Das Porträt[1] - Datenschutz-Ikone - Peter Hustinx

„Ab und zu muss man mal kräftig auf den Tisch hauen“

Jeroen Terstegge und Koen Versmissen

Im Januar lief die zweite Amtszeit von Peter Hustinx als Europäischer Datenschutzbeauftragter (EDSB) aus. Inzwischen ist bekannt, dass er noch bis 16. Oktober dieses Jahres im Amt bleiben wird, damit der Kommission für die Suche eines Nachfolgers ausreichend Zeit zur Verfügung steht. Mit Blick auf seine bevorstehende Pensionierung ist dies für uns ein guter Zeitpunkt, einmal auf Peter Hustinxs beeindruckende Karriere im Bereich des Schutzes personenbezogener Daten zurückzublicken.

Wie sind Sie im Bereich Datenschutz gelandet?

Das ist eine lange Geschichte, aber sie lässt sich in zwei Teile aufteilen. Über einen Zeitraum von fast zwanzig Jahren lag dieses Thema mit andere bei mir auf dem Tisch, dann kam die Zeit der Datenschutzbehörden Registratiekamer und CBP und des EDSB, in der ich mich ausschließlich damit beschäftigt habe. Anfangs war es eine zufällige Folge meines Studiums in den USA, wo ich unter anderem mit den ganz frühen Gedanken zum Datenschutz in Berührung gekommen war. Alan Westin hatte bereits 1967 ein Buch geschrieben (*Privacy and Freedom, Anm. d. Red.).* Zwischen 1970 und 1971 studierte ich jedoch bei Arthur Miller, dem Juristen, der das Buch *The Assault on Privacy* (1971) verfasst hatte und darüber einen Workshop abhielt. Und das fand ich interessant. Als ich dann 1971 ins Justizministerium kam, hatte es auf diesem Gebiet gerade zwei Erdbeben gegeben: Das eine war die Volkszählung (1971, *Anm. d. Red.*), das andere der Wirbel um die CPA-Nummer (die zentrale Personenverwaltung, *Anm. d. Red.)*. Die damalige Regierung Biesheuvel hatte daher in ihre Koalitionsvereinbarung aufgenommen, sich für den Datenschutz einzusetzen, und richtete zu diesem Zweck die Koopmans-Kommission ein, deren stellvertretender Sekretär ich dann wurde. Dadurch kam ich nicht nur in einem frühen Stadium mit den ersten Umrissen einer Datenschutzgesetzgebung in Kontakt, sondern wirkte parallel dazu auch an den Arbeiten im Europarat auf diesem Gebiet mit (Übereinkommen 108, *Anm. d. Red.*).

Als Ende der 1980er Jahre das Dossier des Personenregistrierungsgesetzes, des „Wet Persoonsregistraties“, geschlossen war, beschäftigte ich mich im Ministerium vor allem mit dem Straf- und Strafprozessrecht und dem Verwaltungsrecht. Als dann aber zwei Jahre später der erste Vorsitzende der Registratiekamer, Klaas de Vries, abdankte, sollte ich diesen Posten übernehmen. Ich habe mich dann gefragt, ob ich das nach zwanzig Jahren wirklich wollte, aber inzwischen war mir doch klar geworden, dass dieses Thema weitreichende Konsequenzen und Potenzial hatte und dass es spannend war, hier eine Rolle zu spielen. Hinzu kam, dass es zu Beginn nicht nur um die Grundsätze ging, sagen wir den Inhalt des Rechts, sondern sehr schnell auch um die Frage, welche Mittel eingesetzt werden mussten, um dem Recht zur Durchsetzung zu verhelfen. Sollte dies über das Zivilrecht, das Strafrecht oder

[1] Dieses Interview ist erschienen in „Privacy & Compliance“, Tijdschrift voor de Praktijk, 01/2014, S. 4-13.

das Verwaltungsrecht geschehen? Und welche Einrichtungen sind dazu erforderlich? Aus der staatlichen Koopmans-Kommission kam der Vorschlag, eine Art Informationskammer einzurichten. Durch die Deregulierungswelle in diesen Jahren fand ich es spannend, über eine Kammer nachzudenken, die nicht nur effektiv war, sondern auch nicht zu viel kosten durfte. Daneben lockte das umfassende Arbeitsgebiet: nicht nur Justiz, sondern auch Gesundheitswesen, Telekommunikation, Verkehr, soziale Sicherheit und Bevölkerungsverwaltung.

Am 1. Juli 1991 wurde ich Vorsitzender der Datenschutzbehörde Registratiekamer. Zeitgleich hatten die Niederlande den Ratsvorsitz inne, und in Brüssel lag der Entwurf der Richtlinie 95/46 auf dem Tisch. Die Europäische Kommission hatte eine sehr deutsch geprägte Richtlinie vorgelegt, mit einer deutlichen Unterscheidung zwischen dem privaten und dem öffentlichen Sektor. Unter dem niederländischen Ratsvorsitz wurde beschlossen, dies in eine einzige Rechtsvorschrift zu integrieren. Ich war sehr eng in diese Diskussion einbezogen und rutschte dann quasi wie von selbst in die Rolle des Vorsitzenden der Artikel-29-Datenschutzgruppe. Dann folgten der Vorsitz der CBP und die Ernennung zum EDSB.

Sie waren auch eng an der Entwicklung europäischer politischer Maßnahmen beteiligt.

