Hochrangige Konferenz: „Ethische Aspekte von Datenschutz und Privatsphäre“
Zentrum für Ethik, Universität Tartu/Datenschutzaufsichtsbehörde
Tallinn, Estland, 9. Januar 2013

EU-Regelwerk im Bereich Datenschutz – Sachstand und Zukunftsperspektiven

Peter Hustinx
Europäischer Datenschutzbeauftragter

Schutz der Privatsphäre und Datenschutz – oder präziser ausgedrückt: das Recht auf *Achtung* des Privatlebens und das Recht auf *Schutz* der eigenen personenbezogenen Daten – sind beides eher neue Begriffe einer universellen Idee mit starken ethischen Aspekten: Würde, Autonomie und der *einzigartige Wert* jedes Menschen. Dies impliziert auch das Recht jedes Menschen auf Entwicklung seiner Persönlichkeit und auf angemessenen Einfluss in Angelegenheiten, die möglicherweise unmittelbare Auswirkungen auf ihn haben können.

Der Schutz der Privatsphäre und der Datenschutz haben sich über die letzten vier Jahrzehnte als gesondertes Rechtsgebiet entwickelt, vor allem im Kontext des Europarats und der Europäischen Union und in Anbetracht des wachsenden Einflusses der Informations- und Kommunikationstechnologie (IKT). Dieser Einfluss ist mittlerweile überall um uns herum spürbar, jede Minute eines jeden Tages, sowohl in unserem Privat- als auch in unserem Berufsleben, und wird sich wahrscheinlich in naher Zukunft noch weiter verstärken.

In meinen heutigen Ausführungen möchte ich auf die historische Entwicklung und den Sachstand des Regelwerks in diesem Bereich eingehen sowie auf die Richtung, in die sich das Recht in Bezug auf den Schutz der Privatsphäre und den Datenschutz möglicherweise, im Einklang mit seinen ethischen Wurzeln und Zielsetzungen, entwickeln wird, um einen effektiveren Schutz zu bieten.

In diesem Überblick werde ich auf zwei Hauptthemenbereiche eingehen: Der erste befasst sich mit der Entwicklung *stärkerer* Rechte in Bezug auf den Schutz der Privatsphäre und den Datenschutz an sich, der zweite mit der Notwendigkeit, für eine *kohärentere* EU-weite Anwendung dieser Rechte zu sorgen – beides im Hinblick auf das Voranbringen eines *effektiveren* Schutzes in der Praxis und einer Verringerung *nicht hilfreicher Unterschiede* in Bezug auf die Ausgestaltung dieses Schutzes in den verschiedenen Mitgliedstaaten.

Privatsphäre und Privatleben

Erst nach dem Zweiten Weltkrieg fand das Konzept „Recht auf Privatsphäre" Eingang in internationales Recht. Dies geschah zunächst in eher schwacher Fassung in Artikel 12 der Allgemeinen Erklärung der Menschenrechte (UN-Vollversammlung, Paris 1948), nach dem niemand „*willkürlichen* Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr" ausgesetzt werden darf.

Ein substanziellerer Schutz folgte in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) (Europarat, Rom, 1950), demzufolge jede Person „das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz" hat, und „eine Behörde in die Ausübung dieses Rechts nur eingreifen [darf], soweit der Eingriff *gesetzlich vorgesehen* und in einer demokratischen Gesellschaft *notwendig*" für bestimmte wichtige und gesetzmäßige Interessen ist.

Das Erwähnen der Wohnung und Korrespondenz konnte an verfassungsrechtliche Traditionen in vielen Ländern weltweit, als gemeinsames Erbe einer langen, gelegentlich Jahrhunderte alten Entwicklung, anknüpfen, aber der Fokus auf Privatsphäre und Privatleben war neu und eine offenkundige Reaktion auf die Ereignisse des Zweiten Weltkriegs.

Der Umfang und die Auswirkungen dieses Schutzes wurden durch den Europäischen Gerichtshof für Menschenrechte in Straßburg in einer Reihe von Urteilen erläutert. In allen einschlägigen Rechtssachen prüft der Gerichtshof, ob ein *Eingriff* in das Recht auf Achtung des Privatlebens stattgefunden hat, und wenn ja, ob dieser auf einer *entsprechenden* – d. h. eindeutigen, zugänglichen und vorhersehbaren – Rechtsgrundlage beruhte und ob er in Anbetracht des gesetzmäßigen Interesses *notwendig* und verhältnismäßig war.

In der Rechtsprechung des Gerichtshofes beschränkt sich der Begriff „Privatleben“ nicht auf „private“ Situationen, sondern erstreckt sich auch auf bestimmte Aspekte des Berufslebens und des Verhaltens in der Öffentlichkeit, egal, ob in der Vergangenheit oder nicht, in denen die betroffenen Personen berechtigterweise eine Privatsphäre erwarten. Dies gilt jedoch häufig für besondere Situationen, in denen es um sensible Daten oder aber um polizeiliche oder geheimdienstliche Ermittlungen geht.

Datenschutz

Um das Jahr 1970 kam der Europarat zu dem Schluss, dass Artikel 8 EMRK vor dem Hintergrund neuer Entwicklungen eine Reihe von Defiziten aufwies, vor allem im Bereich IKT: der nicht eindeutige Geltungsbereich von „Privatleben“, die Schwerpunktlegung auf Eingriffe durch staatliche Behörden und das Fehlen eines proaktiveren Ansatzes zur Bekämpfung eines möglichen Missbrauchs personenbezogener Daten durch Unternehmen oder andere Organisationen des Privatsektors.

