te zorgen dat aan de basis goed werd beslist. En een toezichthouder die afwijkt van het standpunt van de EDPB moet uitleggen waarom hij daarvan afwijkt. Een rechter zal het daar niet gauw mee eens zijn. Tegelijkertijd loste ons voorstel ook een ander probleem op, namelijk dat de Commissie zich zelf een te grote rol had gegeven waar iedereen op tegen was. Die oplossing lag in oktober vorig jaar op tafel, maar daarna is er teveel versplintering geweest in de beeldvorming, waardoor er in december geen akkoord kon worden bereikt. Er zijn allerlei oplossingen mogelijk voor dit probleem zonder dat je komt tot een nieuw orgaan (een pan-Europese toezichthouder, *red.*) waar eigenlijk niemand aan wil. De paradox is dus oplosbaar.

Een half jaar is wellicht acceptabel in geval van een onderzoek of een klacht, maar het consistency mechanisme gaat ook gelden voor de consultatie van de toezichthouder voor projecten van de verantwoordelijke waarop een PIA is gedaan. En dan zijn zes maanden wel heel lang.

In zo'n project moet men natuurlijk wel realistische termijnen hanteren. Een bedrijf moet niet denken dat ze een goed idee hebben en dan om vijf voor twaalf nog even een stempeltje gaan halen. Dan is het belangrijk dat je goede adviseurs hebt die tijdig aan de bel kunnen trekken. Het is overigens waarschijnlijk dat de dingen die voor de hand liggen en toch wel aan de orde komen al tijdens de overgangstermijn van de Verordening het eerst door het consistency mechanisme gaan. Op het moment dat de Verordening is werking treedt, zullen er dus al richtlijnen zijn en geverifieerd beleid op de meest voorkomende onderwerpen. Als een bedrijf dus met een niet al te gekke vraag komt, zal er redelijk snel een antwoord kunnen worden gegeven. Ook op dat punt zal je geleidelijkheid zien. Maar als je dat op Europees

niveau doet, moet je dat wel met de juiste maatvoering doen.

Dus de werking van de Verordening kan toch nog verschillen tussen de landen?

Commissaris Reding noemt de Verordening “één wet overal”. Ik zou het “één kaderwet overal” willen noemen. Het is een Verordening geworden met een groot aantal open plekken op belangrijke terreinen. En dat is nodig omdat je de wetten van al die 28 Lidstaten moet laten samenwerken met de Verordening. In een dogmatische benadering kan dat niet. Een verordening is volgens het Europese recht zeer dominant. Maar het hangt af van hetgeen die verordening zegt. Als die verordening zo is gemaakt dat die co-existentie mogelijk maakt, dan is er geen probleem. Daar werkt de Raad op dit moment aan. In de Verordening staat “wettelijke verplichtingen”, maar er staat niet welke wettelijke verplichtingen. Denk bijvoorbeeld aan de belastingwetgeving of de arbowetgeving. Die staan bol van de wettelijke verplichtingen rondom de verwerking van persoonsgegevens. En als die verplichtingen verenigbaar zijn met de grondrechten, dan zijn het wettelijke verplichtingen in de zin van de Verordening. Die kan je dus samen laten lopen. Maar de Lidstaten moeten wel op de Verordening anticiperen, anders is het juridische gevolg dat al die lokale wetgeving door de inwerkingtreding van de Verordening terzijde wordt gesteld. En dat wil niemand, dus daar moet je gedetailleerd over nadenken. Ik denk dat de Commissie dat een beetje onderschat heeft.

Alles overziend, wat voor boodschap zou je nog aan onze lezers willen meegeven?

Laat ik beginnen met te zeggen dat privacy professionals als zodanig een groeifonds zijn en een hele strategische rol gaan spelen in het systeem. Op alle lagen zullen we die privacy professionals nodig hebben. En dan niet alleen juristen, maar we zullen ook mensen nodig hebben met een technische achtergrond of met managementvaardigheden.

Ten tweede moeten ze niet op hun handen blijven zitten, maar het risico is dat je in je eentje gaat proberen een ijsberg uit het water te tillen. Dat lukt natuurlijk niet en dus zal je een plan moeten bedenken waardoor er geleidelijk aan toch verandering in komt. Daar zal je geduld voor moeten opbrengen en enige verbeeldingskracht moeten tonen. Laat het een troost zijn dat dat precies was wat ik moest doen, toen ik hier als EDPS met niks begon. Het feit dat we zijn waar we nu zijn, laat zien dat het kan. En als je ook nog de nodige dosis geluk hebt, kan je dat met een heel team enthousiast blijven doen.

Het derde punt is dat die vernieuwing van het Europese kader denk ik een onvermijdelijkheid is. De datum waarop dat de eindstreep haalt, is op dit moment niet duidelijk. Laten we eerlijk zijn, dat redden we niet meer voor de Europese verkiezingen. Het eindproduct zal ook niet zijn zoals het ingediend is, maar wel iets wat daar heel veel op lijkt en beter is. We trekken op dit moment meer dan één been bij, en dat is maar goed ook. Heel veel mensen realiseren zich niet de kwetsbaarheid en de grote normatieve vragen die daaromheen zitten.

En ten slotte nog dit: we zijn als toezichthouders momenteel bezig bruggen te slaan tussen de conventionele privacy professionals en al die mensen die bezig zijn met internet, software, hardware en standaarden ontwikkelen. Die mensen hebben door de NSA-affaire ook schokken opgelopen. We gaan een aantal mensen die in de wereld van '*privacy-aware internet development*' actief zijn erbij betrekken om te proberen een multipliereffect te bereiken. En dat laat zien dat ook toezichthouders creatief moeten zijn.