Im europäischen Kontext spielte insbesondere der Europarat eine wichtige Rolle, der dieses Thema vom Gesichtspunkt der Menschenrechte aus anging. Es ging ihm vor allem um die Entwicklung eines Rechts, nicht um Wirtschaft oder Technik. Man stellte sich aber die Frage, wie sich Technologie auf die Menschenrechte auswirken würde. Man dachte seinerzeit bereits, dass die Technologie einen sehr weitreichenden Einfluss haben würde. Es wurde vermutet, dass die Frage des Schutzes personenbezogener Daten irgendwo zwischen Schutz der Privatsphäre und Informationsfreiheit anzusiedeln wäre. Es gab hierzu jedoch keinerlei Studien. Darum wollte man wissen, was nun eigentlich die Grundsätze einer ordnungsgemäßen Nutzung von Computern sind. Dies führte noch vor dem Übereinkommen 108 zu zwei Empfehlungen. Die erste betraf den privaten Sektor. Hier ließen sich diese Grundsätze im Grunde recht einfach formulieren. Anschließend kam noch eine Empfehlung für den öffentlichen Sektor, jedoch mit etwas spezielleren Regelungen aufgrund der besonderen Position des Staates, beispielsweise der Polizei. Diese zwei Empfehlungen lagen dem Übereinkommen 108 zugrunde. Dieses Übereinkommen verpflichtete die Mitgliedstaaten, das Übereinkommen in nationales Recht umzusetzen. Die Europäische Kommission machte sich dann Gedanken wegen der sich daraus ergebenden Vielfalt an Rechtsvorschriften. Die ersten zwei Jahre der Verhandlungen über das Übereinkommen haben wir darauf verwendet, die Hauptstruktur des Übereinkommens auszuarbeiten. Die restliche Zeit wurde der Regelung für die Weitergabe personenbezogener Daten (Artikel 12), dem anwendbaren Recht und der nationalen Gerichtsbarkeit gewidmet. Die letzten beiden Aspekte wurden übrigens nicht Gegenstand des Übereinkommens, da sie zu dem Zeitpunkt noch viel zu kompliziert waren. Und das sind sie übrigens immer noch.

Als das Übereinkommen abgeschlossen war, kam die Frage auf, was diese allgemeinen Grundsätze in konkreten Bereichen nun genau bedeuten. Daher wurden einige Korrekturen am Übereinkommen vorgenommen, wie der Begriff

„personenbezogene Daten“. Anfangs stand hier „leicht identifizierbar“, dies wurde jedoch in eine neutralere Begriffsbestimmung umformuliert. Der Grundsatz der Zweckbindung bestand schon zu einem sehr frühen Zeitpunkt. Dies war auch eine logische Folge der Herangehensweise aus der Perspektive der Europäischen Menschenrechtskonvention. Jeder Verstoß gegen ein Grundrecht ist an einen Zweck, ein Maß und eine Rechtsgrundlage gebunden. Der Schritt, den das Datenschutzrecht machte, bestand darin, dass es immer eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten geben muss, ungeachtet der Frage, ob es sich um einen Verstoß gegen ein Grundrecht handelt. Daher sind der Schutz der Privatsphäre und der Datenschutz meines Erachtens dem Wesen nach zwei völlig verschiedene Dinge, auch wenn sie sich überschneiden. Das Merkwürdige ist, dass die Konsequenz, dass dies nicht nur Folgen für die Erhebung und Aufbewahrung hat, sondern auch für die Nutzung – der Unvereinbarkeitsgedanke –, sich erst sehr spät gezeigt hat. Aber dann kamen auch sofort die Zweifel: Nur derselbe Zweck, ist das nicht ein bisschen zu strikt? Dieser Begriff „unvereinbar“ war bereits Teil der Rechtsprechung im Bereich der Menschenrechte, und auch in den Anweisungen für die staatlichen Behörden, die eine Art der Selbstregulierung waren, bevor das Gesetz über die Personenregistrierung, das WPR, kam, gab es bereits den Grundsatz der Unvereinbarkeit. Die Entwicklung der Grundsätze des Datenschutzes kann man daher am besten mit einem Wiki-Prozess vergleichen; in ganz Europa waren Menschen gemeinsam damit beschäftigt, über einen iterativen Prozess Formulierungen zu erarbeiten.

Die OECD-Grundsätze haben dem Zahn der Zeit recht gut standgehalten. Unter dem Einfluss der Entwicklungen wie Big Data werden sie jedoch immer mehr in Frage gestellt.

Natürlich erkenne ich diese Herausforderungen, mich überrascht aber dennoch auch die große Kontinuität. Nichts ist in Stein gemeißelt, das wäre auch unverantwortlich. Aber seit 1980 hat es ungefähr alle zehn Jahre eine Bewertung gegeben, die zu dem Schluss gelangte, dass die Grundsätze noch immer sinnvoll waren. Außerdem sind die OECD-Grundsätze inhaltlich identisch mit denen des Europarats. Als die Europäische Union mit ihrer Review begann, haben auch die OECD und der Europarat beschlossen, ihre Richtlinien bzw. ihr Übereinkommen zu überarbeiten. Die OECD schloss ihre Überarbeitung im Juni 2013 ab. Wenn man sie jedoch näher betrachtet, ist sie im Grunde eine Bestätigung der alten Richtlinien. Nur wird die Accountability, die Rechenschaftspflicht, stärker herausgestellt und es wird mehr über internationale Zusammenarbeit gesprochen. Diese Schlussfolgerungen beruhen somit offenbar auf einer gemeinsamen Einsicht. Wenn man sich beispielsweise anschaut, was Präsident Obama zum Schutz der Privatsphäre im privaten Sektor sagt, so gelangt er im Wesentlichen zu denselben Ausgangspunkten. Die Amerikaner bezeichnen dies als *reinvigorated FIPS* (Fair Information Principles, *Anm. d. Red.*), dem Wesen nach geht es jedoch um dasselbe. Meines Erachtens muss man aber die OECD-Grundsätze immer in einem Kontext sehen, und dieser Kontext hat sich in den vergangenen Jahren enorm verändert. In manchen Kulturen, wie Deutschland und Österreich, wurde beispielsweise übergroßer Nachdruck auf die Einwilligung gelegt. Auf der anderen Seite gibt es auch Länder, die Einwilligung zwar wichtig finden, die Ausarbeitung in der Praxis jedoch eher lasch handhaben. Damit unterminiert man das System.