Nach sorgfältiger Vorbereitung führte dies zur Annahme des Datenschutzübereinkommens, auch als Konvention 108 bezeichnet (Straßburg 1981), dem inzwischen 44 Mitgliedstaaten des Europarats beigetreten sind, darunter alle Mitgliedstaaten der EU.

Zweck dieses Übereinkommens ist es, „im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden („Datenschutz“). Der Begriff „personenbezogene Daten“ wird definiert als „jede Information über eine bestimmte oder bestimmbare natürliche Person („Betroffener“)“.

Der Begriff „Datenschutz“ ist also *breiter gefasst* als „Schutz der Privatsphäre“, da er sich auch auf andere Grundrechte und -freiheiten sowie auf alle Arten von Daten bezieht, *unabhängig davon*, ob sie die Privatsphäre betreffen oder nicht. Gleichzeitig ist der Begriff *enger gefasst*, da er sich lediglich auf die Verarbeitung personenbezogener Daten bezieht und andere Aspekte des Schutzes der Privatsphäre unberücksichtigt bleiben.

Heutzutage stehen sämtliche Aktivitäten im öffentlichen oder privaten Sektor auf die eine oder andere Art im Zusammenhang mit der Erhebung und Verarbeitung personenbezogener Daten. Der Schutz des Einzelnen (von Bürgerinnen und Bürgern, Verbraucherinnen und

Verbrauchern, Arbeitnehmerinnen und Arbeitnehmern, usw.) vor der Erhebung, der Aufzeichnung und dem Austausch seiner personenbezogenen Daten aus ungerechtfertigten Gründen betrifft daher auch dessen Teilhabe an sozialen Beziehungen, egal ob in öffentlichen Räumen oder nicht. Dies kann auch den Schutz des Rechts auf freie Meinungsäußerung, vor Diskriminierung und die Förderung des „Fair play“ in Prozessen der Entscheidungsfindung beinhalten.

Strukturelle Schutzmaßnahmen

Das Übereinkommen enthält eine Reihe von Grundsätzen für den Datenschutz, denen jede Partei zunächst in ihrem nationalen Recht Wirkung verleihen muss, bevor das Übereinkommen in Kraft tritt. Diese Grundsätze bilden noch immer den Kern jeglicher nationaler Rechtsvorschriften in dem Bereich. Gemäß dem Übereinkommen müssen personenbezogene Daten „nach Treu und Glauben und auf rechtmäßige Weise beschafft sein und verarbeitet werden“ sowie „für festgelegte und rechtmäßige Zwecke gespeichert sein und dürfen nicht so verwendet werden, dass es mit diesen Zwecken unvereinbar ist“. Darüber hinaus müssen personenbezogene Daten „den Zwecken, für die sie gespeichert sind, entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen“ und „müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein“.

Weitere Grundsätze des Übereinkommens sind die Forderung bezüglich „geeigneter Sicherungsmaßnahmen” und der „zusätzliche Schutz für den Betroffenen”, wie das Recht auf Zugang zu den eigenen personenbezogenen Daten, das Recht, „gegebenenfalls diese Daten berichtigen oder löschen zu lassen” sowie das Recht auf ein Rechtsmittel, wenn diese Rechte nicht beachtet werden. Das Konzept einer „unabhängigen Aufsicht“ war anfänglich nicht Bestandteil des Übereinkommens, wurde jedoch in der Folge weithin in der Praxis angewendet und dem Übereinkommen zu einem späteren Zeitpunkt in Form eines Protokolls hinzugefügt.

Festzuhalten gilt: Ausgangspunkt des Übereinkommens ist *nicht*, dass die Verarbeitung personenbezogener Daten in jedem Fall als *Verletzung* der Privatsphäre zu betrachten ist, sondern dass im Interesse der Privatsphäre sowie anderer Grundrechte und -freiheiten bei jeder Verarbeitung *stets* bestimmte rechtliche Rahmenbedingungen zu beachten sind. Dies kommt beispielsweise in dem Grundsatz zum Ausdruck, dass personenbezogene Daten nur für festgelegte und rechtmäßige Zwecke verarbeitet werden dürfen, diesen Zwecken entsprechen müssen und nicht so verwendet werden dürfen, dass es mit diesen Zwecken unvereinbar ist.

Gemäß diesem Ansatz wurden die Schlüsselelemente von Artikel 8 EKMR, etwa der Eingriff in die Ausübung des Rechts auf Schutz der Privatsphäre nur soweit gesetzlich vorgesehen und soweit für einen rechtmäßigen Zweck erforderlich, auf einen *allgemeineren* Kontext übertragen. Darüber hinaus sind gemäß dem Übereinkommen keine Ausnahmen von diesen Grundsätzen zulässig, ausgenommen unter ähnlichen Umständen wie für das Recht auf Schutz der Privatsphäre selbst.

Unterschiedliche Kontexte

Es sollte klar sein, dass dies in der Praxis nur dann gut funktioniert, wenn das System von Kontrollen und Ausgewogenheiten – bestehend aus substanziellen Bedingungen, Rechten des Einzelnen, Verfahrensbestimmungen und einer unabhängigen Aufsicht – ausreichend flexibel ist, um unterschiedlichen Kontexten Rechnung zu tragen und außerdem mit Voraussicht und einem guten Blick für die Interessen der Betroffenen und anderen einschlägigen Interessengruppen angewendet wird. Bei diesem Ansatz spielt das Recht auf Achtung des Privatlebens, wie in Artikel 8 EMRK dargelegt, im Hintergrund weiterhin eine wichtige Rolle im Hinblick auf bestimmte spezielle, einschneidendere Maßnahmen.