Der Europäische Gerichtshof hat beispielsweise vor ein paar Jahren Spanien für die unangemessene Beschränkung des berechtigten Interesses in Sachen Marketing auf die Finger geklopft. Die Kehrseite des spanischen Ansatzes war, dass man im Internet sehr viel einfache Einwilligung, oder sogar Missbrauch der Einwilligung, sieht. Man benutzt die Einwilligung gerne als Rechtfertigungsgrund, möchte aber lieber nicht über den Fall nachdenken, dass die Einwilligung verweigert oder zurückgenommen wird. Meine Empfehlung lautet: Wenn es zu schwierig ist, die Einwilligung einzuholen, dann sollte man es auch nicht tun. Man sollte über die Durchführung eines Vertrags nachdenken, die Beachtung gesetzlicher Pflichten oder das berechtigte Interesse. Im letzteren Falle muss man auch viel mehr über die Frage nachdenken, weshalb man denkt, dass das, was man tut, berechtigt ist. Die Frage ist dann: Ist meine Standardposition, die ich dem Betreffenden vorlege, wirklich so ein gutes Angebot? Es gibt also Argumente dafür, den Grund des berechtigten Interesses mit einer externen Verantwortungspflicht zu verstärken.

Im Rahmen der Richtlinie 95/46 wird es ganz deutlich, dass die Einwilligung nur *ein* Rechtfertigungsgrund ist, also neben den anderen Rechtfertigungsgründen, die alle auf ihre eigene Art und Weise funktionieren. Ein ausgewogenes System muss den Spielraum für das berechtigte Interesse lassen. In der Stellungnahme zur Zweckbindung (WP 203 der Artikel 29-Datenschutzgruppe, *Anm. d. Red.*) sieht man, wie diese Gleichgewichte funktionieren. In diesem Bericht geht es auch um Big Data und Open Data. Ich bin der Letzte, der sagt, dass die Anwendung der Datenschutzgrundsätze auf diese Entwicklungen unproblematisch ist, aber der Meinung, diese Grundsätze seien nicht mehr passend, kann ich mich nicht anschließen. Zu sagen, aufgrund der großen Menge von Daten gehe es nur noch um deren Verwendung, trägt nicht zur Klarheit bei. Die Verwendung ist der Test, und hier muss der Schutz also ganz stark sein, aber ich denke, dass man immer aus der Perspektive heraus beginnen muss, wie die Daten erhalten wurden. Gutes Datenmanagement beginnt nun einmal mit dem Nachdenken über die Erhebung von Daten. Wenn man das nicht tut, gelangt man niemals zu den guten Lösungen. Die Grundsätze sind nach meinem Dafürhalten noch immer gültig. Mit ein paar kleinen Nuancen kann man sie einfach beibehalten. Man muss jedoch auf die Gleichgewichte, die sich darin befinden, bedacht sein. In dieser Hinsicht ist die Verteilung der Verantwortlichkeiten im Zusammenhang mit der Anwendung der Grundsätze die Kernfrage der Diskussion. Ich sehe die Überarbeitung des europäischen Datenschutzrechts daher als eine Verdeutlichung der Grundsätze, insbesondere um sicherzustellen, dass diese im betreffenden Kontext praktisch umgesetzt werden.

Wie blicken Sie zurück auf Ihre Zeit als EDSB?

Es war eine Erfahrung, aus nichts etwas zu machen. Als ich kam, gab es überhaupt nichts, noch nicht einmal einen Haushalt. Ich halte es für das größte Verdienst, dass es den EDSB als Einrichtung nun gibt und er vieles tut. Die Verordnung zur Einsetzung des EDSB (45/2001, *Anm. d. Red.*) ist eine Art europäisches Datenschutzgesetz. Darin sahen wir drei strategische Linien: 1) die Aufsicht, 2) die Beratung in legislativen und politischen Angelegenheiten und 3) die Zusammenarbeit mit Amtskollegen. Die erste Hauptaufgabe besteht darin, dafür zu sorgen, dass die Verordnung von den EU-Organen und -Einrichtungen eingehalten wird. Zu Beginn

sah man hier denselben Widerstand wie auf einzelstaatlicher Ebene (keine Priorität, kein Personal usw.). Wir haben die Accountability als Mechanismus eingesetzt, um den Verantwortlichen zwar Spielraum zu geben, sie aber doch zur Rechenschaft zu ziehen. Wir benutzen auch Benchmarking, um die Leistungen der Organe und Einrichtungen einander gegenüberzustellen. Und man sieht, dass sie wirklich Fortschritte gemacht haben.

Eine Verbesserung ist natürlich immer möglich, aber im Allgemeinen erzielen die meisten sehr gute Ergebnisse. Wir verwenden die Benchmark-Ergebnisse auch, um *unterdurchschnittliche Leistungen* sichtbar zu machen. Diese Organe und Einrichtungen werden von uns namentlich genannt. Das gefällt ihnen natürlich nicht. Diese *Underperformer* erhalten von uns besondere Aufmerksamkeit. Wir besuchen sie und es wird eine *Roadmap* für Verbesserungen erstellt, mit monatlichen Berichten. Diese Aufsicht läuft meines Erachtens sehr gut.

Sie haben sich auch stark in die Gesetzgebung in Europa eingemischt.

Die Beratung in legislativen und politischen Angelegenheiten hielt ich strategisch für sehr wichtig, daher habe ich sie kräftig vorangetrieben. Ich war der Ansicht, dass ich nicht abwarten, sondern mich vielmehr aktiv an den Dingen, die hier in Brüssel geschehen, beteiligen sollte. Das hing auch mit meinem Hintergrund zusammen. So ist dies unsere zweite Hauptaufgabe geworden. Wir haben dafür eine bestimmte Methodik. Wir analysieren jedes Jahr die Agenda der Kommission. Wir bewerten sie auf ihre Relevanz und sagen, was wir ungefähr davon erwarten. Und solange die Kommission noch über so ein Thema nachdenkt, sind wir bereit, beratend tätig zu werden, wenn die Kommission uns darum ersucht. Aber wenn der Vorschlag angenommen wird, muss sie ihn uns vorlegen und es folgt eine öffentliche Stellungnahme. Wir haben mit dieser Methodik in einer Zeit begonnen, in der 9/11 noch nicht so lange zurücklag, insbesondere in der dritten Säule (polizeiliche und justizielle Zusammenarbeit, *Anm. d. Red.*) war Datenschutz damals kein beliebtes Thema. Wir haben diese Methodik dennoch über die ganze Bandbreite der Entwicklung politischer Maßnahmen angeboten. Und zu meiner großen Freude haben die Kommission, das Parlament und der Rat all die Jahre aktiv daran mitgearbeitet. Das hätte auch anders laufen können.

Sie sind manchmal in bestimmten Angelegenheiten auch recht kritisch gewesen.

Ab und zu muss man mal kräftig auf den Tisch hauen. Nicht zu oft, sonst denken sie „die schon wieder“. Aber in den letzten Jahren haben wir das ungefähr ein Dutzend Mal mit Nachdruck gemacht, und es hat gut funktioniert. Die Verordnung gibt mir außerdem auch die Möglichkeit, bei Streitigkeiten vor dem Europäischen Gerichtshof zu intervenieren. Juristen zufolge war dies eine strittige Bestimmung. Eigentlich sind nur die klassischen Organe dazu berechtigt. Als aber die Sache der Passagierdaten (PNR) vor den EuGH kam, hielt ich dies für eine historische Gelegenheit zu intervenieren. Und der EuGH ließ dies damals zu. Dem EuGH zufolge sei es Aufgabe des EDSB, die Beachtung des Datenschutzes in der ganzen Breite des Gesetzes zu fördern. Und diese Gelegenheit habe ich natürlich genutzt. Seitdem hat die Beratung eine andere Dynamik erhalten. Unsere Empfehlungen werden ernster genommen, gerade weil wir vor dem EuGH auftreten konnten. Das war ein wirklich unglaubliches

Zusammentreffen von Umständen.

Und die dritte Aufgabe?

Das ist die Zusammenarbeit mit Amtskollegen. Sie ist allmählich gewachsen. In der Artikel-29-Datenschutzgruppe bin ich natürlich das bei weitem dienstälteste Mitglied. Wenn man dann seine Punkte selektiv einbringt, kann man viel erreichen. Wir haben unsere Standpunkte zu den strategisch wichtigsten Themen eingebracht. Beispielsweise zu den Datenschutzgrundsätzen und den BCR. Ich denke, dass dies mit zu dem Vorschlag der Kommission geführt hat, die Dienste des EDSB in die Arbeit des Europäischen Datenschutzausschusses (EDSA) einzubeziehen.

Sind Sie zufrieden mit dem, was Sie erreicht haben?

Ja, ich bin mit dem, was wir als EDSB erreicht haben, ziemlich zufrieden. Es hat natürlich auch Dinge gegeben, über die ich weniger glücklich war, beispielsweise die Datenvorratsspeicherung. Meine Stellungnahme diesbezüglich war negativ, aber letzten Endes wurde sie doch genehmigt. Es ist dann aber doch befriedigend, dass der EuGH uns bei der irischen/österreichischen Verweisung, bei der ich nicht intervenieren darf, ersucht hat, ein Plädoyer zu halten. Jetzt müssen wir abwarten, was der EuGH mit unserer Stellungnahme macht. Ein anderer Höhepunkt war in meinen Augen, dass die Kommission, nachdem ich sie dahingehend beraten hatte, dass eine Änderung der Richtlinie 95/46 unvermeidlich war, diese widerwillig doch noch gemacht hat, und ich habe es anschließend nicht versäumt, einen Beitrag zu dieser Überarbeitung zu liefern.

Was ist die größte Herausforderung für Ihren Nachfolger?

Einige Dinge sind noch nicht abgeschlossen. Das gilt natürlich für die Überarbeitung des europäischen Rechtsrahmens im Bereich des Datenschutzes. Es gibt aber auch Gefahren. Die Kritik wächst auch in dem Maße, in dem man selbst mehr an die Öffentlichkeit tritt. Wir sind kein politisches Organ, aber wir treten bisweilen mit Nachdruck auf. Und dann sollte man nicht zur falschen Zeit am falschen Ort sein. Dann kann man untergehen. Dies erfordert geschicktes Lavieren.

Es sieht fast so aus, als ob Ihr Erfolg als EDSB es schwer macht, einen guten Nachfolger zu finden.

Das kann mich nicht glücklich stimmen. Der Ball liegt derzeit beim Rat und beim Parlament. Sie entscheiden, ob das Verfahren weitergeht oder abgeschlossen wird. Letzten Endes werden sie aber schon jemanden finden, der das Staffelholz übernehmen kann.

Jedes EU-Organ bzw. jede EU-Einrichtung muss mindestens einen DSB haben. Arbeiten Sie mit diesem DSB zusammen?