Es war nicht beabsichtigt, dass die Bestimmungen des Übereinkommens unmittelbar anwendbar sein oder in die gerichtliche Kontrolle einfließen sollten. Seit 1997 hat der Europäische Gerichtshof für Menschenrechte in einer Reihe von Rechtssachen geurteilt, dass der Schutz personenbezogener Daten für das Recht auf Achtung des Privatlebens gemäß Artikel 8 EMRK von „grundlegender Bedeutung“ ist und hat aus dem Übereinkommen außerdem Maßstäbe dafür abgeleitet, zu beurteilen, inwieweit dieses Recht verletzt wurde. Dies lässt darauf schließen, dass der Gerichtshof zunehmend geneigt ist, die Einhaltung des Übereinkommens – wenigstens im Falle „sensibler Daten“ – im Kontext von Artikel 8 EMRK zu bewerten.

Dem Übereinkommen kommt in den meisten Mitgliedstaaten des Europarats bei der Ausgestaltung ihrer Rechtssetzungspolitik große Bedeutung zu. Vor diesem Hintergrund galt das Thema „Datenschutz“ von Anfang an als Frage von großer struktureller Bedeutung für eine moderne Gesellschaft, in der die Verarbeitung personenbezogener Daten eine zunehmend wichtige Rolle spielt. Das Übereinkommen wird derzeit überarbeitet, und wir werden auf das Thema in einem breiteren Kontext zurückkommen.

Harmonisierung

Auch wenn der Europarat mit großem Erfolg das Thema „Datenschutz“ auf die Tagesordnung gesetzt und die maßgeblichen Elemente eines Rechtsrahmens definiert hat, war er weniger erfolgreich darin, EU-weit für mehr Kohärenz zu sorgen. Manche Mitgliedstaaten haben das Übereinkommen erst verspätet umgesetzt, und diejenigen, die es umgesetzt haben, gelangten zu unterschiedlichen Ergebnissen, was in einigen Fällen sogar zu Beschränkungen des Datenaustauschs mit anderen Mitgliedstaaten führte.

Aus diesem Grunde hatte die Europäische Kommission große Bedenken, dass sich diese fehlende Kohärenz negativ auf die Entwicklung des Binnenmarkts in verschiedenen Bereichen – u. a. den freien Personen- und Dienstleistungsverkehr – auswirken könnte, in denen die Verarbeitung personenbezogener Daten eine zunehmend wichtige Rolle spielen sollte. Ende 1990 legte die Kommission einen Vorschlag für eine Richtlinie zur Harmonisierung der nationalen Rechtsvorschriften im Bereich des Datenschutzes im privaten und im Großteil des öffentlichen Sektors vor.

Nach vierjähren Verhandlungen führte dies zur Annahme der aktuellen Richtlinie 95/46/EG, die zweierlei Ziele verfolgt. Erstens verpflichtet sie alle Mitgliedstaaten, die Grundrechte und -freiheiten natürlicher Personen, insbesondere das Recht auf Schutz der Privatsphäre in Bezug auf die Verarbeitung personenbezogener Daten, im Einklang mit der Richtlinie zu schützen. Zweitens verpflichtet sie sie, den freien Strom personenbezogener Daten zwischen Mitgliedstaaten aus Gründen, die mit diesem Schutz in Zusammenhang stehen, weder einzuschränken noch zu untersagen. Beide Auflagen stehen in enger Beziehung zueinander und zielten darauf ab, in allen Mitgliedstaaten ein gleich hohes Maß an Schutz zu erreichen, um eine ausgewogene Entwicklung des Binnenmarkts zu erreichen.

Vor diesem Hintergrund gründete die Richtlinie auf den Grundsätzen des Datenschutzes, wie sie in Konvention 108 des Europarats festgelegt sind. Gleichzeitig konkretisierte sie diese Grundsätze und ergänzte sie durch weitere Anforderungen und Bedingungen. Da in der Richtlinie jedoch allgemein formulierte Konzepte und offene Standards übernommen wurden, hatten die Mitgliedstaaten weiterhin einen recht breiten Ermessensspielraum bezüglich der Umsetzung. So hat die Richtlinie im Ergebnis zu einer sehr viel stärkeren Kohärenz zwischen den Mitgliedstaaten, gewiss aber nicht zu identischen oder vollständig kohärenten Lösungen geführt.

Mehr Substanz

Die aktuelle Richtlinie enthält Kriterien für die Rechtmäßigkeit einer Verarbeitung von Daten. Die Verarbeitung personenbezogener Daten darf nur erfolgen, wenn die betroffene Person „*ohne jeden Zweifel* ihre Einwilligung gegeben“ hat oder die Verarbeitung *erforderlich* ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, für die Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die in Ausübung staatlicher Gewalt erfolgt, für die Wahrung lebenswichtiger Interessen der betroffenen Person oder zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen wahrgenommen wird, sofern die Interessen der betroffenen Person gegenüber diesem Interesse nicht überwiegen. Dies erfordert eine detaillierte Prüfung der verschiedenen Phasen der Datenverarbeitung und verpflichtet die für die Verarbeitung Verantwortlichen, dieser Überprüfung rechtzeitig Rechnung zu tragen.