Ja, wir arbeiten viel mit den DSB zusammen. Dreimal pro Jahr findet ein Treffen mit allen DSB statt. Außerdem arbeiten wir monatlich, wöchentlich oder sogar täglich mit den DSB zusammen, unter anderem per E-Mail oder telefonisch. Bei allen Angelegenheiten wird der DSB in Kopie gesetzt. Wir haben in einem frühen Stadium

die DSB auch als strategische Partner für den Verantwortlichen positioniert. So informieren wir den DSB sehr früh vorab über unsere Aktivitäten. Auf diese Weise organisieren wir die Beteiligung des DSB an den Angelegenheiten, die ihn angehen. Übrigens sieht man beispielsweise bei der Kommission, dass es zwei DSB gibt, aber daneben auch noch rund 35 Datenschutz-Koordinatoren, in jeder GD einen. Diese 30 bis 40 Mitarbeiter, von denen einige in Teilzeit arbeiten, sind das Rückgrat der Accountability-Praxis. Wir haben die DSB fern genug gehalten, um sie nach eigenem Ermessen arbeiten zu lassen, und nah genug heran geholt, um sie zu unterstützen, wo es erforderlich ist.

Die Verordnung fordert eine Reihe von Maßnahmen, die Organisationen ergreifen müssen, beispielsweise die Einsetzung eines DSB. Für andere Compliance-Themen gelten häufig keine derart spezifischen Anforderungen, was gelegentlich zu Widerstand in Organisationen führt. Wie sorgt ein DSB dafür, dass er ernst genommen wird?

Ich finde das klar erkennbar. Wir haben daher eine Mitteilung zur Positionierung der DSB erstellt mit Themen wie Unabhängigkeit des DSB, DSB als Teilzeitfunktion und Berichtspflichten des DSB (wo steht er in der Hierarchie in der Organisation?). Außerdem haben die DSB einen von mir unterstützten Verhaltenskodex entwickelt, in dem steht, was ein DSB tun muss, wenn er gerade ernannt wurde, was seine Prioritäten sein müssen, usw. Ein DSB muss *buy in* organisieren. Er muss ein Programm erstellen und dafür Unterstützung einholen. Dieses Programm muss im Zusammenhang mit der Mission der Organisation stehen. Die Organisation muss verstehen können, welchen Nutzen sie daraus ziehen kann. Natürlich sind manche Dinge vorgeschrieben, aber eine gute Datenschutzpolitik kann auch Chancen bieten. Ein DSB sollte also nicht die Hände in den Schoß legen. Erfolgreiche DSB sind diejenigen, die sich der Herausforderung stellen. Ich denke übrigens, dass die Behauptung, es gebe bei anderen Themen keine detaillierten Vorschriften, nicht richtig ist. Hier sind beispielsweise die seit langem bestehenden Rechnungslegungs- und Bilanzierungsregeln zu nennen. Aber auch auf neueren Gebieten sieht man vergleichbare Regeln. Zum Beispiel die Aufzeichnungspflichten für Chemikalien und Emissionen. Auch im Bereich Arbeitsbedingungen gibt es detaillierte Vorschriften. Im Grundsatz folgt die Überarbeitung der Richtlinie demselben Gedanken.

Es geht darum, Compliance in der Praxis umzusetzen. Verantwortung ist keine Begriffsbestimmung, sondern eine Aktion. Und dann gelangt man zur Accountability. Der Begriff selbst kommt in der Verordnung nicht vor, aber die Wirtschaft hat in den vergangenen Jahren alle Elemente der Accountability umfassend ausgelotet, und dann gelangt man zu denselben Schlussfolgerungen: Es geht um *Datenmanagement*. Ich bin nur teilweise zufrieden damit, wie dies in der Verordnung formuliert wurde. Einige Dinge hat die Kommission zu altmodisch gefärbt, beispielsweise die Nachweisbestimmung (die Dokumentationspflicht von Artikel 28, *Anm. d. Red.*). Natürlich sind Nachweise erforderlich, aber es ist nicht nötig, dass Organisationen jederzeit über eine akkurate Beschreibung ihrer Datenverarbeitungen verfügen. Das hatten wir bei der Meldepflicht. Ich habe empfohlen vorzuschreiben, dass es eine Methodik zur Verwaltung der Verarbeitungen gibt. Das kann dann standardisiert und pro Sektor weiter spezifiziert werden. Es wird jetzt an einem *risk-based approach* gearbeitet, damit derartige Verpflichtungen funktionieren können.

Zu Recht werden in der Verordnung überholte Durchsetzungspflichten gestrichen. Ein Beispiel hierfür ist die Meldepflicht für Datenverarbeitungen. An ihre Stelle sind neue Pflichten getreten, obwohl dabei nicht immer das richtige Maß gewahrt wird. Die Kommission hätte besser die kennzeichnenden Elemente von Verantwortung beschreiben können, wie das Ergreifen von Maßnahmen, die Kontrolle ihrer Effektivität und das Vorhandensein von diesbezüglichen Nachweisen. Und dann hätte beschrieben werden können, welche Maßnahmen mindestens zu ergreifen sind. Die jetzt in der Verordnung genannten Maßnahmen können in einem bestimmten Kulturkreis vertretbar sein, sicher ist aber, dass ihre Wirkung in 28 verschiedenen Ländern sehr unterschiedlich sein wird. Es ist also eine Herausforderung, einheitliche Vorschriften zu erstellen, die dann nicht zu drückend, aber auch überall passend sind. Ich glaube, dass wir in diesem Punkt, vor allem im Rat, dem Ergebnis näher sind, als in der Regel angenommen wird.