Ein weiteres Merkmal der Richtlinie ist die Verpflichtung der für die Verarbeitung Verantwortlichen, der betroffenen Person – soweit diese Informationen ihr noch nicht vorliegen – über die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmungen der Verarbeitung und andere einschlägige Punkte Auskunft zu erteilen, sofern diese näheren Angaben „unter Berücksichtigung der spezifischen Umstände, unter denen die Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten“. Werden diese Auskünfte nicht erteilt, kann dies bedeuten, dass die Daten, mit allen einschlägigen Konsequenzen, unrechtmäßig erhoben wurden.

Darüber hinaus sieht die Richtlinie die Einrichtung unabhängiger Kontrollstellen zur Überwachung der Einhaltung der nationalen Rechtsvorschriften in ihrem Hoheitsgebiet, mit einer Reihe spezieller Funktionen und Befugnisse vor, die sie „in völliger Unabhängigkeit“ wahrnehmen sollen. Diese Stellen arbeiten bei der Ausübung ihrer Funktionen zunehmend enger zusammen, auch im Rahmen der in Artikel 29 aufgeführten unabhängigen „Datenschutzgruppe“, die auf EU-Ebene beratende Funktion hat.

Internationaler Anwendungsbereich

Die Richtlinie gilt für die Verarbeitung personenbezogener Daten „im Rahmen der Tätigkeiten einer Niederlassung […], die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines EU-Mitgliedstaats besitzt“. An welchem Ort die Datenverarbeitung stattfindet, ist in diesem Zusammenhang unerheblich. Dieses Kriterium ist auch für den

Anwendungsbereich einzelstaatlicher Rechtsvorschriften innerhalb der EU von großem Belang. Besitzt der für die Verarbeitung Verantwortliche keine Niederlassung in der EU, findet das Recht des Mitgliedstaats Anwendung, in dem sich die für die Datenverarbeitung verwendeten Mittel befinden.

Darüber hinaus folgt die Richtlinie dem Grundsatz, dass personenbezogene Daten nur in Drittländer übermittelt werden dürfen, die ein angemessenes Schutzniveau gewährleisten. Ist ein solcher Schutz nicht gegeben, ist eine Übermittlung nur unter bestimmten Bedingungen zulässig.

Diese Bestimmungen treffen auf eine komplexe Wirklichkeit, in der sich – sowohl innerhalb der EU als auch in Drittstaaten – immer häufiger die Frage stellt, welches Recht anwendbar und wer für dessen Einhaltung zuständig ist.

Dies wirft auch neue Fragen in Bezug auf das Internet – betreffend die Position von Websites, Suchmaschinen, sozialen Netzwerken und moderner Werbetechnologie – sowie den Datenverkehr innerhalb multinationaler Konzerne, das Outsourcing von Dienstleistungen und Cloud-Computing auf. In der Praxis wird ein angemessener Schutz zunehmend in Form „verbindlicher unternehmensinterner Vorschriften“ bereitgestellt – von Verhaltenskodizes, die von Unternehmen formuliert werden, den spezifischen Anforderungen genügen und von den zuständigen Kontrollstellen als ausreichend effektiv akzeptiert werden.

Einschlägige Rechtsprechung

Alle Mitgliedstaaten haben die Richtlinie in nationales Recht umgesetzt; dies gilt auch für die neuen Mitgliedstaaten, bei denen die Umsetzung eine Bedingung für den Beitritt darstellte. Mittlerweile hat die Kommission mehrere gerichtliche Klagen wegen nicht ordnungsgemäßer Umsetzung der Richtlinie angestrengt. Die erste Klage betraf einen der Mitgliedstaaten mit der längsten Erfahrung in diesem Bereich: Deutschland. Im März 2009 urteilte der Gerichtshof in Luxemburg, dass die geforderte völlige Unabhängigkeit einer Kontrollstelle bedeute, dass diese frei von *jedwedem* äußeren Einfluss sei. Dies wurde vor kurzem in einer Rechtssache gegen Österreich bestätigt und ausgearbeitet.

Der Gerichtshof hat auch einige andere wichtige Urteile in Bezug auf den bestehenden Rechtsrahmen für den Schutz personenbezogener Daten gefällt. So stellte er in seinen ersten Urteilen zur Richtlinie 95/46/EG fest, dass diese einen breiten Anwendungsbereich habe, der

nicht unmittelbar zwingend mit dem Binnenmarkt verknüpft sei. Somit ist die Richtlinie auch auf Streitfälle im öffentlichen Sektor eines einzelnen Mitgliedstaats oder auf die Website einer Kirche oder Stiftung für wohltätige Zwecke anwendbar. Im letztgenannten Fall wurde deutlich, dass die Richtlinie grundsätzlich auch für das Internet gilt, selbst wenn die Verfügbarkeit personenbezogener Daten auf einer Website an sich nicht bedeutet, dass die Bestimmungen über den Datenaustausch mit Drittländern anwendbar sind.

Ist die Richtlinie auf Fälle innerhalb des Anwendungsbereichs von Artikel 8 EKMR anwendbar, ist sie im Einklang mit dieser Bestimmung auszulegen. In diesem Zusammenhang hat der Gerichtshof zwischen Verarbeitungstätigkeiten unterschieden, die Artikel 8 EMKR möglicherweise verletzen oder nicht. Der erste Fall bezog sich auf eine Rechtsvorschrift, der zufolge Arbeitgeber verpflichtet sind, einer staatlichen Stelle bestimmte Lohndaten vorzulegen. Die Verarbeitung derselben Daten durch den Arbeitgeber selbst warf keine Grundsatzfragen auf, sofern die Datenschutzbestimmungen eingehalten wurden. Dies fügt sich in die oben erwähnte Unterscheidung zwischen „Privatsphäre“ und „Schutz personenbezogener Daten“ im Verlaufe der Rechtsentwicklung ein.

Reformbedarf

Die Richtlinie 95/46/EG stellt weiterhin den Kernbestandteil des EU-Regelwerks im Bereich Datenschutz dar, wird aber nun einer weit reichenden Überarbeitung unterzogen. Am 25. Januar 2012, also vor knapp einem Jahr, legte die Europäische Kommission ein Paket von Vorschlägen zur Aktualisierung und Modernisierung des geltenden EU-Regelwerks vor. Seitdem stehen die Komponenten des Pakets im Europäischen Parlament und im Rat zur Debatte.

Warum findet diese Überarbeitung statt? Im Endeffekt aus drei Gründen. Der erste ist, dass das aktuelle Regelwerk – genauer gesagt die Richtlinie 95/46/EG, sein Kernbestandteil – auf den neuesten Stand gebracht werden muss. „Auf den neuesten Stand bringen“ bedeutet in diesem Fall in erster Linie dafür zu sorgen, dass sie in der Praxis weiterhin *effektiv* bleibt.

Als die Richtlinie angenommen wurde, steckte das Internet noch in den Kinderschuhen; heutzutage leben wir in einer Welt, in der die Datenverarbeitung immer wichtiger wird. Folglich brauchen wir auch stärkere Schutzmaßnahmen, die in der Praxis gute Resultate liefern. Die Herausforderungen durch neue Technologien und die Globalisierung erfordern fantasievolle Innovationen, um einen effektiveren Schutz zu gewährleisten.

Der zweite Grund ist, dass das aktuelle Regelwerk zu einer wachsenden *Vielfalt und Komplexität* geführt hat, allein aufgrund der Tatsache, dass es sich um eine Richtlinie handelt, die in nationales Recht umgesetzt wurde – so ist es nun einmal bei Richtlinien – und wir nun in der EU 27 Versionen derselben Grundprinzipien haben. Das ist schlicht und einfach zu viel und führt zu zusätzlichen Kosten, aber auch zu einem Verlust an Effektivität.

Anders ausgedrückt gibt es einen Bedarf an weiterer Harmonisierung, um das System in der Praxis nicht nur stärker und effektiver, sondern auch *kohärenter* zu machen. Dies wird zu einem Abbau von *nicht hilfreicher* Vielfalt und Komplexität führen.

Der dritte Grund hat mit dem neuen institutionellen Rahmen der EU zu tun. Vor einigen Jahren, im Dezember 2009, ist der Vertrag von Lissabon in Kraft getreten. Dieser setzt einen Schwerpunkt auf Grundrechte, darunter insbesondere auch auf den Schutz personenbezogener Daten, u. a. mit Artikel 8 der EU-Grundrechtecharta und einer neuen horizontalen Rechtsgrundlage für Datenschutzregelungen in Artikel 16 AEUF, die für einen umfassenden Schutz in *allen* Politikbereichen der EU sorgt, egal, ob es um den Binnenmarkt, Strafverfolgung oder fast alle anderen Bereiche des öffentlichen Sektors geht.

Bei der Überarbeitung des Regelwerks geht es also um einen stärkeren, effektiveren, kohärenteren und *umfassenderen* Schutz personenbezogener Daten.

Ein enormer Fortschritt

Wir haben also ein Paket bestehend aus mindestens zwei Hauptvorschlägen: eine Richtlinie für – kurz gesagt – den Strafverfolgungsbereich und eine unmittelbar bindende Verordnung für den vorher von der Richtlinie 95/46/EG abgedeckten Bereich, also die Privatwirtschaft und den öffentlichen Sektor ausgenommen die Strafverfolgung.

Ich habe den Vorschlag für eine Datenschutzverordnung als „enormen Fortschritt“ hin zu einem effektiveren und kohärenteren Schutz personenbezogener Daten in der gesamten EU begrüßt, habe aber auch in Bezug auf eine Reihe wichtiger Einzelheiten um Klarstellung und Verbesserungen gebeten. Interessierte finden die substanzielle Stellungnahme des EDSB vom 7. März 2012 auf unserer Website, einschließlich aller einschlägigen Dokumentation.

Die Architektur des Pakets an sich – eine Richtlinie und eine Verordnung – weist jedoch darauf hin, dass dessen Zusammensetzung ein Problem darstellt; und in der Tat sehe ich darin den wichtigsten Schwachpunkt des Pakets. Das Schutzniveau in der vorgeschlagenen Richtlinie ist deutlich niedriger als in der vorgeschlagenen Verordnung.

Dies kann für sich genommen untersucht werden, aber der Austausch von Daten zwischen öffentlichen und privaten Stellen – etwa zwischen Strafverfolgern auf der einen und Banken, Telefon- und Reiseanbietern usw. auf der anderen Seite – nimmt zu, und ein Mangel an Ausgewogenheit an dieser Schnittstelle wird sehr viel weitgehendere praktische Auswirkungen haben.