Übrigens werden die Kosten der Maßnahmen meines Erachtens gewaltig übertrieben. Es werden weder der Nutzen noch die durch Reibungsverluste verursachten Kosten berücksichtigt. Außerdem wird die aktuelle Non-Compliance ignoriert. Die Kommission hat die Gemüter wach gerüttelt, indem sie mit Geldstrafen in Millionenhöhe droht. Diese können natürlich abgestuft werden, stellen aber nichtsdestoweniger ein außerordentlich effektives Mittel dar, um Aufmerksamkeit in der *Chefetage* zu erhalten. Und dann braucht man Aufsichtsbehörden, die damit vernünftig umgehen. Das bedeutet, dass sie vorbildliche Lösungen belohnen müssen und bei Verfehlungen auch nachdrücklich auftreten müssen. Die Aufsichtsbehörden müssen daher nicht nur die Befugnis haben, Geldstrafen zu verhängen, sondern auch, einen Maßnahmenplan und Fortschrittsberichte zu fordern, verknüpft mit Sanktionen, um Organisationen dazu anzuhalten. Das kann man jedoch nicht für die gesamte Wirtschaft tun. Eine Aufsichtsbehörde muss daher gut darlegen können, warum sie in einem bestimmten Falle Durchsetzungsmaßnahmen ergreift.

Die digitale Wirtschaft ist heutzutage sehr international. Wie fügen wir unsere europäischen Datenschutzwerte in das weltweite Spielfeld ein, ohne uns selbst aus dem Spiel zu drängen?

Es besteht ein hohes Maß an Übereinstimmung in der Welt über die Grundsätze auf diesem Gebiet. Man betrachte einmal die neuen Grundsätze der OECD. Daran haben sich nun mehr Länder beteiligt als letztes Mal, und das Ergebnis ist überraschend gleich. Das sehe ich auch auf internationalen Konferenzen. Natürlich gibt es Unterschiede zwischen der APEC und der EU, aber es gibt auch Übereinstimmungen. Und wenn es auf die Umsetzung in der Praxis ankommt, denke ich, dass wir sehr ähnliche Vorstellungen haben. Das gilt auch für die USA, auch wenn es dort eine große Zurückhaltung gibt, einen Schritt nach vorne zu machen. Man darf jedoch nicht den Einfluss unterschätzen, den Europa auf diesem Gebiet hatte und noch immer hat.

Wenn wir den Moment also gut nutzen können, führt das de facto zu einer Weltnorm mit einem enormen Einfluss. Es gibt verschiedene Wege, eine solche Norm zwischen den verschiedenen Ländern interoperabel zu machen. Ein Weg besteht darin, davon auszugehen, dass Organisationen Regeln beachten wollen, sie aber am liebsten nur ein Mal weltweit zu möglichst geringen Kosten implementieren wollen. Diese

Möglichkeit besteht jetzt. Außerdem ist da noch die enorme Marktmacht Europas. Auch die Federal Trade Commission in den USA ist auf dem Gebiet des Datenschutzes viel aktiver geworden. In den USA wird die Nichtbeachtung von Datenschutzmaßnahmen, anders als in Europa, als unlautere Geschäftspraktik betrachtet, aber damit kommen sie ziemlich weit. Die FTC hat sich in einer Reihe von Dingen bereit gezeigt, etwas, das in Europa versprochen, aber nicht geliefert wurde, seitens der USA mit einer Sanktion zu belegen. Das haben sie nicht zufällig getan.

Es besteht also eine zunehmende Bereitschaft, mit Europa zusammenzuarbeiten. Im Lichte des transatlantischen Marktes ist das ein großartiger Beitrag zur Interoperabilität. Ich habe bei der Gelegenheit das europäische System der *Adequacy*, der Angemessenheit, als Beitrag zur Interoperabilität dargestellt. Wir stehen kurz vor einigen bedeutenden Entwicklungen. Man schaue sich beispielsweise Google an, gegen das jetzt in verschiedenen Ländern Ermittlungen laufen. Dies führt wahrscheinlich auch zu Gerichtsurteilen, und das ist auch notwendig, da unsere Welt immer stärker zusammenwächst.

Wie soll ein Compliance Officer mit diesen weltweiten Unterschieden umgehen?

Der DSB kann dafür sorgen, dass er im Kontext seiner Organisation eine Agenda entwickelt, in der diese Dinge systematisch benannt werden. Der DSB muss also versuchen, die (weltweiten) Anforderungen in die Produkte und Dienste seiner Organisation zu übersetzen. Gegebenenfalls werden natürlich kleine Unterschiede zwischen Ländern und Märkten sichtbar sein, aber es muss sich dennoch um ein integriertes Vorgehen handeln. Wenn man in einer Organisation arbeitet, in der der korrekte Umgang mit personenbezogenen Daten einen hohen Stellenwert hat und das nicht das Risiko einer negativen Presse aufgrund eines Datenlecks oder einer Durchsetzungsmaßnahme eingehen will, muss man also darin investieren. Wenn die Durchsetzungsmaßnahmen zunehmen, wird dieses integrierte Vorgehen umso wichtiger, und das wäre eine gesunde Entwicklung.

Und wie muss eine Aufsichtsbehörde mit dieser Komplexität umgehen?

Es ist Aufgabe des Verantwortlichen, die Regeln einzuhalten. Und es ist Aufgabe der Betroffenen, ihre Rechte auszuüben. Für die Aufsichtsbehörde ist es somit wichtig, dass das System generell gut funktioniert. Wenn es irgendwo im System hapert, muss man als Aufsichtsbehörde handeln. Das gilt auch bei strukturellem Fehlverhalten von Parteien. Die Aufsichtsbehörde muss sich also nicht allzu viel mit Kleinkram beschäftigen, aber Kleinkram muss auch bedient werden. Es muss also eine Anlaufstelle dafür geben, eventuell irgendwo anders.