Kontinuität und Wandel

Aber wenn wir uns nun auf die Verordnung konzentrieren, gibt es einige zentrale Punkte, die Sie alle bedenken müssen.

Erstens gibt es – trotz aller Weiterentwicklung – ein hohes Maß an Kontinuität. Sämtliche grundlegenden Konzepte und Grundsätze, die wir derzeit haben, haben weiterhin Bestand, wenn auch teilweise verdeutlicht und weiterentwickelt. Ein Beispiel für die Weiterentwicklung ist die stärkere Betonung der „Datenminimierung“ – sprich, nicht mehr Daten als unbedingt nötig zu verarbeiten. Ein weiteres Beispiel ist die Anerkennung des „eingebauten Datenschutzes“ als allgemeines Prinzip. Zusätzlich wird der Begriff „Einwilligung“ klargestellt: *Wenn* Sie eine Einwilligung benötigen, muss es sich um eine echte und robuste Einwilligung handeln.

Dort, wo Weiterentwicklungen ins Spiel kommen, geht es hauptsächlich darum, „den Datenschutz in der Praxis effektiver zu gestalten“. Das beinhaltet, wie wir sehen werden, eine starke Schwerpunktlegung auf die Umsetzung von Prinzipien und die Durchsetzung von Rechten und Pflichten, um den Schutz auch in der Praxis sicherzustellen.

Gleichzeitig sorgt die Verordnung für eine Vereinfachung und Kostensenkung. Ein gutes Beispiel ist, dass die Meldepflicht für Datenverarbeitungen abgeschafft wurde und nur noch in Situationen mit besonderen Risiken erforderlich ist. Darüber hinaus sieht die Verordnung eine zentrale Anlaufstelle („One-stop shop“) für Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten vor. Dies beinhaltet die Schaffung einer federführenden Behörde, die eng mit anderen zuständigen Behörden zusammenarbeitet.

Natürlich wird eine unmittelbar bindende Verordnung – im Prinzip ein einzelner, in allen Mitgliedstaaten anwendbarer Rechtsakt – auch eine deutlich stärkere Harmonisierung und Kohärenz mit sich bringen. Dies bedeutet für sich genommen auch eine wichtige Vereinfachung und Kostensenkungen für Unternehmen, die in verschiedenen Mitgliedstaaten tätig sind.

Allgemeine Anwendbarkeit

Lassen Sie mich auch betonen, dass die vorgeschlagene Richtlinie einen breiten Anwendungsbereich hat: Sie gilt sowohl für den privaten als auch für den öffentlichen Sektor. Dies entspricht vollständig der Situation, wie sie sich gemäß der aktuellen Richtlinie 95/46/EG darstellt. Die Möglichkeit einer systematischen Unterscheidung in der Richtlinie zwischen öffentlichem und privatem Sektor wurde ausdrücklich in Erwägung gezogen und verworfen.

Dieser umfassende Ansatz der aktuell gültigen Richtlinie war machbar, weil einige ihrer Bestimmungen, die sich auf öffentliche Aufgaben beziehen, relevanter für öffentliche Stellen sind, während andere, die sich auf Verträge und berechtigte Interessen beziehen, eine höhere Relevanz für die Privatwirtschaft haben.

Der EuGH hat eindeutig klargestellt, dass die aktuelle Richtlinie auch auf den öffentlichen Sektor der Mitgliedstaaten anwendbar ist, wobei er jedoch ebenfalls unterstrichen hat, dass einzelstaatliche Rechtsvorschriften nur dann als rechtmäßige Grundlage für Datenverarbeitung dienen können, wenn sie mit den Grundrechten vereinbar sind.

Gestärkt wird diese Position durch den Umstand, dass Artikel 8 der EU-Charta nun ebenfalls eine ausdrückliche Anerkennung des Rechts auf den Schutz personenbezogener Daten beinhaltet und Artikel 16 AEUF eine ausdrückliche horizontale Rechtsgrundlage für die Annahme von Regelungen in Bezug auf den Schutz personenbezogener Daten – sowohl auf EU-Ebene als auch in den Mitgliedstaaten – bietet, wenn im Rahmen des EU-Rechts gehandelt wird.

Gleichzeitig habe ich gefordert, das Verhältnis zwischen EU-Recht und einzelstaatlichem Recht in der vorgeschlagenen Verordnung sehr viel genauer zu untersuchen. Der Eindruck, dass durch die Verordnung sämtliche einschlägigen nationalen Rechtsvorschriften ersetzt

werden, ist nicht korrekt. Es gibt mindestens vier unterschiedliche Arten, wie einzelstaatliche und europäische Rechtsvorschriften nebeneinander bestehen und zusammenspielen werden. Dazu gehört auch, dass die Verordnung auf einzelstaatlichen Rechtsvorschriften aufbaut, sofern diese mit den Grundrechten vollständig vereinbar sind.

In diesem Zusammenhang sollten wir auch sehr genau abwägen, ob - und wenn ja, wo und wie – die Verordnung mehr Raum für eine Spezifizierung ihren Bestimmungen in einzelstaatlichem Recht zulassen sollte. Ich halte es jedenfalls grundsätzlich für nicht hilfreich, eine Umgestaltung der Verordnung in zwei verschiedene Rechtsakte – einen für den öffentlichen Sektor und einen für den Privat- bzw. den Wirtschaftssektor – in Betracht zu ziehen. Ganz im Gegenteil: eine solche Umgestaltung hätte *fatale* Folgen, sowohl für die Effektivität als auch für die Kohärenz des neuen Regelwerks, insbesondere für grenznahe oder grenzüberschreitende Dienstleistungen.

Sehen wir uns die Verordnung nun inhaltlich an. Sie stärkt die Rolle der Schlüsselakteure, also der betroffenen Personen, der verantwortlichen Organisation und der Aufsichtsbehörden.

Nutzerkontrolle

Die erste Perspektive kann als eine Aufwertung der Nutzerkontrolle betrachtet werden. Die aktuellen Rechte der betroffenen Person wurden sämtlich bestätigt, dabei jedoch gestärkt und ausgeweitet.

Das Erfordernis einer Einwilligung wurde klargestellt. Es gibt ein stärkeres Einspruchsrecht. Zusätzlich wurden auch die Mittel gestärkt, um sicherzustellen, dass die Rechte der betroffenen Person in der Praxis gewahrt werden. Es wird mehr Gewicht auf Transparenz gelegt. In einer Bestimmung wird ein kollektives Rechtsmittel eingeführt – keine Sammelklage im US-amerikanischen Sinne, aber immerhin Organisationen, die im Namen ihrer Mitglieder oder Stakeholder handeln.

Außerdem ist das „Recht auf Vergessen“ in aller Munde, aber wenn man genau hinsieht, wird im Grunde betont, dass Daten zu löschen sind, wenn kein ausreichender Grund vorliegt, sie weiter vorzuhalten. Das Recht auf „Datenübertragbarkeit“ ist im Grunde ebenfalls eine Präzisierung des derzeitigen Rechts, eine Kopie aller personenbezogenen Daten anzufordern.

Verantwortlichkeit

Das größte Augenmerk liegt auf einer echten Übernahme von Verantwortung durch verantwortliche Organisationen. Verantwortlichkeit ist kein Konzept, das erst *am Ende* greift, wenn etwas schief gegangen ist. Vielmehr handelt es sich um eine Verpflichtung, in der Praxis eine gute *Datenverwaltung* zu entwickeln. Dies zeigt sich in Formulierungen wie „sämtliche geeigneten Maßnahmen ergreifen, um eine Einhaltung sicherzustellen“ und „die Wirksamkeit dieser Maßnahmen zu überprüfen und den Nachweis dafür zu erbringen“.

Dies ist eine der wichtigsten Neuerungen. Sie impliziert auch, dass die *Beweislast* in vielen Fällen bei der verantwortlichen Organisation liegt, die z. B. den Nachweis erbringen muss, dass es eine angemessene Rechtsgrundlage gibt, dass es sich bei der Einwilligung um eine echte Einwilligung handelt und dass Maßnahmen weiterhin effektiv sind.

Die Verordnung beinhaltet auch einige spezifische Anforderungen, etwa die Notwendigkeit einer Datenschutz-Folgenabschätzung, die Dokumentation der Datenverarbeitung und die Ernennung eines/einer Datenschutzbeauftragten. Manche dieser Anforderungen, insbesondere zur Dokumentation, sind meiner Ansicht nach zu detailliert und bedürften gewisser Änderungen, um sie angemessener zu gestalten. Einige Ausnahmen in denselben Anforderungen sind möglicherweise nicht völlig gerechtfertigt. Eine bessere Ausgewogenheit in diesem Abschnitt der vorgeschlagenen Verordnung könnte beide Probleme auf einen Schlag lösen.

Darüber hinaus wurde eine allgemeine Bestimmung zur Meldung von Sicherheitsverletzungen aufgenommen. In den aktuellen EU-Rechtsvorschriften besteht eine solche Verpflichtung lediglich für Telekommunikationsanbieter.

Aufsicht und Durchsetzung

Ein dritter Schwerpunkt der Verordnung ist die Notwendigkeit einer effektiveren Aufsicht und Durchsetzung. Die Garantien für eine vollständige Unabhängigkeit der Datenschutzbehörden wurden in voller Übereinstimmung mit dem Urteil des EuGH in der Rechtssache gegen Deutschland gestärkt.

Die Verordnung sieht auch in allen Mitgliedstaaten Aufsichtsbehörden mit starken Durchsetzungsbefugnissen vor. Bußgelder in Millionenhöhe – in derselben Größenordnung wie im Wettbewerbsrecht – ziehen viel Aufmerksamkeit auf sich, aber die Botschaft ist:

„Wenn das hier wichtig ist, soll entsprechend damit umgegangen werden.“ Dies wird dazu führen, in Chefetagen den „Datenschutz“ sehr viel weiter nach vorne auf die Tagesordnung zu bringen, was sehr begrüßenswert ist.

In der Praxis sehen wir bereits jetzt eine rasche Zunahme verschiedener strengerer Durchsetzungsmaßnahmen: Abhilfesanktionen, Bußgelder und in einigen Fällen höhere Verbindlichkeiten. Dieser Trend wird in naher Zukunft zweifellos anhalten.

Die internationale Zusammenarbeit zwischen Datenschutzbehörden wird ebenfalls nachdrücklich unterstützt und erleichtert. Die Einführung einer federführenden Behörde für Unternehmen mit mehreren Niederlassungen wird begrüßt, wobei diese – wie gesagt – nicht alleine handeln wird, sondern im Rahmen eines eng zusammenarbeitenden Netzwerks in enger Abstimmung mit anderen zuständigen Behörden.