Die Herausforderung für die Aufsichtsbehörde besteht darin, sich weiterhin auf das große Ganze zu konzentrieren und dann rechtzeitig einzugreifen. Man darf sich als Aufsichtsbehörde nicht in einem Tunnel fangen lassen, da man dann zu sehr mit den täglichen Dingen wie Beschwerden, Meldungen usw. beschäftigt ist. Man muss sich als Aufsichtsbehörde immer fragen, ob man sich mit den richtigen Dingen beschäftigt, ob man seine knappen Mittel auch effektiv einsetzt.

Die Aufsichtsbehörden plädieren für mehr Accountability, finden aber in der Praxis häufig immer noch ein Haar in der Suppe und würdigen nicht, was in einer Organisation im Bereich des Datenschutzmanagements bereits passiert. Wird es den Aufsichtsbehörden gelingen, diese Kehrtwende zu machen?

Ich hoffe es. Einige tun es bereits. Dabei ist so ein Europäischer Datenschutzausschuss auch hilfreich. Letztlich wird es immer kohärenter werden, aber das ist ein Wachstumsprozess. Als EDSB arbeiten wir bereits auf diese Weise. Wir schauen, wo die großen Risiken beim Verantwortlichen liegen, wie Inhalt der Information und deren Verwendung. Wo ist es generell gut genug und wo müssen wir eingreifen, da die Risiken zu hoch sind?

Derzeit sind der One-Stop-Shop-Gedanke und der Proximity-Grundsatz ein großes Hindernis für den Fortschritt der Verordnung. Es ist jedoch nicht unwichtig, dass hierfür eine gute Lösung gefunden wird, auch aus der Sicht des DSB, der die Organisation zu den Vorschriften und Risiken beraten muss. Wie sehen Sie das?

Der One-Stop-Shop-Gedanke und der Proximity-Grundsatz stehen in der Tat im Widerspruch zueinander. Dies ist das Thema, um das es sich momentan dreht und von dem das Gelingen oder Scheitern des Überarbeitungsprojekts in diesem Stadium abhängt. Im Oktober waren wir, denke ich, der Lösung näher als im Dezember. Die Themen dürfen nicht unabhängig voneinander betrachtet werden. Der One-Stop-Shop ist ein hervorragendes Konzept, aber man muss einsehen, dass es einen One-Stop-Shop für Organisationen gibt und einen One-Stop-Shop für Betroffene. Und da diese sich in grenzüberschreitenden Situationen unterscheiden, muss man akzeptieren, dass es niemals nur eine Anlaufstelle gibt. Die Lead Authority ist nicht exklusiv zuständig. Man muss dies also als eine Art Aufgabenverteilung betrachten. Wenn die Lead Authority als Führer eines Teams angesehen wird, kommt man der Lösung viel näher. Und das gilt umgekehrt auch. Das Problem ist meiner Ansicht nach also sicherlich lösbar.

Aber geht es letztlich nicht einfach ums Geld? Man will nicht, dass jedes Land gesondert eine Strafe verhängen kann, aber man ist neidisch, wenn die gesamte Strafe an ein Land fließt.

Auch daran könnte man etwas ändern. Wenn man den Gedanken der Zusammenarbeit konsequent weiterführt, könnte man sogar noch regeln, dass eine solche Strafe von 100 Millionen zwischen den betroffenen Ländern geteilt wird. Das steht jetzt nicht in der Verordnung, aber wenn man dieses Problem lösen muss, ist das die Methode. Wichtiger ist jedoch, dass wir uns fragen, was der One-Stop-Shop nun eigentlich ist. Einerseits hat eine Aufsichtsbehörde im Rahmen des One-Stop-Shop eine Aufgabe; andererseits hat sie bestimmte Befugnisse, die damit nicht in Einklang stehen. Die französische Aufsichtsbehörde kann nun einmal in Deutschland keine Untersuchung vor Ort vornehmen. In diesem Fall muss die französische Aufsichtsbehörde die deutschen Kollegen um Mitarbeit bitten. Und so entsteht bereits eine Zusammenarbeit im Untersuchungsbereich. Auch bei der Durchsetzung von Pflichten ist eine Zusammenarbeit möglich. In der Verordnung wird unter dem One-Stop-Shop somit eigentlich eine Form der Zusammenarbeit weiter ausgestaltet. Und

das ist auch die Lösung für Proximity. Hier spielt auch Vertrauen eine Rolle zwischen Richtern untereinander und Aufsichtsbehörden untereinander. Der Verantwortliche muss nicht immer lange auf eine Entscheidung warten.

Wir können im EDSA versuchen, eine Angelegenheit zu beschleunigen. So könnte der EDSA versuchen, innerhalb eines halben Jahres einen Standpunkt zu erarbeiten, an den sich jeder hält. Ich sehe ein, dass ein halbes Jahr im Internetzeitalter eine Ewigkeit ist, aber es geht um derart wichtige Dinge, dass eine solche Frist durchaus gerechtfertigt ist. Das Schöne an dem Vorschlag war, dass er die verfahrenstechnischen *Trigger* hatte, um für gute Entscheidungen an der Basis zu sorgen. Und eine Aufsichtsbehörde, die vom Standpunkt des EDSA abweicht, muss ihre Gründe dafür erläutern. Ein Richter wird sich dem nicht so einfach anschließen. Zugleich löste unser Vorschlag auch ein anderes Problem, nämlich dass die Kommission sich selbst eine zu große Rolle zugeteilt hatte, womit niemand einverstanden war. Diese Lösung lag im Oktober vergangenen Jahres auf dem Tisch, aber danach gab es zu viel Uneinheitlichkeit in der Ausgestaltung, so dass im Dezember keine Einigung erzielt werden konnte. Für dieses Problem sind mehrere Lösungen möglich, ohne dass ein neues Organ (eine gesamteuropäische Aufsichtsbehörde, *Anm. d. Red.*) erforderlich ist, das eigentlich niemand will. Das Paradox ist somit lösbar.