Ein sehr wichtiges Zusatzelement ist die Einführung eines Kohärenzmechanismus im Zusammenhang mit einem Europäischen Datenschutzausschuss, der sich auf die derzeitige Datenschutzgruppe gemäß Artikel 29 stützen wird. Dieser Mechanismus wird für kohärente Ergebnisse der Aufsichts- und Durchsetzungsmaßnahmen in allen Mitgliedstaaten sorgen.

Datenschutz weltweit

Ein letztes Element ist die internationale Dimension der Verordnung im weiteren Sinne. Der Anwendungsbereich der Verordnung wurde klargestellt und erweitert. Ihre Bestimmungen werden nicht nur auf die gesamte Datenverarbeitung durch Niederlassungen in der EU anwendbar sein, sondern auch für den Fall, dass aus einem Drittstaat Waren auf den europäischen Markt eingeführt oder Dienstleistungen dort erbracht werden oder das Verhalten von betroffenen Personen in der EU überwacht wird.

Wie Sie verstehen, ist genau das zunehmend die Wirklichkeit im Internet. Gleichzeitig ist es ein realistischer Ansatz, der auf einer wachsenden Synergie im Datenschutz in zahlreichen Ländern weltweit aufbaut.

In Bezug auf internationale Aspekte wurden zudem die Bestimmungen über grenzüberschreitende Datenströme erweitert und in einigen Aspekten modernisiert und vereinfacht. Es gibt nun eine spezifische Bestimmung über verbindliche unternehmensinterne Datenschutzregelungen, die verschiedenen Vereinfachungen beinhaltet.

Lassen Sie mich abschließend erwähnen, dass sich die internationale Zusammenarbeit zwischen Datenschutzbehörden – zum Beispiel zwischen der *Federal Trade Commission* in den USA und Datenschutzbehörden in der EU – auch in einem breiteren Kontext (GPEN) weiter entwickelt. Dies wird die Vorgehensweise in Bezug auf globale Akteure im Internet erleichtern und gründet ebenfalls auf einer zunehmenden Konvergenz von Datenschutzgrundsätzen und -verfahren weltweit.

Schlussbemerkungen

Meiner Meinung nach handelt es sich also um einen sehr begrüßenswerten Vorschlag, vorausgesetzt, dass einige wichtige Elemente in gewisser Hinsicht verbessert werden.

Abgesehen von der aktuellen Unausgewogenheit zwischen der Verordnung und der Richtlinie im Hinblick auf die Strafverfolgung habe ich bereits den Bedarf an mehr Raum für ein Zusammenspiel zwischen EU- und einzelstaatlichem Recht erwähnt, ebenso wie die Notwendigkeit, einige der derzeitigen Ausnahmen, u. a. diejenigen für kleine und mittlere Unternehmen, zu überdenken. Meiner Ansicht nach ist es *unerlässlich*, dass allgemeine Bestimmungen grundsätzlich *skalierbar* sind. Unangemessene Detailbestimmungen könnten hingegen zu unnötigen Ausnahmen führen.

Lassen Sie mich aus einer umfassenderen Perspektive betrachtet aber auch sagen, dass dies eine Zeit großer Chancen ist. Auch wenn es erforderlich ist, die ethischen Aspekte von Datenschutz und Privatsphäre erneut abzuwägen, ist es ebenfalls notwendig, den Bedarf an einem effektiveren und kohärenteren Schutz der Privatsphäre und personenbezogener Daten mit anderen wichtigen Themen, etwa einer wirtschaftlichen Erholung, zu verknüpfen. In diesem Zusammenhang werden die Digitale Agenda für Europa und die Strategie EU 2020 wahrscheinlich großen Einfluss haben.

In jedem Fall bin ich davon überzeugt, dass ein „intelligentes, nachhaltiges und integratives Europa“, wie es in diesen politischen Programmen angestrebt wird, ohne einen entsprechenden Schutz der Grundrechte, u. a. den Datenschutz und den Schutz der Privatsphäre, nicht erreichbar ist. Aus diesem Grunde ist diese hochrangige Konferenz so begrüßenswert und der Veranstaltungsort so gut ausgewählt.

Wie ich bereits kurz angerissen habe, steht die EU in ihren Reformbemühungen im Bereich des Datenschutzes nicht allein. Der Europarat und die OECD (noch nicht erwähnt) überprüfen ihre jeweiligen Regelwerke ebenfalls. Bislang gibt es eine bemerkenswerte Synergie zwischen den Anstrengungen. Dies ist von Bedeutung, um ein hohes Maß an Kohärenz und Zusammenarbeit weltweit zu gewährleisten.

Zu guter Letzt: Wo stehen wir in Brüssel? Im Moment finden Diskussionen im Parlament statt: dem LIBE-Ausschuss liegt mittlerweile ein Berichtsentwurf vor. Vom Rat wird erwartet, dass er im Verlauf des irischen Ratsvorsitzes bis Mitte des Jahres zu Schlussfolgerungen gelangt. Kommission und Parlament wollen zweifellos beide bis zum Ende ihrer derzeitigen Mandate 2014 zu abschließenden Ergebnissen kommen.

Auch wenn die Zukunft stets ungewiss ist, gehe ich davon aus, dass die vorgeschlagene Verordnung am Ende, natürlich mit gewissen erforderlichen Verbesserungen, angenommen wird, und ich werde mein Möglichstes tun, um dazu beizutragen.

Herzlichen Dank.