Ein halbes Jahr ist im Falle einer Untersuchung oder Klage vielleicht akzeptabel, aber der Consistency-Mechanismus gilt auch für die Konsultation der Aufsichtsbehörde für Projekte des Verantwortlichen, für die ein PIA durchgeführt wurde. Und dann sind sechs Monate durchaus eine sehr lange Zeit.

In solch einem Projekt muss man natürlich realistische Fristen handhaben. Eine Organisation darf nicht denken, dass sie eine gute Idee haben, und dann um fünf vor zwölf noch eben einen Stempel abholen. Es ist auch wichtig, dass man gute Berater hat, die rechtzeitig die Alarmglocke betätigen können. Übrigens werden wahrscheinlich die Dinge, die auf der Hand liegen und dennoch zur Sprache kommen, bereits während der Übergangsfrist der Verordnung als erste den Consistency-Mechanismus durchlaufen. Sobald die Verordnung in Kraft tritt, wird es also zu den häufigsten Themen schon Richtlinien und eine geprüfte Politik geben. Wenn eine Organisation also mit einer nicht allzu verrückten Frage kommt, wird verhältnismäßig rasch eine Antwort erteilt werden können. Auch in diesem Punkt wird es ein schrittweises Vorgehen geben. Aber wenn man das auf europäischer Ebene tut, muss man es mit dem richtigen Maß tun.

Die Umsetzung der Verordnung kann also in den Ländern doch noch unterschiedlich sein?

Kommissarin Reding nennt die Verordnung „ein Gesetz überall“. Ich würde es „ein Rahmengesetz überall“ nennen. Es ist eine Verordnung mit einer großen Zahl von offenen Punkten in wichtigen Bereichen geworden. Und das ist notwendig, da die Gesetze aller 28 Mitgliedstaaten mit der Verordnung zusammenarbeiten müssen. In einem dogmatischen Ansatz ist das nicht möglich. Eine Verordnung ist nach europäischem Recht sehr dominant. Es hängt jedoch davon ab, was diese

Verordnung besagt. Wenn diese Verordnung so gestaltet ist, dass sie eine Ko-Existenz ermöglicht, gibt es keine Probleme. Daran arbeitet der Rat derzeit. In der Verordnung ist von „rechtlichen Verpflichtungen“ die Rede, aber es wird nicht gesagt, um welche rechtlichen Verpflichtungen es sich handelt. Man denke beispielsweise an das Steuerrecht oder Rechtsvorschriften im Bereich Gesundheit und Sicherheit am Arbeitsplatz. Diese strotzen nur so vor rechtlichen Verpflichtungen im Zusammenhang mit der Verarbeitung personenbezogener Daten. Wenn diese Verpflichtungen mit den Grundrechten vereinbar sind, sind es rechtliche Verpflichtungen im Sinne der Verordnung. Die kann man also nebeneinander bestehen lassen. Die Mitgliedstaaten müssen jedoch der Verordnung vorgreifen, sonst ist die rechtliche Folge, dass all diese lokalen Rechtsvorschriften durch das Inkrafttreten der Verordnung hinfällig werden. Und das will niemand, darüber muss man also im Detail nachdenken. Ich denke, dass die Kommission das etwas unterschätzt hat.

Als Fazit, welche Botschaft möchten Sie unseren Leserinnen und Lesern noch mit auf den Weg geben?

Zunächst möchte ich sagen, dass Datenschutzspezialisten als solche immer wichtiger werden und eine wichtige strategische Rolle im System spielen werden. Diese Datenschutzspezialisten werden wir auf allen Ebenen benötigen. Nicht nur Juristen, wir brauchen auch Menschen mit einem technischen Hintergrund oder mit Managementfähigkeiten.

Zweitens dürfen sie nicht untätig bleiben, aber es besteht die Gefahr, dass man im Alleingang versucht, Berge zu versetzen. Das gelingt natürlich nicht, und daher muss man sich einen Plan überlegen, mit dem man schrittweise doch Veränderungen schaffen kann. Dafür muss man Geduld und ein gewisses Vorstellungsvermögen mitbringen. Zum Trost sei gesagt, dass ich genau das tun musste, als ich hier als EDSB mit nichts anfing. Dass wir jetzt sind, wo wir sind, zeigt, dass es möglich ist. Und wenn man dann noch das nötige Quäntchen Glück hat, kann man das mit einem ganzen Team mit Begeisterung weitermachen.

Der dritte Punkt ist, dass diese Erneuerung des europäischen Rahmens meines Erachtens unvermeidlich ist. Das Datum, an dem hier der Schlusspunkt gesetzt werden kann, ist derzeit noch offen. Wir müssen ehrlich sein, vor den Wahlen zum Europäischen Parlament schaffen wir das nicht mehr. Das Endprodukt wird nicht dem entsprechen, was eingereicht wurde, aber es wird dem doch sehr ähnlich sein und besser sein. Wir machen derzeit viele Kompromisse, und das ist auch gut so. Sehr viele Leute sind sich des Gefährdungsgrads und der großen normativen Fragen, die damit zusammenhängen, nicht bewusst.

Abschließend noch eines: Wir sind als Aufsichtsbehörde derzeit dabei, Brücken zu schlagen zwischen den konventionellen Datenschutzspezialisten und all den Menschen, die an der Entwicklung von Internet, Software, Hardware und Standards arbeiten. Diese Menschen waren durch die NSA-Affäre auch stark getroffen. Wir werden einige Fachleute, die in der Welt des „*privacy-aware internet development*“, der Entwicklung eines datenschutzbewussten Internets, aktiv sind, einbeziehen, um zu versuchen, einen Multiplikatoreffekt zu erreichen. Das zeigt, dass auch Aufsichtsbehörden kreativ sein müssen.